consultant editor: Jonathan Reuvid

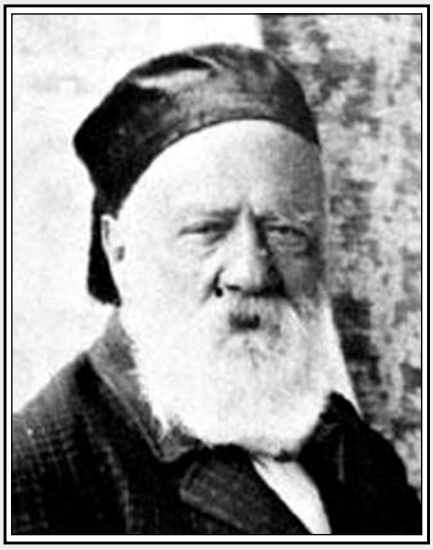
irm

7th edition

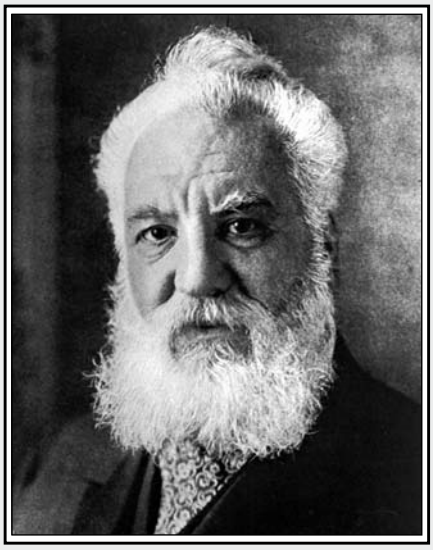
Managing Business Risk

A practical guide to protecting your business

Managing Business Risk



Antonio Meucci
Invented the telephone in 1849.



Alexander Graham Bell
Invented the telephone in 1876.

If you are the first, make sure you benefit from it.

Managing Business Risk

A practical guide to protecting your business

7th edition

consultant editor:
Jonathan Reuvid

LONDON PHILADELPHIA NEW DELHI

Publisher's note
Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and authors cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the editor, the publisher or any of the authors.

First published in Great Britain and the United States in 2003 by Kogan Page Limited
Second edition 2005
Third edition 2006
Fourth edition 2007
Fifth edition 2008
Sixth edition 2009
Seventh edition 2010

120 Pentonville Road
London N1 9JN
United Kingdom
www.koganpage.com

525 South 4th Street, #241
Philadelphia PA 19147
USA

4737/23 Ansari Road
Daryaganj
New Delhi 110002
India

ISBN 978 0 7494 5713 6
E-ISBN 978 0 7494 5901 7

British Library Cataloguing-in-Publication Data

A CIP record for this book is available from the British Library.

Library of Congress Cataloging-in-Publication Data

Managing business risk : a practical guide to protecting your business /
(consultant editor), Jonathan Reuvid. — 7th ed.
p. cm.
ISBN 978-0-7494-5713-6
1. Risk management. I. Reuvid, Jonathan.
HD61.M26 2010
658.15′5—dc22
2009045600

Typeset by Saxon Graphics Ltd, Derby
Printed and bound in Great Britain by MPG Books Ltd, Bodmin, Cornwall

IPR 360°

We take a broader view on your intellectual property rights.

We at BORENIUS & Co help your company to integrate your intellectual property rights with your core business operations through our unique IPR 360° service concept. Our **IPR 360° services** include defining strategies and processes, analysing markets and competitors, registering patents and trade marks, and licensing. BORENIUS & Co professionals have years of experience in international business, technological development, intellectual property rights, and IPR law.

Est. BORENIUS & Co 1928

WE KNOW HOW TO PROTECT KNOW-HOW™

BORENIUS & Co | Tallberginkatu 2 A, 00180 Helsinki, Finland | Tel +358 9 686 6840 | www.borenius.fi

Contents

Foreword

Where do we go from here?

With the world in the deepest recession since the 1930s, it's a good time to reflect both on our current woes and on how risk management might contribute to achieving a stronger and more sustainable basis for the future.

In her Preface to this edition, Dr Marie-Gemma Dequae stresses the importance of risk management at both board and operational levels. Adopting a 'bolt-on' approach will never be sufficient; risk policies must instead be ingrained at every level throughout the enterprise – from business objective setting to remuneration to reward policy.

There are some simple but powerful lessons on how we got to this state of affairs:

1. *Language.* The banks are recruiters of some of the best mathematics graduates in the world – people with the intellectual capability to develop and use ever more sophisticated approaches to market and credit risk calculation. Yet, even recently, articles with titles such as 'Fast Monte Carlo Bermudan Greeks' and 'Stepping through Fourier space' still graced the risk press. Whilst these are undoubtedly of value to those in the field, risk specialists must also learn to communicate in a language comprehensible to all if the assumptions inherent in such mathematical models are to be properly understood.
2. *Reward.* Pay and reward systems must reflect the longer-term mission and goal of the organization. The old maxim 'What gets paid gets done' holds true even in industries as sophisticated as banking. Rewarding short-term risk taking will inexorably lead to a focus on the short term, with scant regard to sustainability, yet it is the latter (and especially environmental sustainability) that consumers increasingly focus on when making buying decisions.
3. *Crowds.* There is a fascinating effect known as 'the wisdom of crowds' that says that, if you ask a large group of people to estimate the outcome of something, such as the number of sweets in a jar, the more people you ask, the closer the answer will be to the correct one. Whilst of value to quantitative conundrums in a situation where the crowd in question is rational, diverse and independent, it can be positively misleading in simple true/false situations. No

mathematical algorithm will ever be 100 per cent accurate and if, as happened in investment banking, everyone uses variations of the same algorithms to calculate risk then any inherent errors or assumptions in such systems will be amplified until they have a distorting effect on the market overall.

4. *Trends.* Macroeconomics will no doubt always suffer from market bubbles. From the rapidly escalating price of tulips in the 17th century, the run on railroad stocks in the late 1800s, and the belief only 10 years ago that every internet business had an inherent value, to today's residential property bubble, they will always be with us. Readers may indeed speculate (if that's the right word in this context) where the next one will come from – social networking media, green industries, emerging markets and even the recent retreats to gold from stocks and from paid employment to education are all areas to watch. More than these, the most important lesson is to keep our risk radar attuned to trends and to act at the right time – not, indeed, to follow the crowds.

If we look ahead, it is easy, like the proverbial 'rabbit in the headlights', to hunker down, paralysed by fear, and wait for better times ahead, only to suffer the inevitable fate of being run down by a competitor. Looking to the past, however, tells us that those firms that capitalize intelligently on the emergence of new markets, products and routes to business during a recession are those that will emerge most strongly from it.

In today's global economy, competition comes from the most unlikely sources – setting one's 'risk thermostat' too low will probably lead to ultimate commercial failure. As an example, the 2009 IFA Consumer Electronics Exhibition in Berlin, the world's leading show for that industry, was the largest ever, spanning over 23 halls – and in a recession too. In the words of Paul Otellini, CEO of Intel, 'If we want to return to prosperity, we have to invest in the future, not merely preserve the past.'

But do we all recognize this great time of opportunity? Recent research shows that, whilst 63 per cent of UK business leaders recognize current opportunities for growth, only 45 per cent expect to see it. Furthermore, just over a third said firms should positively avoid taking risks in the current climate, and only a quarter see risk as a way of making money. Risk taking therefore is getting a bad press. The signs are that much of this comes not from an appreciation of actual risk but from perceptions. We stop spending not because of any actual change in personal circumstances but because of fear that something bad might happen. As with the trends that led the world into recession, so again we are seeing what happens when firms follow the crowd. Not understanding risk leads both consumers and firms to avoid it – and potentially face the ultimate risk of extinction.

Faced with such extreme macroeconomic trends, what is the risk manager to do? Risk management is certainly much more in the spotlight than ever before, so risk managers need to make sure they are effective throughout the whole organization, not just up and down the chain of command. This is not an easy task. The burgeoning range of risk standards can help make sense of interdependencies and place

them in an enterprise-wide context, as can getting a formal qualification in the profession.

Books like this, too, provide invaluable advice on a range of relevant and practical topics, with a particular focus in this edition on the importance of intellectual property protection. Without a resilient strategy in this particular area, firms risk losing control over not just their products and markets but their brand and identity and ultimately their very survival.

In my experience, taking a wider view is of much value, as is communicating in straightforward language, listening but not following the herd, getting qualified, and being able to work effectively throughout the organization – all the while avoiding the rabbit syndrome. Risk management, ultimately, is about people who have the courage and determination to act effectively…

Steve Fowler
Chief Executive Officer
The Institute of Risk Management

Preface

Putting down the yo-yo

Marie Gemma Dequae, Federation of European Risk Management Associations (FERMA)

Scrutiny of risks must take place throughout the business cycle instead of the yo-yo approach to risk and performance management we are now seeing. Businesses should be more circumspect during a boom and prepared to take risks when conditions get tougher.

The global financial crisis has exposed weaknesses in our governance systems, and the way risks are treated and reported must evolve if the board of directors is to have the right oversight. Before the crisis, risk management had been inward-looking and short-term without sufficient attention to external and longer-term risks. There also was over-reliance on financial models.

By definition, the scope of enterprise risk management (ERM) is the enterprise, but even where companies had adopted ERM many of them failed to integrate it fully. The board of directors is responsible for overseeing the ERM process and management's responses. Merely adopting a risk management process is not enough; it must extend across and down through the programmes and implement a true risk culture within the enterprise. There must be continuous integration of the management of enterprise-wide risks and operational risk management.

In the heady period before the crash, management frequently did not organize the management of risk appetite well; nor did it set appropriate risk tolerance levels. The reporting structure was neither transparent nor adapted to a dynamic environment, and cooperation and risk management reporting and internal audit were not sufficient.

Suddenly, these weaknesses came into very sharp focus. Residual risks that had been reasonable or ignored when business was buoyant became unacceptable owing to the financial and economic crisis. Credit limits were cut, for example, jeopardizing supply networks. Top management reacted instinctively, perhaps because the risk acceptance policy had not originally taken into account the full and longer-term environment.

Better

There is room for improvement at board level and at operational level, and both must work in concert for ERM to be effective. The risk landscape constantly moves. Sometimes it does so in a fairly gradual way, but it is also subject to sudden seismic shifts. We need a more dynamic approach in risk management, starting with a more dynamic risk-mapping process that makes it possible to adjust policies in light of changing circumstances, not abruptly alter direction.

To agree a strategy and set the risk appetite, directors need to receive the right information and advice from senior executives. The design of the ERM programme has to be in line with the expected and desired outcome: is the organization mainly concerned with the downside protection (resilience) or with the upside opportunity (sustainability) or with a combination of both?

In terms of execution, the audit committee needs knowledge of the risks inherent to the strategy, and should evaluate the efficiency of the risk management system so it can give an accurate overview to the directors.

The best way to organize this is to create a risk performance committee, whose responsibility is to ensure that there is continuous coordination between the risk strategy and appetite sanctioned by the board and policy and practice at operational level. The audit committee can do this by becoming a risk and audit committee, or the business can create a separate committee reporting to the board.

How this risk performance oversight is organized will depend on the complexity of the risks the committee is to supervise, the sector of the company and the nature of the competencies that will need to be mobilized. Having at least one board member who understands risk management and its techniques is desirable. Perhaps it would be a good idea to organize training in risk management techniques for board members.[1]

The board should receive regular risk reporting from the chief risk officer (CRO) if the company has one and through another established channel if not. General management should provide the following information to the risk performance committee for possible transmission to the board:[2]

- risk-mapping results and balanced scorecards measuring performance and risk;[3]
- information on important incidents or trends within the company's activities;
- reports on CRO activities;
- reports from risk owners of big risks, risk elements in mergers and acquisitions and other strategic decisions.

Operational level

Not only should a good ERM reporting system be in effect, but it should also be linked with an efficient operational risk management and risk management process, including risk financing and insurance.

A sustainable risk programme calls for risk managers with suitable skills who will be responsible for leading the risk activities within the business. Technical, conceptual, business, personal and interpersonal skills are essential, and we need to pay special attention to developing leadership skills, strategic thinking, ethical judgement, innovative decision making and communication.

With lessons from the financial crisis, we can see that, as part of an effective ERM programme, businesses should take into account:

- the broader context, with risk management looking at and working with functions such as procurement, finance, performance and remuneration management;
- new technical and regulatory material, such as the European Environmental Liability Directive;
- greater interdependence of risks, as a result of the globalization of business,[4] for example in supply and distributions chains, including credit, and insourcing and outsourcing;
- project risk, as businesses increasingly organize activities like new product lines or geographical expansion in terms of projects;
- invisible risks, such as those assumed in contracts, which companies often take without full awareness of their potential consequential damage.

The reward structure for managers has to reflect risk performance and management and can include, in part, variable income based on good anticipation and follow-up of risks, reflecting the level of risk generated by their decisions.

To conclude, we can see how important it is to build good 'enterprise governance'[5] and to find risk managers with the right competencies. Successful ERM practices depend on the behavioural attributes of the organization at all levels. As such, the areas of opportunity for greatest organizational improvement concern risk appetite and risk tolerance, and a true risk acceptance process, together with risk performance management.

There is a need for a good organization and reporting system, bottom up as well as top down. Risk has to be part of all business decisions, and all types of risk have

to be analysed and treated. To be successful, ERM must be a dynamic, iterative activity.

> … for ERM to be effective, occasionally one does have to swim against the tide and run the risk of getting eaten by the sharks.
>
> Chris Duncan, former CRO of Delta Airlines

Notes

1. IFA and AMRAE (2009) *Rôle de l'Administrateur dans la Maîtrise des Risques*, IFA and AMRAE, Paris.
2. IFA and AMRAE (2009) *Rôle de l'Administrateur dans la Maîtrise des Risques*, IFA and AMRAE, Paris.
3. Ernst & Young (2009) *A New Balanced Scorecard: Measuring performance and risk*, Ernst & Young, London.
4. World Economic Forum (2009) *Global Risks 2009*, World Economic Forum, Geneva.
5. Wim Van der Stede (2009) Enterprise governance, *Financial Management*, February, pp 38–40.

Achieving Competency in Risk Management

In October 2008 a group of the UK's most senior businessmen and union leaders took advertising space in the national press to call on employers not to cut staff training in order to cut costs. They argued that "Now is precisely the time to keep investing in the skills and talents of our people. It is the people we employ who will get us through. When markets are shrinking and order books falling, it is their commitment, productivity and ability to add value that will keep us competitive. Investing now in building new skills will put us in the strongest position as the economy recovers."

Improved skills and competencies are needed at every level and in every business area, including risk management, if we are to weather the current financial and economic turmoil. Organisations have become starkly aware of the complex and interconnected risks that they face and should be starting to put into place the people and processes to address them. Stakeholder expectations of effective risk management are also rising. Yet there is still a long way to go: Aon's 2007 Global Risk Management Survey[1] found that over 25% of firms were not ready to handle the key risks identified - they had not undertaken any form of formal review and had not formulated a plan to deal with them. When it came to reputational and market risks up to 65% of firms were unprepared.

So we all know that there is much to be done – but do we have the skills to do it? A 2005 study[2] by Lloyd's concluded that whereas global business leaders were taking risk much more seriously (in just three years the time spent by boards on risk management had risen four-fold), there was a need for better education and training – less than a third of boards were training their staff in risk management skills and only 18% of board members had obtained such training themselves. Hopefully the picture is now starting to change.

So how can an organisation improve its competence in risk management? Here are some pointers:

- Get trained – it's right to say that all good managers are instinctively managing risk but there is a limit to how much you can make it up as you go along. There are specialist risk management skills and techniques that can be learned that will make life easier and improve results. Short courses in risk management include the new introductory course from the Institute

1 AON Global Risk Management Survey April 2007, Aon Corporation. www.aon.com

2 'Taking Risk on Board', Lloyd's in association with the Economist Intelligence Unit, 2005, www.lloyds.com

of Risk Management (IRM) – this is available either as a public course or can be brought in house and tailored to your organisation.

- Get educated – look out for the internationally recognised qualifications CIRM, SIRM, MIRM and FIRM (Certificant, Specialist, Member and Fellow of the Institute of Risk Management respectively). There are also an increasing number of specialist MSc courses in risk related subjects being offered by Universities. Other professional bodies may also have a risk management module available as part of their qualifications.
- Get in the experts – if you decide to seek advice from consultants or other professional firms then check that they also have relevant professional qualifications.
- Get the right tools – there are a number of risk management standards in circulation that will help you develop a systematic and organised approach. These range from the IRM/Alarm/AIRMIC Risk Management Standard[3], which is a simple plain language guide for the average business manager through to the COSO standard from the USA which has a strong regulatory/audit focus. In the UK British Standards (BSI) have issued their first Code of Practice in Risk Management: BS31100 and an ISO standard, ISO31000, has been published.
- Get yourself a network – strengthen your risk management contacts and access to information resources. Link into other risk professionals via attendance at risk conferences or through membership of a professional body such as the IRM which provides local and specialist groups and an online community and resources. IRM offers affiliate membership to anyone with an interest in risk who wishes to plug into the international network.
- Get your act together – organisations that aren't good at communicating, managing or relationships won't be much good at managing risk either. Successfully embedding effective risk management across your organisation requires a healthy management competence overall.

Carolyn Williams
Development Manager
The Institute of Risk Management
www.theirm.org
+44 (0)20 7709 9808
enquiries@theirm.org
November 2009

3 Downloadable for free from www.theirm.org

Contributors' notes

Dr Gunnar Baumgärtel is a partner at Maikowski & Ninnemann, a leading Berlin-based patent attorney firm specializing in all aspects of intellectual property law, including patent and utility model law, design patents and trademark law, as well as contract law (development contracts, licence agreements, etc). The firm concentrates on both prosecution and litigation and serves national as well as international clients. Dr Baumgärtel studied physics in Berlin and Paris and received his PhD in 1993, starting a career in intellectual property law immediately afterwards. He became a partner at Maikowski & Ninnemann in 1999. His work is evenly shared between litigation and prosecution, in particular concerning automotive technology, measuring technology, telecommunication and optics.

William E Bird is a founder partner of the IP law firm Bird Goën & Co. During the last 20 years he has worked as both a corporate and a private practice patent and trademark attorney in Germany and Belgium. He has expertise in both common law and codified legal systems, and in IP law, technology transfer, IP licensing and setting up spin-off companies. He is a European, British and German patent and trademark attorney, a tutor of CEIPI and a lecturer at the Vlerick School of Management.

Alistair Black is an Executive Advisor for KPMG LLP and a member of KPMG's European enterprise risk management practice. He has over 10 years' experience in the area of risk management and has worked with a number of global organizations to develop their approach to governance, risk and assurance. Alistair has worked across a variety of sectors and specializes in the areas of corporate governance and risk management framework design and implementation.

Armin K Bohmann is the founder and managing partner of the law firm bohmann || bohmann, founded as Bohmann & Loosen. The firm of bohmann || bohmann specializes in intellectual property law. Armin K Bohmann is involved in both prosecution and litigation of biotech and pharma cases and is a regular lecturer at the Santa Clara University School of Law and the Ludwig-Maximilians-Universität in Munich.

David Breden is Head of Operational Risk in the Strategic Risk Consulting Practice at HSBC Insurance Brokers Limited. He has been involved in operational risk management since 1995 and is a council member and fellow of the Institute of Operational Risk.

Emma Brooks is a Representation Manager at the Chartered Institute of Purchasing & Supply (CIPS).

Julian Buck is Version One's General Manager. Julian has over 20 years' experience in the IT industry, with previous roles including customer services and support director at COA Solutions, services director at Pegasus Software (now part of Infor) and director at ComputerLand UK. Version One Ltd is the author of electronic document management and imaging solutions. This 'paperless office' technology is seamlessly integrated into all major ERP and accounting systems.

Stephen Cash is Chief Executive Officer of NanoCentral, an alliance of organizations providing access to a broad range of leading edge technologies, equipment and services in the nano technology field. NanoCentral is driving the safe, beneficial and profitable commercialization of nano materials.

Corene Crossin and **James Smither** manage Control Risks' global political risk consulting practice. They have more than 20 years' combined experience addressing business risk issues in emerging markets and have led a variety of consulting engagements across multiple business sectors including energy, construction, pharmaceuticals, mining and defence. They have developed bespoke offerings and delivered training packages in areas such as supply chain risk management, business security and human rights. Asia and Africa specialists respectively, they publish regularly on regional and sectoral risk issues, present papers at leading industry and investment forums and are regularly interviewed by journalists on regional and global risk developments. Control Risks is an international business risk consultancy, whose aim is to enable its clients to take risks and accelerate opportunities in hostile and complex business environments. Since its foundation in 1975, Control Risks has worked in 150 countries for more than 5,300 clients – including three-quarters of the Fortune 500 largest global companies. It offers a range of integrated services designed to help in the analysis, management and monitoring of political, integrity, operational, security and reputational risks for corporate, government and non-profit clients worldwide.

Marie Gemma Dequae is Director Risk Management Platform at Vlerick Leuven Gent Management School. She is a member of the Board of the Federation of European Risk Management Associations (FERMA) and led a workshop at the FERMA Forum in Prague in October 2009 on the subject of mergers and acquisitions and another on supply chain risk management. The Forum programme is available on the FERMA website at www.ferma.eu.

Martin Drury is a risk management consultant with Towergate Corporate in East Anglia, undertaking client risk reviews and risk-related project work. He has 16 years' experience of risk consulting in various guises and is a strong proponent of

the greater integration of traditional insurance practices with evolving risk management practices. The Towergate Partnership is a UK award winning private company and is Europe's largest independent insurance intermediary, employing over 3,500 people and controlling £1.8 billion in gross written premium (GWP). Towergate Corporate division was created to deliver integrated insurance and risk management programmes that protect corporate clients' assets, liabilities and brand strength and help to promote their competitive advantage.

Barry Franks is a European patent attorney and manager of the Uppsala office of Brann AB. He started his career in IP as an examiner at the European Patent Office (EPO) in 1983 and, since leaving the EPO in 1993, has worked at GE Healthcare as in-house counsel, as well as in private practice. He works on strategic IP decisions, due diligence, freedom to operate, patent drafting, prosecution, oppositions, appeals and litigation.

Kristian Fredrikson is an attorney-at-law and partner at Brann AB. He has more than 10 years of IP experience and is specialized in IP litigation, licensing and marketing law. Prior to joining Brann AB he worked at the IP law firm RydinCarlsten. Brann AB was founded in 1949 and today has about 90 employees, of whom half are qualified attorneys dealing with patent, design, trademark and copyright matters. The company offers full IP services covering patents, trademarks, designs and copyrights, as well as litigation and agreements and other matters concerning marketing and competition law. In all these areas Brann AB offers qualified services and advice.

Allan Gifford is Head of the Enterprise Risk Management Practice at HSBC Insurance Brokers. By accessing the broad resources of HSBC Group, the practice helps clients to assess risk, and design and implement strategies for treating risk (ie blending financial solutions, risk transfer, risk retention and mitigation) within a framework of process, education and culture that provides management oversight and direction.

Rhys Griffiths is a senior associate within the Corporate Risk Management Group at Field Fisher Waterhouse LLP. He advises clients on the proper approach to health and safety planning and cultures. He also represents clients in their defence of all proceedings that may flow from a safety-related incident and has much experience in this area, both in the UK and abroad.

Keith Hardy is the Marketing and Technical Communications Manager at Nortech Control Systems Limited, a leading UK access control manufacturer and solutions provider. He has over 30 years' experience in the electronics industry and has been providing technical consultancy in access control to companies and institutions for five years. Nortech designs and manufactures complete access control solutions, including control panels, proximity readers and management software, plus specialist access management systems. These products have been used in key installations such as hospitals, hotels, ports, airports, sports stadiums and government buildings in over 20 countries. Nortech's success has been largely achieved through a close relationship with its customers and partners in the industry.

Matthew Hogg is Vice President at Liberty International Underwriters (LIU) with divisional responsibility for intangible assets and non-physical risks. He was formerly the EMEA Technology Leader for Marsh and Senior Vice President of the Communications, Media and Technology Practice (CMT). LIU is a division of Liberty Mutual Group and a global specialty business with an emphasis on niche insurance products. With a background in law, Matthew Hogg is a recognized expert on intellectual property risk and regular contributor in the media, at conferences and in book publications. He is also Chairman of the charity BELS, an Intangible Asset Finance Society (IAFS) membership committee member, a member of the Licensing Executive Society (LES) and an associate of the Chartered Insurance Institute.

Annelise Holme is an MSc in chemical engineering. Her experience includes the preparation and prosecution of domestic and international patent applications in pharmacology, biotechnology, biochemistry, cell biology, immunology and genetic engineering. She has previously carried out considerable work in the field of vaccines. She is further experienced in litigation practice, as well as oppositions and appeals before the European Patent Office. She is a member of FICPI, AIPPI and DDPAF and is a European patent attorney. Holme Patent A/S is a progressive firm of patent, trademark and design attorneys founded on the philosophy of providing quality work and fulfilling the diverse requirements of a spectrum of clients covering virtually every sector of business. The professional staff comprise experienced and qualified European patent attorneys and European trademark and patent attorneys practising in the variety of technical and legal disciplines required in an international intellectual property practice.

Pauline Hylton has been with the Lloyd's Register Group for 18 years. During her time with Lloyd's Register, she has held a variety of appointments in marketing, business development and product management. In her current role as Head of Strategic Marketing and Development, she manages the activities that drive LRQA's strategic thinking and direction. Pauline has delivered strategic direction and planning across a wide range of service development projects including supply chain assurance and sustainability assurance. As a member of the strategy team she has been integral to the development of LRQA's business assurance positioning.

Ari-Pekka Launne, LLM is a European trademark attorney and Vice-Director of Trademarks and Designs Operations at patent and trademark agency Kolster. He has had a career in trademark-related issues since 1998 and has been with Kolster since 2002. He is most experienced in IP litigation, anti-counterfeiting and brand strategies.

David Lawson is a management systems expert currently working with risk management programmes supporting LRQA's business assurance initiatives. David has worked with a variety of public and private sector clients, particularly in the areas of professional, technical, financial and project management. He is a member of the Chartered Management Institute and holds an MBA from the Open University.

Karri Leskinen is Managing Director, partner and patent attorney at Borenius & Co. With an MSc in chemical engineering, he specializes in chemistry as well as the

food and process industries. He handles innovation risk assessment, IP strategy planning and IP due diligence, as well as training and lecturing on IP matters. Drafting and prosecuting patent applications as well as litigating patents are also within his field of expertise. Borenius & Co is a consultant organization that has been practising intellectual property law in Finland since 1928. Borenius & Co offers worldwide protection of intellectual property rights and comprehensive insight and profound IP know-how to support its clients' strategic decision making.

Graham Massie is a director of CEDR (Centre for Effective Dispute Resolution) and a practising accredited mediator. He is a qualified chartered accountant and spent 10 years with KPMG in Chicago and London. He has been a company director in the United States and has established his own business consultancy practice, with extensive experience of multinational corporate consultancy.

John Moetteli, Esq is an international patent attorney and Managing Attorney of Moetteli & Associés SàRL, an IP firm in Switzerland specializing in preparing and filing US and European patent applications for global clients. He is currently a faculty member (PED programme) at IMD in Lausanne, where he teaches intellectual property strategy to business managers from around the world. Besides his almost 20 years' total IP experience, he has more than 12 years' experience filing US patent applications directly from Europe.

Fredrik Motzfeldt, CPCU, is a Senior Vice President of the Marsh Global Communications, Media and Technology (CMT) Practice, with responsibility for the Practice in EMEA. Marsh is the world's leading insurance broker and risk adviser, with 24,000 employees, revenue approaching US $5 billion and offices in over 100 countries.

In his current role, Fredrik is responsible for technical advice and new business development within the Technology, Media and Telecommunications sector in Europe, the Middle East and Africa. He acts as an adviser to and liaison with clients and Marsh offices worldwide on a broad range of technology, media and communications industry-related issues, including specialty subjects such as intellectual property and non-material damage business interruption.

Ruth Murray-Webster is an organizational change consultant, Managing Partner with Lucidus Consulting and a Visiting Fellow at Cranfield University School of Management. Success in business happens in a social setting, and her primary interest is in helping organizations bring together the 'hard' and 'soft' competencies they need to achieve their objectives. Lucidus Consulting exists to create value by shedding light on the implementation issues surrounding managed change through portfolios of programmes and projects. Decision making under uncertainty and the wider discipline of risk management for business and life are a key part of the Lucidus offering.

Jon Murthy is Marketing Manager at the United Kingdom Accreditation Service (UKAS), which has gained recognition in relation to risk management and the role that accreditation plays within the industry.

Stephan Peters is co-founder and CEO of Deposix, a leading software escrow firm in Europe and the United States. During his 18 years of professional experience in the IT industry, Stephan handled, among other things, a wide range of software licensing and intellectual property projects for clients at Accenture and Booz & Company. Additionally, he was involved in several technology start-ups, among others as a co-founder of WebToGo, a wireless ISP based in Munich. Stephan holds an MBA from Columbia Business School, New York and an MIS degree (Diplom-Informatiker) from the European Business School in Frankfurt. He is a frequent speaker and contributor to technology and business publications. The growing international client base of Deposix Software Escrow, which provides professional software and escrow services, is supported out of offices in Munich, Germany and California, United States.

Richard Pike is CCH Sword product director at Wolters Kluwer and has more than 15 years' experience in risk management and treasury IT. He has analysed, designed and managed the development of core risk management systems for large international financial institutions. He was recently chosen as one of the 50 most influential people in operational risk by *Operational Risk & Compliance* magazine. He is a regular speaker and writer on risk management issues.

Rolf Rings is a European and German patent attorney in a Munich-based patent attorney law firm. He is co-founder and Managing Partner of Rings & Spranger Patentanwälte and regularly publishes articles on IP management topics. In particular, he specializes in the elaboration of patent-related validity and infringement expert opinions. Owing to his combined technical and economic background, he was recently nominated as court expert for the purpose of the economic evaluation of a mid-size patent portfolio. Rings & Spranger Patentanwälte offers a full range of services in patent, trademark and design matters.

Allan Robinson is the Head of Risk and Value Management at Appleyards. After starting his career as a glaciologist with the British Antarctic Survey, he is now an expert in the use of quantitative and qualitative techniques to support decision makers facing complex problems. Appleyards is a Sunday Times Top 100 Best Company, as voted in both 2008 and 2009. Founded and run as a family business in 1936 and incorporated in 2000, Appleyards provides consultancy, advisory and management support services to the public, private and third sectors.

Daniel Rouse is a senior associate in the Dispute Resolution Group at Field Fisher Waterhouse LLP. He specializes in complex insurance and reinsurance disputes.

Paul Saville-King is a managing director of Critical Engineering Solutions for Norland Managed Services. He champions the reduction of risk in engineering services through a unique critical engineering and risk management (CERM) business model in collaboration with key account clients, technical experts and consultants from the industry. He holds an MBA with distinction from Ashridge and is a full member of the Institute of Incorporated Engineers (IIE), a fellow of the Chartered Management Institute (FCMI) and a member of the British Institute of Facilities Management (MBIFM).

Andrea Schüssler is a German and European patent and trademark attorney and one of the founding partners of Huber & Schüssler. Based in Munich, Huber & Schüssler is an internationally orientated intellectual property law firm with patent attorneys and attorneys-at-law. The firm has particular expertise in technologies and legal issues relating to the technical field of life science in its broadest sense. Huber & Schüssler and its staff support their clients in all issues of intellectual property and have great experience in the identification of valuable inventions, worldwide prosecution and enforcement of patents and questions of technology transfer.

Marco Serravalle is the founder of Serravalle sas, a boutique intellectual property practice that provides a broad spectrum of activity, from priority searches to non-infringement opinions. Thanks to his experience as an EPO examiner, Marco Serravalle specializes in the prosecution of European patent applications and oppositions to EP patents.

Kim Simelius is the Managing Director and a patent attorney at Tampereen Patenttitoimisto Oy, and has experience in science, international business and intellectual property rights. He has the degree of Doctor of Science and Technology from Helsinki University of Technology in the field of biomedical engineering, and the degree of Master of Science in economics from the University of Tampere. His specialisms in IPR are business risks related to patents owned by competitors and hostile patent holders. Tampereen Patenttitoimisto offers a complete range of services in patents, trademarks and IP law and is a member of the Berggren Group, a leading intellectual property agency in Finland.

Peter Simon is a project management specialist, Managing Partner with Lucidus Consulting and a Visiting Fellow at Cranfield University School of Management. He has extensive experience of risk management, both in businesses in general and on major projects and programmes, which gives him a sound platform on which to advise others.

Nathan Skinner is Associate Editor of *StrategicRISK* magazine, the European risk and corporate governance journal (www.strategicrisk.co.uk). He grew up in the Brecon Beacons in Wales and has an MA postgraduate degree in journalism and cultural studies from Cardiff University. Whilst primarily a business journalist with specialisms in risk, insurance and corporate governance, he has also worked for other periodicals including newspapers. Immediately after graduating, Nathan spent two years in Toronto, where he began his career in business journalism.

Andrew Templeton is the Deputy Head of the Risk Management Services team with the Corporate Customer Group team of HSBC Insurance Brokers Limited. The team provides a range of survey, risk management and consultancy services to clients. He has worked in the insurance industry for 36 years for major insurance companies and brokers, with the last 30 years in the risk management arena. He is a chartered safety practitioner, a chartered institute practitioner and a member of the International Institute of Risk and Safety Management.

Alexandra Underwood is a senior associate in the Disputes Resolution Group of Field Fisher Waterhouse LLP.

Helene Vik is Director of Business Development, US Operations at Ipendo Inc. She holds an MBA in strategic management from Alliant International University, San Diego, United States and an MSS in social and economic geography from Uppsala University, Sweden. She has a background in business consulting, with a specialism in strategic management. Ipendo is a leading provider of IP management software and services, providing companies with a paperless system to organize and streamline the global management of intellectual property. The Ipendo Platform™ is a powerful yet user-friendly and simple tool that supports the management of all IP processes, including invention submission, contract management, prosecution, licensing, maintenance, budgeting and forecasting of IP rights. The platform enables safe and secure online collaboration and service exchange with law firms, agents, partners and patent and trademark offices.

Simon White is Environmental Branch Manager for XL Insurance, one of the largest global suppliers of specialist environmental insurance policies. He has over 10 years' experience in environmental insurance underwriting. He joined XL Insurance in 2005 and is currently responsible for the international underwriting team, servicing clients outside North America. Simon holds a BSc and MSc in environmental policy and an LLM in environmental law. He has also written various articles on environmental insurance and spoken at numerous conferences across Europe on this topic. 'XL Insurance' is the global brand name used by member insurers of the XL Capital Ltd group of companies.

As a global leader in its field, XL Insurance helps industrial and commercial businesses manage their risks by offering integrated, comprehensive and cost-effective insurance and risk engineering solutions with the expertise to cover exposures in fields ranging from worldwide property and casualty to professional lines, energy, marine and aviation and environmental insurance.

Introduction

Past editions of *Managing Business Risk* have featured a wide variety of topics. Areas of risk management that were highlighted have ranged successively from change and continuity, integrity, corporate governance and accountability to crime and terror, and from good practice, innovation and expansion to the use of IT in risk solutions. The 2009 edition was focused on corporate risk, areas of legal risk and risk in managing sustainables.

The primary focus of this new edition is on risk in intellectual property (IP), in terms both of identification and management and of the various aspects of patent filing and defence, and litigation in the event of infringement. These topics occupy two of the five parts of the book.

Readers may ask themselves why the 2010 edition should concentrate to this degree on IP. Steve Fowler's thought-provoking Foreword provides the clue. At a time when businesses are still coming to terms with the after-effects of the credit crunch and a slow emergence from recession, the most successful firms will be those 'that capitalize intelligently on the emergence of new markets, products and routes to business'. The creation, safeguarding and maintenance of IP are integral to this activity and may give a company the critical competitive edge in developing and expanding its business.

The three remaining parts of *Managing Business Risk* this year cover risk management strategies (Part 1), which are of key concern at board level, the management of insurance and legal liability risks (Part 2) and core topics of operational risk management in current business conditions (Part 4). In these areas, we welcome back regular contributors from previous editions who have chosen to write on new topics or have returned to their areas of expertise and updated their texts.

Of the 15 chapters on IP topics in Parts 3 and 5, all but one are authored by leading international experts from firms based in continental Western Europe and one in California. This international coverage is, of course, entirely appropriate to the risk management of patents, copyright and trademarks, which are by definition of an international nature, and confirms the global attention that professional IP management commands today. Together, they provide a comprehensive study of the subject.

Steve Fowler of the Institute of Risk Management (IRM), our publishing associate, and Marie Gemma Dequae of the Federation of European Risk Management Associations (FERMA), with whose writing readers of previous editions will be familiar, have written the Foreword and the Preface respectively for this edition. We offer our sincere thanks to them, as well as to all chapter authors for their contributions.

The Contributors' Notes section of the book, which precedes this Introduction, provides biographical detail of all authors and their firms. Readers who wish to get in touch with any author will find contact details at the end of the book.

As always, the sponsorship and advertisements of many contributors are an essential ingredient to the publication of *Managing Business Risk*, and our thanks are due to them for their participation.

In my Introduction to the 2009 edition I wondered what would be the dominant themes of this edition; again, without any prior knowledge, I shall look forward to the next collection of topics that contributors to the 2011 edition select.

Jonathan Reuvid

1

Risk Management Strategies

Putting your risk management needs at the centre of our world.

At HSBC Insurance Brokers we strive to provide our clients with the confidence and certainty to pursue their objectives. As one of the largest insurance broking organisations in the world, HSBC Insurance Brokers has the depth of knowledge to analyse complex situations from multiple perspectives and develop innovative solutions that proactively meet the specific needs of our clients.

The Intelligent Alternative

Call: +44 (0)20 7661 2050
Email: insurancebrokers@hsbc.com
Web: www.insurancebrokers.hsbc.com

HSBC Insurance

1.1

Using risk tolerance statements to embed operational and strategic risk management

David Breden, Strategic Risk Consulting Practice, HSBC Insurance Brokers Ltd

Introduction

The financial crisis that swept around the world through 2008 and 2009 has drawn attention to many failings of risk management in financial institutions.[1] We have learnt that, in today's global market, risk is highly contagious. We have seen how a problem in a geographically restricted business area such as the US housing market is now capable of sending shock waves around the world capable of destroying firms that had previously been considered sound and resilient in their own market. We have learnt that risk management now needs to be much more aware of the threat posed by international market trends and by counterparty failure.

Such awareness has, however, not come naturally to many organizations, for a further shortcoming highlighted by the crisis is the failure of many to fully comprehend the true potential impact of a disaster. This tendency, technically known as disaster myopia, leads managers of businesses to dismiss the possibility of significant high-impact disruption in their business area as much too unlikely to warrant close attention. Even when disaster scenarios have been considered, the collective wisdom of the business tends to minimize potential impact, meaning that possible corrective action is not considered appropriate given the understated potential damage to the firm. There is no need here to provide examples of this condition, for the danger of black swan events has been fully explored by Nassim Nicholas Taleb[2] and indeed has featured prominently in the press in the last two years as a series of banks failed around the world. Now, just like motorists slowing down after an accident, financial institutions are more than ready to take account of potential disaster scenarios – until the memory of the accident fades and they revert to normal speeds!

The temptation to disregard risk was of course favoured by the fact that individuals and businesses were incentivized to take increasing risks in order to earn ever greater rewards. Potential negative events were minimized, as we have seen, and, following 10 years of unprecedented economic stability, all financial models that were based on recent historical data confirmed that the economic downturn had indeed been banished, as the data the models used contained no extreme shocks. Armed with such reassurance and faced with increasing financial targets in order to win bonuses, there was little reason for ambitious and intelligent people to consider the potential downsides of their strategies and actions.

All of the above points to one common lesson. This is that risk management has to be embedded in the strategic decision-making process of all businesses. If this does not occur, then the failings highlighted above will come to the surface. The businesses will be able to disregard potential negative scenarios and will not 'waste' time and money trying to protect themselves against such unlikely events. When events do not turn out in precisely the way planned then the businesses will not have considered such eventualities and will find themselves wholly unprepared to meet the challenge posed by the unexpected adverse circumstances that have arisen. To quote the recently published British Standard BS 31100: 'Risk management has to continuously, systematically and proportionally address the risks surrounding an organisation's activities. It cannot be separated from the culture of the organisation.'[3]

Achieving the integration of risk management into the culture of the firm represents a significant challenge – particularly for a risk such as operational risk. To achieve this integration it is fundamental that clear direction is given by the firm's board or other governing body that percolates through the organization to ensure that all are aware of their responsibilities to manage risk in conjunction with commercial activities in order to ensure that the business does not unwittingly or consciously take on more risk than those responsible for the firm's strategy consider appropriate. A statement of risk tolerance or appetite is the usual way of achieving this objective.

Risk tolerance statements for operational risk

Risk tolerance or appetite reflects the degree of uncertainty that a firm or an individual is prepared to accept in order to achieve financial objectives. It is a common concept in investment decisions, where a responsible investor will consider the extent of loss that he or she is prepared to accept to obtain a higher rate of return. Here, an investor can choose to accept a high level of risk in return for a more generous level of reward, whilst the more conservative will seek to protect their capital investment and receive a lower rate of return.

In the case of an investment, the individual is choosing to accept risk in a conscious manner, and an investment firm will look to ensure that its client follows a clear process to understand his or her appetite or tolerance levels for risk. In the case of operational risk, however, we encounter an immediate difficulty. Operational risk is often defined as 'The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events'.[4] Consequently it covers a vast array of risks, most of which are inherent to the day-to-day working of the firm. Every business (or at least all those that employ people, use systems or processes or are exposed to external threats – which is the same thing) is subject to operational risk, and will be from the moment that it commences trading to the moment the firm is liquidated. Businesses have little choice but to accept the presence of an exposure to operational risk. However, they can make a conscious choice as to their attitude to this risk. By investing in robust and effective control frameworks the firm can limit the likelihood and impact of risk events, but in doing so will add to its cost base, whether through payment of an insurance premium or by increasing staff numbers or system security, to implement additional controls and checks – and this will evidently reduce bottom-line profitability. .

Amongst regulated firms the insurance industry is obliged to create a risk tolerance statement for operational risk. Financial Services Authority (FSA) regulation states that an insurance firm must include in its risk policy documentation details of 'the operational risks that the firm is prepared to accept and those that it is not prepared to accept, including where relevant some consideration of its appetite or tolerance for specific operational risks'.[5] For unregulated firms, the British Standard on Risk Management also recommends inclusion of a risk appetite statement in the governing risk policy document.[6]

The FSA, meanwhile, also clarifies exactly what such a tolerance statement should cover:

> Tolerance describes the types and degree of operational risk that a firm is prepared to incur (based on factors such as the adequacy of its resources and the nature of its operating environment). Tolerance may be described in terms of the maximum budgeted (that is expected) costs of an operational risk that a firm is prepared to bear, or by reference to risk indicators such as the cost or number of systems failures, available spare capacity and the number of failed trades.[7]

Therefore, tolerance can be quantitative and describe levels of risk impact or number of events, or qualitative by addressing factors that are likely to lead to increased levels of risk (number of unresolved complaints, number of errors, etc).

The statement will generally also distinguish between risks for which the firm has no appetite (such as internal theft and fraud or breach of law or regulation) and those that may be accepted within reason (staff error, some degree of inevitable system downtime, etc). Acceptance is likely to reduce rapidly, however, when accepted risks are repeated too often.

The statement will also need to recognize that tolerance levels for risk may change over time or in certain circumstances. A firm that has recently taken over a competitor and then suffers a series of losses will be accused of biting off more than it can chew, with consequent damage to the reputation of the firm's board and management, whilst the failure of a high-profile initiative will damage reputations for some time ahead. For example, the early problems in respect of baggage handling at London Heathrow Airport's new Terminal 5 continue to mean that any traveller arriving from that terminal will still be asked, with concern, whether baggage has arrived safely 18 months after the unfortunate events associated with the launch.

Integrating the risk tolerance statement into the operational risk process

The risk tolerance statement therefore serves as a signpost provided by the board of directors to the rest of the organization that indicates the type of organization that the firm aspires to be. As such, it should direct the response that all levels of the firm should produce when confronted by a risk (whether actual or potential) that may exceed risk tolerance levels. As a result, the tolerance statement will be closely entwined with all aspects of the operational risk management process.

Risk identification and assessment

The operational risk framework will normally seek information from business units regarding the risks that are faced in the business. This will be achieved either by way of a series of workshops designed to identify the risk or through a self-assessment process whereby business units assess exposure against a checklist of risk types. In both cases the unit will be asked to assess both the likelihood and the potential impact of an event in a worst-case scenario. In many cases the unit will also be asked to assess the effectiveness of the existing control framework. In this way the business will be able to consider both the inherent risk that the unit faces and its residual risk, on the assumption that the control framework does not fail. Regardless of method, assessment will be made on a constant scale that will normally consider a range of impacts running from financial to impact on staff, customers, media, etc. The categories of impact should be driven by the tolerance statement, and the board should be prepared to indicate to the business where priorities lie across the categories. They may indicate, for example, that a loss of service to clients lasting more than six hours or a critical and justified story reported by the BBC is equivalent to a one-million-pound loss and is, therefore, to be avoided whenever this can be done in a cost-effective manner. In general terms, most risk identification processes will

set a threshold combination of likelihood, potential impact and effectiveness of controls, which if exceeded will require targeted action to be taken either to reduce the potential effects of the risk or to enhance control structures. The further the threshold is exceeded the greater the priority for action. By adjusting this threshold or varying the assessment bands, the risk management department can reflect changing board attitudes to risk. By lowering the threshold, more risks will be identified that require corrective action, and a tighter attitude to risk will be achieved. Of course, care will need to be taken to ensure that business units do not relax assessments to offset the tightening of thresholds.

The same principle will apply to actual losses suffered. Whenever a loss of sufficient severity occurs, the organization will tend to mobilize resources to prevent recurrence, again weighing the cost of prevention against the benefit of preventing repetition. The tolerance statement will generally indicate where this boundary lies, either by specifying an absolute level of incident that the firm wishes to avoid or by defining a percentage of income or profitability that, if exceeded by a loss, would constitute a severe event for any business unit.

Equally, indicators that have been found to point to higher levels of risk can be adjusted to ensure that issues are addressed earlier or later depending on levels of tolerance for risk.

Of course, this activity will also determine at what levels firms will purchase insurance or any other form of financial protection. It is to be expected that, when risk tolerance is low, more high-impact risks will fall to be transferred, as the business seeks to protect a core level of profitability that is less susceptible to unpleasant surprises. The activity will imply greater costs as insurance companies seek higher premiums to take on the increased levels of risk. As an alternative, the business may choose to accept a higher level of lower-value losses that can be expected to occur with greater frequency in return for higher limits that will protect the business from the most significant shocks. This has the potential to reduce the increase in premium, but will also expose the business to higher levels of expected loss (which may be addressed by enhanced control structures). In any of these cases the result will be acceptance of higher costs in return for avoidance of extreme losses that might endanger the firm's future.

In all cases, the tolerance statement drives the behaviour of the firm in ensuring that the most severe risks that the business faces are addressed with greater speed when there is less willingness to accept risk. The board's strategic position will be cascaded down through the firm and factored into the firm's risk management processes.

Scenario analysis in operational and strategic risk management

Naturally, the firm will be concerned to identify potential scenarios that may threaten its future success. The board will seek to develop an understanding of the sort of circumstances that could lead to the failure of the business, and will expect mitigating action to be taken to prevent events that could have a fatal impact on the firm.

The use of scenarios will be particularly helpful when evaluating the risks associated with new products or services. With no past experience, the role of the risk management team will be to work alongside the commercial team, examining the performance of the product under a range of market conditions and evaluating the threats when market or operational conditions are not as hoped in the commercial projections. It should be made clear that the risk manager will not be seeking to prohibit a particular initiative; rather the intention will be to highlight those circumstances in which the proposal has the potential to breach tolerance levels. In those cases, identification of the risk will often enable the business to develop a mitigation or control framework that will be effective in addressing product performance under the adverse events detected. This may be through purchase of a financial hedge or an insurance policy, with a resultant increase in costs and a reduction in best-case profits, but a more consistent income stream will be achieved as the project will be less subject to surprises and volatility caused by changed circumstances. Failure to consider the potential downside scenario will leave the firm unprepared and exposed to negative results.

Incentive structures to support risk management

The risk tolerance statement should also influence the reward structure in the firm. In the introduction to this chapter I made reference to the negative impact of incentives that merely focus on the generation of income. It is necessary to recognize that the remuneration framework should reward the behaviour that the board of directors wish to see. If we assume that there is no desire to encourage behaviour that has the potential to destroy the firm, then all members of staff must be rewarded for managing risk in such a way as to support the firm's desired stance for risk. There is a balance to be struck between all-out pursuit of a short-term profit and total risk aversion. This balance is described in the tolerance statement and should then be reflected in the objectives that are set in each business unit. When tolerance levels are relaxed in favourable circumstances, then the balance swings towards reward, but without eliminating the input of risk management. In more straitened times the focus shifts towards risk management, with an acceptance of lower but less volatile levels of profitability. In either case the reward system follows the board's lead on the levels of risk that the firm can afford to take on.

Conclusion

The financial crisis has shown that risk management cannot be effective unless it is firmly embedded in the way that the firm considers its strategic direction and makes business decisions. The risk manager must understand what level of risk is appropriate for the business and must then adjust the risk management processes and systems to ensure that this level of risk is achieved. The guidance is provided by the risk tolerance statement, duly reinforced by the reward and remuneration struc-

ture. In this way the firm can achieve a consistent, embedded approach to risk management.

The views expressed in this chapter are the author's personal views and do not necessarily represent the views of the HSBC Group.

Notes

1. For a more extensive discussion of the failings of risk management processes in banks in the financial crisis see 'Why banks failed the stress test', speech by Andrew G Haldane, Executive Director, Financial Stability, Bank of England, 9–10 February 2009. Available on the website of the Bank for International Settlements, www.bis.org.
2. See *The Black Swan* by Nassim Nicholas Taleb (Allen Lane, London, 2007).
3. See BS 31100:2008, 'Risk management: code of practice', BSI British Standards, October 2008.
4. Definition drawn from Basel II documentation 'International convergence of capital measurement and capital standards: a revised framework – comprehensive version', June 2006, by the Basel Committee on Banking Supervision, Bank for International Settlements.
5. Taken from the FSA *Prudential Sourcebook for the Insurance Industry*, Ins Pru 5.1.10 (2), June 2009, Financial Services Authority, London.
6. See BS 31100:2008, 'Risk management: code of practice', para 3.3.2, BSI British Standards, October 2008.
7. Taken from the FSA *Prudential Sourcebook for the Insurance Industry*, Ins Pru 5.1.12, June 2009, Financial Services Authority, London.

1.2

Back to basics – getting enterprise risk management right in turbulent times

Alistair Black, European Enterprise Risk Management Practice, KPMG LLP

Introduction

The current economic climate has increased business exposure to uncertainty and volatility. The differentiation between those organizations with effective risk management systems and those without is more evident than ever. Despite the evolution of risk management systems since Turnbull, recent events would appear to demonstrate that many organizations are still driving their risk approach from a compliance 'tick in the box' perspective that does not engender business buy-in or drive improved performance.

What are the reasons for failure?

It could be argued that there are a number of reasons why risk management has failed – limited buy-in and involvement of executive management with the business being a significant contributor.

The fact that many organizations still view risk management as essentially an annual risk identification exercise for presentation to the board has also resulted in business failure. Whilst this is important, it is also important not to lose sight of other areas of activity that make a risk management process sustainable: such as ensuring appropriate governance structures to oversee the risk management process, using the output of the risk process to determine focused internal audit activity and using risk information to inform strategic decision making, allocation of resources and business planning activities.

As a result of insufficient oversight and challenge from many boards and executive management, the company risk profile for many organizations has remained static year on year. This lack of movement indicates that 'risk management' is being viewed as a compliance requirement and not a business critical activity. As evidenced by the recent financial crisis, these are the organizations that have struggled to adapt their strategy quickly enough to respond to the challenging and rapidly changing economic environment.

What opportunities are being missed?

One of the key benefits to the board and audit committee of an effective risk process is the assurance it also provides over its key controls to manage high-risk areas. At times, however, assurance activity is limited to the traditional risk areas such as health and safety, with insufficient focus on emerging risk areas such as technological or regulatory change. This can create a false sense of security over the effectiveness of the system of internal control. Ensuring that sufficient capability exists within an organization's internal audit department to test enterprise-wide controls is therefore also key.

Further opportunities to be gained from an effective risk management system include a reduction in volatility in performance outcomes through forward planning and anticipation of emerging risk areas.

We often observe boards and executive management bombarded with too much risk information and limited mechanisms for receiving a consolidated view of the key risks facing their organizations. Furthermore, risk registers do not always reflect the real risk environment of the organization. Effective risk identification, analysis and reporting are therefore critical to ensuring buy-in, involvement and effective challenge from the top.

The starting point to overcome some of these challenges often begins with a review of 'risk governance', ie positioning of risk within the organization, including a clearly defined role for the risk function, supported by clear accountabilities for risk management at all levels across the organization.

What improvements are required?

If the last few years are anything to go by, ineffective and uncoordinated risk management has been a cost to the organization that has delivered little value. This will continue to be the case unless a number of key improvements are made:

1. *Greater engagement from the board and the executive.* The board and executive must set the tone from the top and be fully involved in the development and communication of risk management across the organization. This will also ensure alignment between the risk management process and the strategic agenda. Since the fallout of the financial crisis there has been greater external focus on governance and risk management (eg the Walker Review, the FRC review of the Combined Code, etc). Boards of companies are now under increasing pressure to demonstrate how they intend to respond and improve their approach to risk management. Therefore, it is critical for them to embrace risk management and be seen proactively to increase awareness of risk throughout their organization.
2. *The risk management function should be positioned appropriately within the organization's governance structure.* In a recent survey of 500 senior banking managers, approximately three-quarters believed the risk function was stigmatized. How the risk function and its role are positioned within the organization is key to the success of the risk management approach. However, the survey did indicate that seven out of 10 believe the risk function holds more influence than it did two years ago, while even more believe the way they manage risk to be a source of competitive advantage. In addition, many respondents felt the process is exerting greater authority over the key areas of strategy development and capital allocation. They did however acknowledge that the tag of being a back-office support function should be cast off if the risk function is to progress still further – this must be addressed, and a clear tone from the top is critical to delivering this enhanced value. There has been much talk of the chief risk officer role but, regardless of whether this role is deemed appropriate, organizations must ensure risk management considers and informs core processes such as M & A, financial strategy, product development and forecasting. This all-inclusive approach is critical in embedding a risk-aware culture across the organization.
3. *The business case must be clear and it must not be focused solely on compliance.* There must be a clear understanding of stakeholder expectations for risk management as well as the business case. Senior management must be able to articulate very clearly what the drivers are for risk management and how the process will deliver value across all levels of the organization. We often find our clients spending a disproportionate amount of time on compliance aspects of the role and not enough time on building relationships and raising awareness of risk management with key stakeholders across the organization. It is critical that the risk function does not become solely focused on controls and monitoring. A balance must be struck, with the appropriate amount of time being spent on horizon scanning and spotting opportunities.

4. *Roles and responsibilities must be clear.* In many cases the business does not believe it owns risk and sees this to be the role of the risk manager. Therefore, roles, responsibilities and accountabilities must be clearly defined and understood by those individuals. In order to effect positive change in the risk environment and derive value from the risk process, it is important for the risk function to work closely with the business and to be on hand to provide support and advice where required. It is critical that this advice is not confused with ownership. The business must own the risk to ensure that an improvement in the risk culture takes place across the organization – with improved decision making.
5. *The audit committee, board and executive must have sufficient experience, skills and capabilities in order to oversee and challenge the risk process.* The recent financial crisis has highlighted concerns over the level of risk expertise of top-level management and independent non-executive directors and their ability to perform their role effectively. Owing to the lack of risk expertise across some boards, this has resulted in insufficient time spent in the boardroom discussing and challenging the management of risks across the organization. It is therefore critical for boards to take stock of their risk management capabilities and determine appropriate steps to ensure that they are suitably qualified to fulfil their duties effectively.

How organizations should respond

The current economic conditions are making it more difficult to respond. Despite recognizing that there is a general lack of expertise in the organization, many companies are unwilling to recruit these skills because of budget constraints. A number of organizations are now seeking to provide formal training to their boards and personnel with formal risk management responsibilities to ensure that an effective system is in operation.

Other obstacles to developing robust risk management that we see include poor data quality and availability, shortage of relevant expertise, and ineffective tools and technology. It is therefore key that, despite budget constraints, organizations take a holistic approach to improving risk management within their organizations and also address the shortcomings noted above.

In recognition of this, as risk professionals, we must all challenge how our organizations are currently managing risk. We must:

1. consider whether we have a single, accurate and dynamic picture of existing and emerging business risks in today's environment;
2. challenge whether risk and assurance activities need to be redefined in the light of the economic climate;
3. confirm whether an appropriate supporting framework to maintain and incentivize appropriate risk management behaviour exists;
4. understand if risk information informs strategy (including scenario analysis) as well as informing assurance activities;

5. challenge whether it is clear 'who does what' on risk at the executive, board and audit committee levels;
6. determine whether risk and assurance teams have the authority and skills to drive the necessary change.

One thing that is clear from the recent developments is that risk management is a more prominent issue on the board and external stakeholder agendas. This is driving the need to refocus efforts and define what the future model for risk management should look like and the practical steps required to improve organizations' ability to assess and manage risk more effectively.

To achieve this future model, organizations should be developing a culture that can address risk at all levels. Such a culture effectively requires all employees to become risk aware. For an appropriate culture to be fostered, however, it is vital that senior management provide proactive sponsorship and demonstrable support. To achieve this, risk management must now be viewed as a strategic imperative.

1.3

Scenario-building techniques for improved risk management

Richard Pike, CCH, a Wolters Kluwer business

The practice and theory of risk management have taken a battering over the last number of years. Between scandals of corporate malfeasance and financial meltdown it has become clear that a reliance on mathematical modelling and laissez-faire regulation is not a good recipe for mitigating the real risks that face business in our global economy. There are many good reasons for these risk management failures, and they have been written about in detail in many other publications. However, there seems to be a common thread running across these reasons, and that is one of incorrect assumptions. These failed assumptions result in a breakdown in the business model owing to some factor that was almost impossible to foresee. This chapter aims to introduce readers to a process used in long-term planning that is proving useful in understanding these extreme tail risks and in assisting people to plan for and mitigate them.

All complex human thinking is based upon assumptions and models; we make an assumption, test its efficacy and, when it is proven, build on that with further assumptions and tests. The problem comes with situations where the models are so

complex that the original assumptions are lost or misunderstood. This results in the users of the models being blind to the underlying principles of their systems. This is, of course, an everyday situation; very few people truly understand all of the systems in a car but most of us happily trust our lives to them every day. This is because in most physical systems (and some very well-controlled human systems) it is possible to tightly control the variables and constantly retest the underlying assumptions. In more complex human systems that include sociological, cultural and psychological variables it is almost impossible to understand all of the variables, much less retest the assumptions. The recent sub-prime crisis saw Wall Street bankers assume that the information they were receiving on borrowers' ability to repay was correct. They had not taken into account the very real fact that mortgage brokers and mortgage holders were bending the truth for their own gain. Therefore these (and many more) basic assumptions underlying the complex mathematical models were found to be incorrect. One of the core new skills that risk management needs is a manner in which these possibly variable assumptions can be distilled from a model (mathematical, business or managerial) and tested both for variability and for their effect on the model outcomes.

Scenario building

There is an area of practice and associated research called scenario building, developed in the long-term planning arena, which is being increasingly used to find and play with these core assumptions. This process was first developed in a business context by Shell Corporation to assist with long-term planning and has since been researched and written upon widely within that context. As the process of defining long-term plans is as much about avoiding risk as it is about seeing opportunity, this process is now starting to be seen as a possible addition to the risk management field.

There are a number of schools of scenario building, and they differ on the actual manner in which a scenario-building exercise is undertaken. Here I will try to give a general overview of the process and how it might be utilized in a pure risk management framework.

Scenario-building projects can take anything from days to years, but most go through some standard phases.

1. Scope agreement

It is vital that the scope of the scenario-building exercise is agreed and understood by all participants and the final customer of the project. The elements that should be agreed include:

- *Timescales.* As scenario building is predicated on stressing certain variables it is important to understand the time period into the future that the scenarios will involve. Certain variables will have a very quick effect on the underlying model, and others will encourage very slow change. For example, the volatility of the

stock market quickly affects option prices on that market, whereas the change in oil prices takes a while to affect the oil exploration process.

- *The boundaries of the model in question.* For some scenario projects this will be an easy task, as they are well defined in systems like mathematical models or engineering systems. In others this will be a very difficult but even more vital task.

2. Model understanding

The second phase is one of familiarizing all participants with the model under review. This model may be a business model, a mathematical model or a complex social system. It is important that all of the people involved have a basic understanding of the model to be reviewed but is not vital that they are all experts in the field, and it actually helps when there are some novices in the team. One key area of concern here is that members of the team have a different view of the model and that a lot of time is wasted finding the areas where people disagree on the basic model even before they have commenced the project. In the more complex systems, this will always be the case to some degree, and actually the entire scenario process will help to coalesce these various views, but at least a basic agreement on the model at hand is a requirement.

3. Discover variables

A key and difficult phase of the project is to identify many of the main variables that affect the model in some manner. In a mathematical model this will be a fairly simple exercise, but in a more diffuse model (eg business, social) it may be very long, drawn out and complicated. In order to help, the variables should be broken into three types (see Figure 1.3.1):

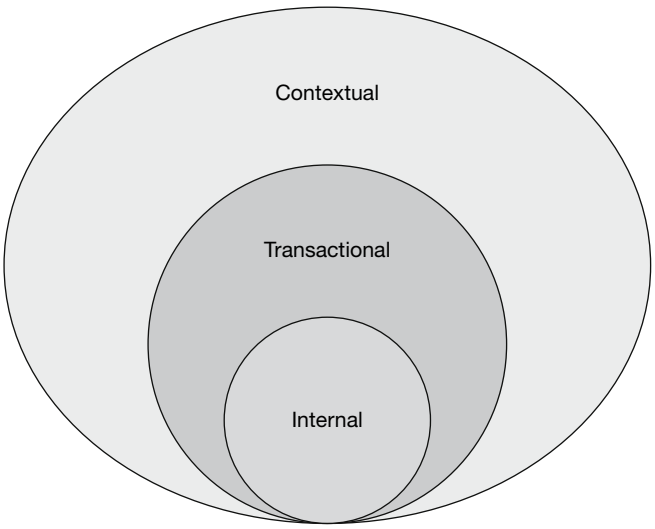


Figure 1.3.1 Variable types

- *internal:* those variables that are within total control of the model, eg percentage of funds invested in R&D;
- *transactional:* the variables that are key actors on the model but are not within total control of the model, eg the maximum price customers are willing to pay for the product;
- *contextual:* variables that affect the model but are in the surrounding environment and in no way controlled by the model, eg the price of oil.

The variables that the project is interested in finding are those contextual ones that have a large effect on the model. These are the variables, illustrated in Figure 1.3.1, that, if there are basic assumptions made about their stability, have the capability to completely undermine the model.

4. Score contextual variables

Once the above-mentioned variables have been identified (this may be an iterative process, as it is impossible to say that you have found all of the contextual variables in a system), these variables must be scored as to their importance or impact on the model outcomes and the ignorance or uncertainty as to their workings or future directions, as in Figure 1.3.2.

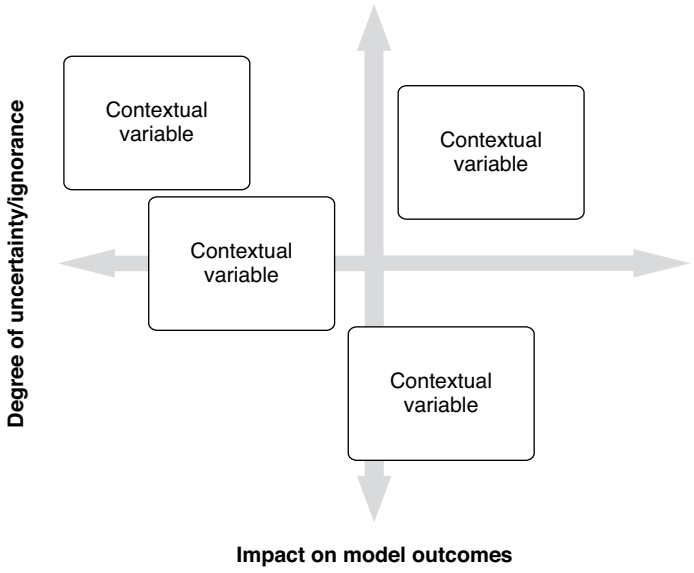


Figure 1.3.2 Contextual scoring matrix

This is a key phase, as it is when scenario builders will try to ascertain which contextual variables have the most impact on the model at hand. This is the most challenging part of the process, as it is here that underlying assumptions are torn apart and reviewed. Within this phase it is vital that deep and lengthy conversation

takes place between all of the participants to ensure that all possible views of the variable are taken into consideration. It is also in this phase that the importance of people from outside the world of the model shows up, as they will not be as set in their presumptions and world view. When the variables with the main impact are found, the process of deciding which variables are least well understood takes place. The basis for this scoring should be the understanding of the variable within the user of the model, not general understanding. For example, if the team finds that the price of oil has a major effect on the long-term outcomes of the model, but the model users have no real understanding of how the price of oil moves, it gets a high score, even though there are lots of people in the world who deeply understand the variability of the oil price.

5. Scenario creation

This phase involves taking the relevant variables, scored as having a great impact on model outcomes and least understood by model users, and creating future worlds where those variables have been stressed to extremes. For example, if the team has found that the price of oil and the importance of the US dollar as the world's reserve currency are the two most importance but least understood contextual variables, then your possible scenarios might look like those in Figure 1.3.3.

6. Scenario plausibility

This phase is undertaken to ensure that the scenarios the team has created in the previous phase are indeed possible. For each scenario a 'story' of how this situation comes about in the future should be created. This story can be derived with a number of tools, including systems thinking or inductive reasoning. The important result is a believable story of how the particular scenario might come about. If a story cannot be derived reasonably then the scenario should be excluded or at least de-emphasized within the project.

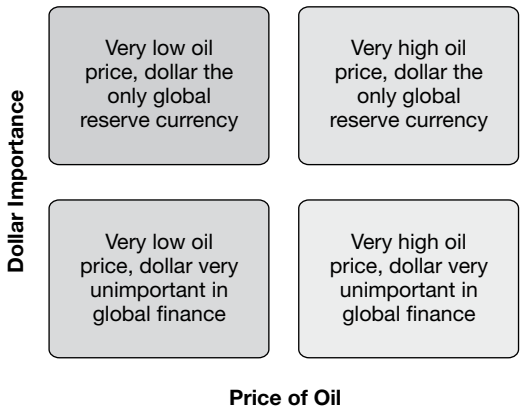


Figure 1.3.3 Example scenarios

7. Scenario description

The final phase of the project is to examine what the world looks like in the case of each scenario. A detailed document should be drawn up in which the world surrounding the model is described in enough detail for users of the model not engaged with the scenario project to be able easily to understand it and its effects on their model. A short example follows for the scenario described in the top left of Figure 1.3.3: very low price of oil, dollar the only global reserve currency. 'In this world the dollar is the only real currency of global trade and finance. Most large trade deals are carried out in dollars, and all large bond and share issuance is dollar denominated. The price of oil is such that oil use has exploded, and outside of carbon production issues there are no brakes on oil usage throughout the world.'

The description of each scenario should be detailed enough so that users of the model in question can ascertain what the probable effect on the model outcomes will be under each scenario.

8. Scenario usage

These scenarios can be used in a multitude of ways (including strategic planning and model communication); however, it is their usage in risk management that interests us here. The variables derived in the process of defining the scenarios are in themselves very interesting to risk managers. These are variables that may not have been reviewed before and, therefore, may be added to the list of risk indicators. The variables that are scored as being high-impact can be reviewed for mitigation techniques including insurance. Where these techniques are not available, detailed analysis of the variable and its driving forces may be undertaken so that indicators of change can be put in place to forewarn risk managers of impending outcomes.

In general, however, it is the power of the scenario-building process itself that will assist risk managers. As stated at the beginning of this chapter, one of the core failures of modern risk management is its inability to understand the base assumptions underlying systems and models. The scenario-building process was derived to better understand these assumptions and drive out new thinking about the possible future worlds where these variables have changed.

Many modern institutions utilize scenario building to better understand the future, including Shell plc, the Global Economic Forum and the Singapore government. Some of these have operationalized the process of scenario creation and review so that it is now a core process within senior management. Those that have done so have now realized that scenarios have a very important role within their risk management practices and will track indicators linked to scenarios on a monthly basis.

The tool of scenario building is one that complements the other tools in the risk manager's bag, including impact and frequency modelling, incident recording, issue management, control testing and risk assessments, and should be part of any modern enterprise risk management framework.

1.4

Standardizing risk management – business enabler or the risk manager's straitjacket?

Allan Gifford, Strategic Risk Consulting Practice, HSBC Insurance Brokers Ltd

Today's business environment has meant that risk management has risen up the board agenda as companies realize that their ability to manage risk fundamentally impacts on their ability to operate successfully. It seems fateful then that the British Standards Institution (BSI) released BS 31100 for risk management at the end of 2008.

Ironically, the word 'standard' has a number of connotations. A standard specification is likely to be an explicit set of requirements for an item, system or service. It is used to formalize the technical aspects of a procurement agreement or contract. A standard practice or procedure will give a set of instructions for performing operations or functions. A standard guide might be general information or options, which might not necessarily require a specific course of action.

To further muddy the water, many risk management 'standards' referred to are often actually codes of practice, general guidance notes, or documented forms of recognized or perceived best practice.

According to the BSI:

> Standards are written guidelines which help to do things, or make things, more efficiently or more safely. They are written through a formal prescribed process which involves consultation with relevant bodies and reaching consensus across all interested parties so that the final document meets the needs of business and society. All standards take the form of either: specifications, methods, vocabularies, codes of practice or guides.

So to risk management; is it a business discipline worthy of, or in need of, standardization?

BSI's Code of Practice for Risk Management, BS 31100

Over an average year, BSI undertakes 45,000 company audits, ranging from quality and health and safety to information security. When the assessors visit companies for whatever reason they look out for some indicative markers that contribute to an overall impression of that organization. The approach to risk – or the lack of it – is a pretty obvious one. Anecdotal opinion is that most organizations, irrespective of size or market, need a greater understanding of the broader risks they face. Some record or treat 'point' risks such as business continuity or financial risks, and manage or insure against those. However, of those organizations that understand their risks, fewer treat risk as a business-wide issue.

The process presented in the new BS 31100 puts forward a business-wide model from identifying risks to treating them, one that can be used in large organizations or small ones. Although every business is different, the core requirements of understanding risk are the same for all. By being a national code of practice, BS 31100 is available and applicable to all organizations regardless of size and sector, and no formal membership to any particular professional body is required, therefore providing independence. In terms of an organization demonstrating its own risk management maturity, the ability to compare to the code published by the BSI provides a credible 'brand' behind the declaration. This can only help in the dealings with various stakeholders.

Riskier business environment?

Few can doubt that we are currently living through the most testing set of business challenges that we will experience in our professional careers. In the last 18 months we have seen a confident and ambitious business environment slump into recession and have been forced to review the basic assumptions that we make about our market as household names such as Woolworths, General Motors, AIG, Royal

Bank of Scotland and HBOS have disappeared into bankruptcy or required bail-out from public funds.[1] So is it not the case that attributes like 'framework', 'formality', 'adherence', 'compliance' and so on will help provide an environment that gives the best chance of business success?

Yet we also intuitively understand that it is sometimes the risk takers, or those who respond more quickly, or the entrepreneurs, who can build successful businesses. We have read recently about pizza delivery firms whose fortunes have changed as people dine out less often, acquirers who buy up insolvent companies (and therefore their customer bases, products or intellectual property) at bargain prices, and the banks that passed up on government offers of a capital injection (in exchange for shares) and are now faring relatively well as compared to their more constrained government-owned competitors.

So does competitive advantage come from doing things in a consistent, agreed and structured manner or from allowing people the freedom and flexibility to act on instinct, free of bureaucracy?

Of course, we know the answer. Both, and neither.

Help or hinder?

In order for us to consider the efficacy of risk management standards, let us refer to a few. The last decade has seen the publication of a plethora of codes, standards and other authoritative guides.

In 2002 the Institute of Risk Management (IRM), Association of Insurance and Risk Managers (AIRMIC) and Public Risk Management Association (ALARM) worked together to produce 'A Risk Management Standard'. The standard notes:

> Risk management is a rapidly developing discipline and there are many and varied views and descriptions of what risk management involves, how it should be conducted and what it is for. Some form of standard is needed to ensure that there is an agreed:
>
> - terminology related to the words used;
> - process by which risk management can be carried out;
> - organization structure for risk management;
> - objective for risk management.

The standard recognizes that there are many ways of achieving the objectives of risk management and it would be impossible to try to set them all out in a single document. Therefore, it was not intended to produce a prescriptive standard, which would have led to a box-ticking approach, nor to establish a certifiable process. By meeting the various component parts of this standard, albeit in different ways, organizations will be in a position to report that they are compliant. The standard notes that it 'represents best practice against which organisations can measure themselves'.

HM Treasury's 2004 *Orange Book: Management of risk – principles and concepts* clearly positions itself as providing 'broad based general guidance on the

principles of risk management'. It acknowledges that, since the publication of the first *Orange Book* in 2001, the challenge addressed in the 2004 update is one of ongoing review and improvement of risk management, accepting that most government organizations now have basic risk management processes in place.

Also in 2004 the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published its *Enterprise Risk Management – Integrated Framework*, an enterprise risk management (ERM) follow-up to the internal control framework it published over a decade before. The ERM framework expands on and incorporates internal control, providing a broader approach for identifying, assessing and managing enterprise-wide risk management.

In 2006 there was a review of the Turnbull guidance notes for directors on the internal control requirements of the Combined Code of the London Stock Exchange. The revised guidance reinforces the board's responsibility for risk management, including ongoing review and the extent to which it is embedded.

A reassuring factor in the development of risk management standards is the inclusive and consultative manner in which they are developed. They are almost all developed as the result of work done by a team drawn from the lead organization, and incorporating the views and opinions of a wide range of other professional bodies and industry sector practitioners with interests in risk management. Therefore we can rely on their scope, practicality and applicability to today's businesses. The same approach to involvement applies, incidentally, to the development of BS 31100.

Let us remember, too, that risk management is an important discipline in all streams of business and sectors. A key function for the NHS Litigation Authority (NHSLA), as set out in its Framework Document, is to 'contribute to the incentives for reducing the number of negligent or preventable incidents'. The NHSLA aims to achieve this through an extensive risk management programme, which comprises a range of standards and assessments.

One of the perpetual challenges in the world of risk management is one of definition. There are differing labels given to it (eg enterprise[-wide] risk management, business risk management, operational risk, etc); there are numerous statements and descriptions of what it is (this chapter cannot begin to list them, but a simple internet search will illustrate this point); and there is a fuzzy line between whether, when risk management is embedded, it is actually risk management or simply good, general, business management. After all, business leaders manage risk every day as they go about their work.

What is common across all these publications is the recommendation for framework, structure, common language, the provision of tools and techniques, appropriateness and so on.

Some observers note that, given the numerous individual standards that already exist for specific tasks or activities (to note a few: ISO 14001, BS 25999, OHSAS 18001, ISO 9001, PAS 99, ISO 27001, BS 25777, ISO 22000 and so on), the role of risk management is the oversight, coordination and achievement of them, which should help companies meet their organizational objectives.

Do these 'standards' restrain risk management or enable it?

A framework by which this is all managed is useful for consistency of terminology, targeted deployment of resource and smooth implementation. By their very nature, existing risk management 'standards' are general in their outlook and scope. They suggest methods, tools and techniques. They provide guidance and recommendations. They cannot prescribe activity, as they are written to apply to organizations regardless of turnover, sector or ownership. Therefore they generally accept that their execution and implementation are open to interpretation, as they must be appropriate to the organization.

However, these standards often miss making explicit links with the specific contribution of other related standards, specifications or processes, such as modelling, financial products or the use of management information systems for reporting. Activities such as these add to the various stages of the risk management journey, whether that is risk identification, assessment, treatment or monitoring. The role of such activities might be referred to in the various standards; however, the absence of clear links can only dilute the thoroughness of the standard and therefore limit its effectiveness and perceived value. A standard often states the need for such activity but gives little direct assistance towards how to do it. To some professionals, the standard then only presents part of the story and, as such, constrains risk managers or, at worst, disengages them from the concept of following a standard at all.

Supporting the risk manager

So let us consider the risk manager, and the role of standards within the context of his or her job. Let's assume that risk managers operate at varying levels, as influenced by their experience or personal bias, or the culture and expectations of their employer. A risk manager might, generally, adopt any of the positions identified in Table 1.4.1.

Table 1.4.1 Risk management positions

Level	*Typical activities*
Traditional risk management	Risk identification, claims management, insurance and risk transfer.
Advancing risk management	As above, plus perhaps business continuity and crisis management, and some alternative risk financing, recognized as the internal 'risk champion'.
Enterprise-wide risk management	As above, including the application of technology, risk modelling and scenario planning.

Newspaper stories, anecdotal evidence and experience of working with many companies of varying size lead us to conclude that company size is not a determining factor when assessing the nature of the engagement of the risk manager. Therefore a standard for risk management is as useful to an organization with a turnover of £20 million as it is to one of £200 million or £2 billion.

There is, of course, little substitute for experience, and most risk managers with, say, 10 or more years of experience may well wonder what all the fuss is about when they read any new or existing standard. After all, risk management… is risk management… is risk management; surely there aren't any new or different angles to be created? Perhaps standards take away, dilute and maybe even disrespect the skill, knowledge and creativity that are inherent in the risk manager who has the war stories.

Doesn't a prescribed standard make it as easy as taking the manual off the shelf? This way a new hire can do the job as effectively as the experienced practitioner. If standards lead to defined ways of doing things then it almost becomes a checklist approach and might devalue the role, maybe even lessening its (already limited) boardroom airtime.

However, today's professional risk managers know that risk management is a complex subject requiring the ability to think and act broadly while also retaining the capacity to dive into the detail. They know that if they are still to be in their position in the future they will need to improve continually if they are to serve the needs of their business and have a regular voice in their boardroom. It is here that they secure the support and sponsorship for risk management improvement and investment, and being able to align their company against a standard is an excellent way of showing where the gaps are and internally selling what needs to be done.

Most companies will agree that risk management is an important aspect of their business success. Most senior management teams will agree that they understand the risks facing their company. So how, then, do they decide what structure or framework to adopt? Standards provide that answer, as long as they allow for interpretation in a manner that best suits the organization. Standards also recommend regular review of both the risk management 'system' and the risks, thus avoiding complacency or a framework that becomes out of date after organizational or industry changes.

However, standards will have more to offer those risk managers who operate at the 'traditional' level, as they will be a tool that will direct traditional managers in how to raise their risk management game. These risk managers, while having most to gain, will also believe they have most to fear in the form of increasing accountability, taking their day job into unfamiliar territory, or pure workload.

But, if standards bring framework and structure, they will produce transparency, accountability and empowerment, and ultimately produce better decisions.

The outside world

Risk management is often considered a 'given' by external stakeholders such as investors, major customers, banks and so on. There is little evidence to suggest that

investors, for example, specifically look for adherence to specified risk management standards (the exception being the world of financial services, where compliance against the risk management aspects of Basel II, and soon Solvency II, is, and will be, directly assessed).

However, there is an increasing level of attention being paid to 'corporate risk management', demonstrated by the growing interest that rating agencies are paying to it. There is also evidence that insurers and banks are taking an increased interest in how well their customers can manage their risks. While it might not be top of decision making for investors, these bodies recognize the importance and role of risk management for company performance, and that alignment with a standard provides a major opportunity to enhance communication with stakeholders and bring credibility to systems in which they manage risk.

Conclusions

The many individual standards, assessments and codes of practice collectively form the overarching modus operandi of today's professional risk manager. There are various standards to choose from, with orientations according to the professional body from which they originated and the sector they serve. They do indeed provide framework and structure, set the rules and acceptable norms, and provide the assurance of risk management maturity to those stakeholders who need to know or care.

However, they should not restrict risk managers in carrying out their daily, monthly, quarterly, annual and ongoing role. Successful organizations will employ risk managers (or whoever adopts that role) who act promptly in the present, learn from the past while looking to the future, and provide the insight and direction into risk management. So standards need to protect us from harm but not restrain our freedom, flexibility and responsiveness. This will be the best combination to avoid downside, enable upside, and contribute to success.

The new BS 31100 provides a timely opportunity for businesses to introduce an approach that best fits their purposes, and seek commercial and competitive advantage from its implementation, while leveraging the strength of the BSI brand when communicating adherence to stakeholders.

The risk that the standards themselves run is the potential lack of completeness. While they regularly refer to the need for further specific tasks, such as modelling or the execution of financial products, they can often fall short in making explicit links to other specifications or providing specific advice. As a result some standards are occasionally accused of being vague, woolly or too high-level.

This said, a professional risk manager with full support of the board and good internal and external advice can successfully implement risk management against the many standards available. Not only will this position the organization well operationally and in the eyes of its stakeholders, but it is also likely to enhance the standing of the risk manager.

Therefore, the risk manager can avoid the straitjacket of rigidity and bureaucracy that the word 'standard' implies, and instead use the framework of structure,

tools and techniques that today's risk management standards provide to play his or her part in enabling business success.

The views expressed in this chapter are the author's personal views and do not necessarily represent the views of the HSBC Group.

Note

1. David Breden, 'Managing risk in turbulent times', Unpublished paper.

1.5

Corporate responsibility – a risk management tool

Pauline Hylton, Lloyd's Register Quality Assurance (LRQA)

Background

It's fair to say that the single greatest risk to any business is the loss of trust and credibility in the eyes of critical stakeholders. The difficulty for executives, however, is that this risk is both highly complex and highly dynamic. Trust simply cannot be managed in rule books, spreadsheets and IT systems. It requires direct and constant engagement with a wide range of stakeholders whose needs are constantly changing, and it requires concerted commitment and vigilance by the entire organization. Trust can be broken on the front line or in middle management, just as easily as in the boardroom. Wherever trust breaks down, the consequences can be devastating.

When it comes to addressing these complex risks, there is no simple recipe. Each stakeholder's needs must be considered individually. For shareholders, trust may be a function of governance or the clarity of board communication. For customers, it may arise from product quality, provenance or innovation. For employees, consistency in remuneration may be the driver, or the honouring of pension commitments. For suppliers, trust may depend upon fairness in procure-

ment or the prompt settlement of invoices. For every critical factor that drives goodwill and competitive advantage, there is an equivalent risk of failure. Fail in your environmental duties and you don't just pay a fine or run a legal risk. Your product brands and your corporate reputation are imperilled too.

Once your organization has understood the corporate risks as stakeholders see them, it must balance these against the priorities of the business. It must then design appropriate and proportionate strategies to address these 'material' risks. Corporate standards must be defined and upheld through comprehensive management systems. Then, and only then, should the organization's attention turn to monitoring these systems, and finally to reporting on these systems as a means of providing accountability and driving continual improvement. Too many organizations still work the other way around. The result of this topsy-turvy approach is unverified reports consisting of partial, potentially misleading data about meaningless issues. Despite the best intentions of their advocates, these token reporting approaches never succeed in driving corporate performance. Divorced from real risks, corporate responsibility (CR) reports provide little or no assurance, either to stakeholders or to management.

By contrast, properly executed CR offers an organization a truly unique lens on its strategic and operational priorities – the chance to examine its performance through the eyes of the outside world. Effective CR can remove the guesswork from corporate risk management by injecting insights directly into the operations of the business and ensure genuine sustainability.

According to figures published on CorporateRegister.com, 75 per cent of the global top 500 companies (up from 67 per cent in 2005) now produce some sort of CR report. Even businesses that do not currently produce a CR report often describe their impact on the environment within their annual reports, recognizing the risk associated with environmental complacency. Today, 70 per cent of CR reports are unverified. It is hard to resist the conclusion that many would simply not stand up to scrutiny.

Organizations that duck out of the cycle of report assurance are also missing the wider benefits that come from adopting a systematic approach to exposing stakeholder risk and extracting real operational lessons from the data. More often than not the production of a CR report surfaces waste, inefficiency and inconsistency, which can drop straight to the bottom line. The process by which a CR strategy is developed should serve to establish targets for continuous improvement, potentially in every area of a business, and generate clear plans of action to get there.

A number of recent high-profile business scandals have resulted in enormous damage to companies and brands. The failure of these organizations to recognize and respond responsibly to the kinds of risks associated with inappropriate corporate behaviour has changed stakeholder attitudes towards them; businesses can no longer expect stakeholders automatically to trust them – they have to prove trustworthiness.

It remains a major concern that CR reports have often been created solely for PR and marketing purposes, rather than providing accountability for the triple bottom line – people, planet and profit. The Global Reporting Initiative (GRI) has estab-

lished a framework that sets out the principles and indicators that organizations can use to measure and report their economic, environmental and social performance.

The GRI believes that the lack of transparency in the existing system multiplies risk. During the G20 meeting in London in April 2009 it called upon all governments to extend and strengthen the global regime of sustainability reporting. In particular, the GRI believes that assumptions about the adequacy of the current voluntary reporting must be re-examined. It has argued that the root causes of the current economic crisis would have been moderated by a global transparency and accountability system based on the exercise of due diligence and the public reporting of environmental, social and governance performance. Trillions of dollars of risk were compounded by a lack of effective mechanisms for stakeholder scrutiny. The GRI also believes that the profound loss of trust in key institutions is best addressed by the adoption of a global reporting framework that enhances transparency and is informed by the legitimate interest of all key sectors of society.

LRQA's own approach to CR assurance is based not just on the quality and accuracy of reporting data, but on the meaningfulness of the data to stakeholders. We work to assess the rigour with which the programmes have been created and the effectiveness with which they have been delivered:

- Have the stakeholders been mapped and contacted in some way to encourage open and honest dialogue?
- Have their needs been fully identified, prioritized and addressed?
- Has there been a verifiable assessment of all business risks?
- Has there been an honest assessment of the current position?
- Have realistic, measurable targets for improvement been established?
- In other words, is the CR delivering against the material risks to the business – as perceived by stakeholders?

In considering the robustness of a company's activities our key assurance principles are materiality, accuracy, completeness and transparency.

With corporate reputations at an all-time low, businesses need to focus on rebuilding trust in order to survive the economic downturn. The way in which an organization measures, monitors and communicates on issues such as safety, ethics and the environment provides an important opportunity to reconnect with stakeholders, demonstrating commitment through genuine actions. In the current climate of mistrust, stated intentions, goals and accomplishments are all in danger of being regarded as 'greenwash' unless organizations can prove them through independent, third-party channels.

What transparency means

Corporate transparency is not achieved through advertisements, glossy brochures, company websites, press releases and so on. Rather, transparency, in this context, is about understanding stakeholder (customers, shareholders, staff, supply chain, community) concerns and ensuring that relevant data that prove actual actions and

performance are communicated in a timely and independently verified manner. Transparent disclosure implies an honest willingness to disclose all data, good and bad, even when such information could reflect poorly on the organization. Done properly, this can help develop a two-way communication between organizations and their stakeholders, resulting in increases in both consumer trust and brand reputation. Further, stakeholder groups, both internal and external, are increasingly seen as an independent, trusted voice regarding the activities of an organization. Online corporate watchdogs are viewed as a trusted source of opinion and information regarding corporate behaviour.

What consumers are saying

A new research report, 'What assures consumers in an economic downturn', from AccountAbility investigates what enables consumers to trust in a business's integrity and fairness during difficult times. The report is the fifth in the 'What assures?' series of research-based reports, which explore and advance innovative approaches to building credible assurance. The research, based on a survey of 2,000 UK consumers, indicates that they no longer trust organizations that traditionally could have taken such trust for granted. Instead, they are placing trust in organizations that either are regarded as impartial or are able to provide third-party independent assurance to support their ethical or green claims.

High levels of cynicism and mistrust were revealed in both business and government. Conversely, consumer watchdogs enjoy a high level of trust, and the research indicates that a real window of opportunity exists for businesses that can provide independent assurance to rebuild consumer trust by demonstrating transparency and accountability in areas such as ethics and social and environmental responsibility.

The research highlights an 'accountability gap' – the gulf between responsibility to act and capability to deliver – which poses a huge problem as the recession tightens its grip. Alex MacGillivray of AccountAbility says, 'Consumers are sticking to their ethics (the Co-operative reported a 44 per cent growth in the sale of Fairtrade products in 2008) but feel let down and businesses are desperate for new ways to rebuild trust. Government sees the need for game changing policies, but rebuilding assurance is the missing piece of the recovery plans.' Helen McTaggart, ethics adviser at the Co-operative, believes:

> There is a prevailing mood in the media at the moment, and it's a bit of a myth to be honest, that there's a sort of universal flight away from values towards value, but at the Co-operative we believe that this simply isn't true. It's not borne out in sales data and it's not borne out in research such as 'What assures consumers'. Therefore we urge all businesses to stick by responsible business practices and to keep working with non-government organizations [NGOs] and third-party accreditations, because, come the upturn, consumers will think particularly badly of those businesses who have been seen to shy away from responsibility as soon as times get hard.

Where to start

An international standard, ISO 26000, providing guidelines for social responsibility, is currently under development. This standard offers useful guidance on socially responsible behaviour and possible actions; it does not contain requirements and, therefore, in contrast to ISO management system standards, is not certifiable. However, the standard AA 1000AS is used by professional assurance organizations such as LRQA to provide independent third-party verification of the data, information and related processes within a CR programme.

The GRI framework mentioned above can also be employed in the development of a CR programme.

Transparency needs to be embedded in the culture of an organization in order for the CR programme to be successful. Only when stakeholder concerns are proactively a part of the strategic decision-making process can organizations begin to win back consumer and stakeholder trust.

The key for organizations is to establish a performance baseline and to acknowledge past failings whilst clearly demonstrating an understanding of what needs to be done to correct those errors, including a clear plan (which again includes measuring and monitoring elements) that provides stakeholders with assurance that what is being said is also being done. Alan Knight, from the think-tank AccountAbility, says, 'Research clearly indicates that the companies which do admit to shortcomings and then explain how they've addressed those shortcomings benefit from improved performance and are rewarded in the marketplace.'

Understanding stakeholder needs

In order to create an effective CR programme that addresses a business's specific risks, it is vitally important to have a clear understanding of stakeholder needs.

According to Matt Christensen, Executive Director of the European Social Investment Forum, financial reporting captures less than 20 per cent of corporate risks and value-creation potential, with the other 80 per cent deriving from intangibles such as human capital and resource efficiency. This is where the CR report becomes a crucial tool to help potential investors to better gauge longer-term risks.

One of the most important means by which an effective CR programme can reduce risk is stakeholder engagement to better understand customer needs. A clear understanding of changing customer demands will enable organizations to adapt accordingly. Consumers increasingly expect their suppliers to 'choice-edit' products for them and to make purchasing decisions on their behalf, for example by providing ethically and environmentally acceptable goods, such as Fairtrade products or energy-efficient lighting and electrical items.

Dialogue with customers about their requirements on ethical and environmental issues can extend to cover the specific features and benefits of products or services. This delivers vital data to inform product development and marketing activities.

Once stakeholder needs have been established, businesses need to have systems in place that are focused on meeting or exceeding those expectations, and they need to be able to demonstrate genuine measurable targets and actions to achieve the objectives. For example, if the target is to reduce greenhouse gas emissions (GHG), the starting point has to be a clear communication of the current verified level of emissions, as well as a defined, transparent plan, including timelines, on how the reductions will be accomplished. Audit, data verification and assurance against a relevant global, regional or national standard or scheme provide further proof that an organization is treating the process as more than a PR exercise. Engaging employees and suppliers in the process, from both an information and a participation standpoint, will help ensure engagement on every step of the journey.

To benefit fully from the transparent disclosure of GHG data, organizations will need to have their carbon emissions independently verified. This provides confidence in the robustness of the organization's systems, proves that the data-gathering methodology is accurate and inspires trust in the recipients of the data. In other words, it is not enough to say it; it's not even enough to do it; you now have to prove it!

In the current economic climate, businesses are focused on short-term cost reduction and revenue protection. However, just as there was a 'flight to quality' in the early 1990s, as evidenced by a sharp increase in ISO 9001 quality management systems certification, we are now seeing a similar move towards certification and assurance services, with the addition of health and safety and environmental management systems. Companies are looking to differentiate themselves from their competition and have identified compliance with international standards as offering a competitive advantage in the marketplace.

Now that CR activities have become mainstream, those companies that have taken the lead are starting to uncover benefits beyond the competitive advantage that is provided by compliance with standards. For example, the implementation and certification of an environmental management system (EMS) across an organization's supply chain will, in most cases, lead to a reduction in waste and CO_2 emissions. This translates into less energy use and significant cost savings, often well beyond the cost of setting up and certifying the EMS.

In 2008, Atlas Copco's revenues increased in volume by 17 per cent (including acquisitions). However, through efficiency improvements and a greater focus on environmental issues enhanced by ISO 14001, the use of many natural resources has increased at a lower rate. For example, in absolute figures, energy use increased by just 2 per cent, water use by 3 per cent and CO_2 emissions from energy by 3 per cent.

From a risk reduction perspective, it is important for businesses to remember that CR is built on three pillars: economics, environment and social issues. In order to achieve optimal risk reduction and derive maximum benefit, all three issues should be considered together rather than in isolation.

Internal and external stakeholder engagement initiatives

Many excellent examples of internal and external stakeholder engagement exist. Planet Me, for example, is a three-pronged approach to radically reducing TNT's CO_2 emissions. It comprises:

1. Count Carbon – a commitment to transparent reports on carbon footprint;
2. Code Orange – a comprehensive programme for reducing CO_2 emissions from daily operations;
3. Choose Orange – a means for encouraging TNT employees to undertake personal environmental initiatives.

Similarly, Go Green at Kellogg's aims to inspire and motivate people to behave in an environmentally friendly way at work, at home and in the surrounding communities.

Increasingly, companies such as BT are assessing their suppliers in terms of their corporate responsibility activity. Suppliers that are able to provide independent verification of their environmental and sustainability claims will lead the list of preferred suppliers. Those suppliers that are unable to provide proof of their environmental performance will, over time, find it increasingly difficult to tender for work with large organizations.

What are the pitfalls?

A company that produces a 40-page glossy document extolling nothing but virtue is likely to invite cynicism. The first step therefore is to start making improvements internally and to ensure that your employees are with you. Green communications specialist Solitaire Townsend believes: 'The best, most productive, safest and most ethical place to start is to talk to your staff because if your staff don't believe (in your CR policy, for example) then they are going to undermine you every step of the way.'

It is vitally important for a CR programme to address all risks and not just reputational risk. So supply chain risk should be assessed, not just to assess the risks associated with potential delivery interruptions or cost rises but also to assess the supply chain from a social and ethical perspective. For example, several international brands have suffered from revelations relating to child labour and unfair trading within their supply chains.

What are the benefits?

Reductions in waste, energy consumption and emissions help the environment, but can also deliver substantial cost savings and help an organization to comply with health, safety and environmental regulations. An effective CR programme can

therefore improve competitiveness and reduce the risk of sudden damage to your reputation and revenues. Major financial institutions, private equity firms and other investors recognize this, and research from the Institute of Business Ethics shows that companies with an ethics policy are more likely to be commercially successful in the long run and therefore more trustworthy and attractive in their respective business environments.

Proof of good corporate behaviour can be very beneficial to brands, and a good reputation makes it easier to recruit employees, whilst existing employees stay longer, reducing the costs and disruption of recruitment and retraining. Employees are also better motivated and more productive.

In its latest CSR report, 'How we do business', Marks and Spencer says its Plan A project (to work with customers and suppliers to combat climate change, reduce waste, safeguard natural resources, trade ethically and build a healthier nation) has reduced some of its energy usage and landfill waste and that Plan A became cost-positive at the end of its 2008–09 business year. The following is an extract from the M&S Annual Report 2009:

> We are not put off by the short-term impact of the recession. We set ourselves 100 rigorous commitments as part of Plan A, and have achieved 39 with 24 of them now going even further. In addition to being the right thing to do, these commitments are generating cost savings across the business that we can invest back into our prices.

Summary

The publication of a CR report does not in itself reduce business risk. In fact it may increase risk levels by exposing a business to allegations of window-dressing, greenwash and hypocrisy. It is vitally important, therefore, that there is real substance to the plan, because the development of a transparent programme of corporate responsibility initiatives that stands up to external scrutiny, meets the needs of stakeholders and demonstrates that the business is fully accountable for its actions can help to create a leaner, greener, more efficient, financially secure, lower-risk business.

1.6

Political risk

Corene Crossin and James Smither, Control Risks

- Investors should take an active rather than passive approach to addressing political risks, moving beyond a narrow conception that insurance of certain named risk categories is their only viable management tool.
- A broad and nuanced step-by-step process is needed to understand the various stakeholders and agendas that can and do interplay to create a wide range of project-specific 'political risks'.
- This is a critical prerequisite to identifying areas of common interest between stakeholders and the project that can be leveraged to maximize the investment's success prospects in the market.
- A truly effective political risk management strategy will also need to be fully integrated with other aspects of the business's management approach, including its community relations and corporate social responsibility agenda, its public affairs strategy, its security function, and its legal and human resources teams.

Traditionally, investors in foreign markets (and particularly emerging markets) have viewed political risk as emanating from adverse decisions taken by a national host government. However, this narrow view overlooks the multifaceted, multi-layered nature of political risk and in particular fails to recognize the importance of sub-sovereign-level political issues for investments.

Political risk management seeks to reduce the likelihood and impact of politically motivated events on an investment. A 'good' international investment should therefore incorporate a form of political risk management that takes into account the complexity of political risk and the ways in which the investment itself can affect and influence the political risks to which it may be subject, and adopts an accordingly nuanced approach to the management of such risks.

This chapter provides an outline of the key steps involved in a best-practice political risk management programme, as summarized in Figure 1.6.1.

Step 1: evaluate the threat context

A critical first step in managing an investment's political risks effectively is to gain as full a picture as possible of the threat environment within which the project will be operating.

Too often, the insurance industry – which sometimes misleadingly describes itself as 'risk management' – narrowly drives an organization's view of its political risks. Risk classes defined in advance by underwriters – expropriation, strikes, riots and civil commotion (SRCC), non-payment – dominate considerations of the events that may be confronted. The exclusion-crammed policies to transfer the liability created by such an event offered by those same underwriters in turn dictate the corporate response. This is both an incomplete and a short-term approach: risk conditions in a market can change rapidly and can often manifest themselves at a non-sovereign level where policy coverage may not apply.

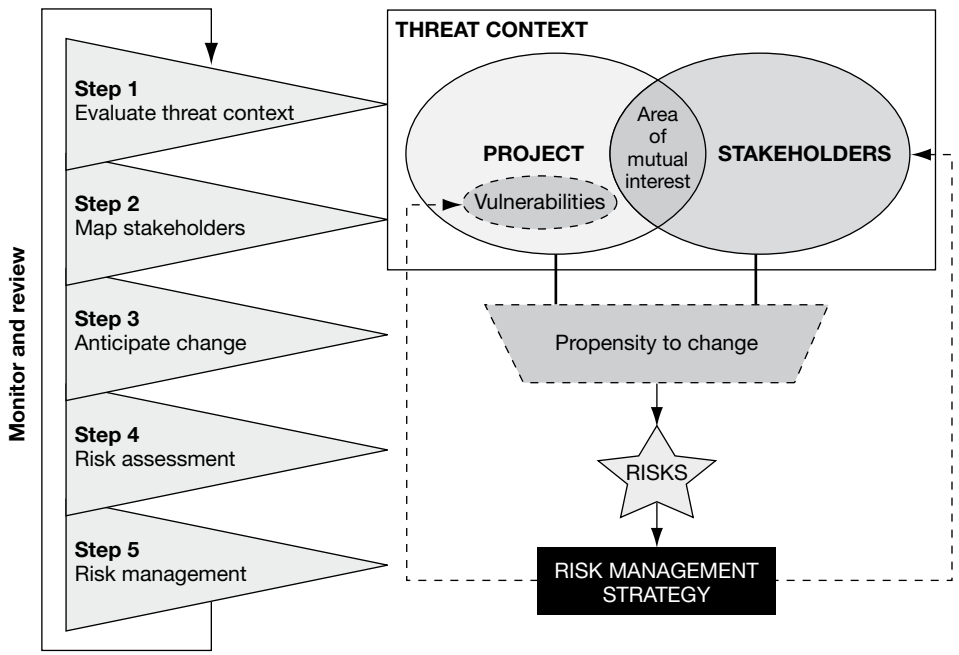


Figure 1.6.1 Stages and aspects of political risk management

A broader definition of political risk is one that evaluates the likelihood of a variety of state or non-state political actors negatively affecting business operations in a country through regime instability or direct and indirect interference. State actors can include domestic (central and local) as well as foreign governments, parliament, the judiciary and the security forces. Non-state actors can include insurgent groups, secessionist movements, lobbies, other companies, organized criminal groups, and ethnic and indigenous groups in the project vicinity, as well as international organizations.

In taking this broader view, investors can begin to assess in a comprehensive way the specific political, economic, social and security threat environment they confront at a national, regional and local level. As part of this threat assessment process, it is crucial to consider how the full spectrum of political stakeholders (at every level) view the investment, for example their prior opinion of the industry sector where the investment is to be placed, local perceptions of the nationality of its owners and operators, and the precise physical footprint of its assets and supporting infrastructure on the ground.

Step 2: map stakeholders

This analysis of an investment, by an active party that can provoke rather than simply receive reactions from stakeholders in the wider political context, underlines the importance of undertaking as fully as possible an identification of the principal sources of political risk to the project, for example a political party, a rebel faction, an indigenous community or an individual bureaucrat, and the threats they pose to the investment.

Since the core of good political risk management is developing a plan to influence political stakeholders, the stakeholder identification process needs to be as comprehensive as possible and to recognize that different stakeholders can be providers of support as well as sources of risk to a project. Therefore, the next step is to identify and map stakeholders and understand how their objectives may affect the investment in positive and negative ways.

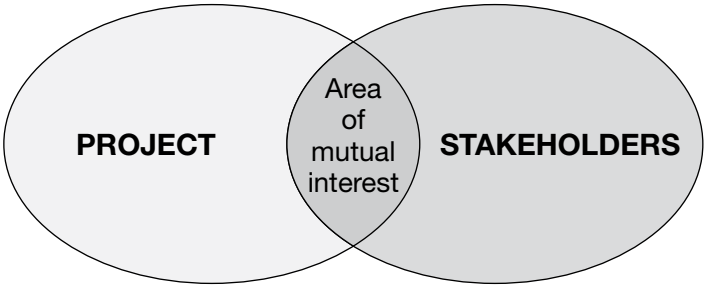


Figure 1.6.2 Identifying areas of overlap

Mapping stakeholders fully involves:

- identifying the full spectrum of political stakeholders that may have an interest in, or influence over, the investment: this can include international actors, as well as national and local players in the project country;
- conducting detailed research to identify each stakeholder's interests, motivations and position vis-à-vis the investment: these may not have emerged yet, or may be incoherent or contested;
- in each case, identifying areas where there is overlap between the aims and objectives of the investment and those of the stakeholders (see Figure 1.6.2).

Step 3: anticipate change

A critical further aspect of political risk assessment is the acknowledgement that things will rarely remain static, either in the host context and amongst the various stakeholders located there or in the actions and progress of the investment itself. Holistic political risk management therefore requires the development and constant updating of scenarios to identify how the current national and local political risk environment may change, and how these changes will interact with changes during the life of the investment itself, for example as it moves from a construction phase (where local employment requirements are traditionally highest) through an operational phase (when its physical and fiscal output will probably be most attractive) to its potential closure. These should include worst-case as well as best-case scenarios: unanticipated regime change, be it through coup, incapacitation or the ballot box, is a classic source of political risk, as the new leadership often seeks to renegotiate the business deals concluded by predecessor administrations on terms deemed more preferential to the host country and less exploitative of its inhabitants.

To understand this dynamic fully, the organization needs to audit the investment's own risk management structure and approach, and identify whether this is sufficiently well structured and implemented to effectively manage identified political threats. This involves the recognition that steps taken or not taken by a project, even if undertaken in good faith, can themselves create political risks – especially with local community stakeholders – and provide a perfect pretext for the imposition of other political risks by authorities with an already hostile agenda.

Step 4: risk assessment

A proper political risk assessment considers both the likelihood and the impact of the full range of possible political risks on the investment stemming from all stakeholders identified, and anticipates all credible changes in the underlying circumstances.

To accurately measure the likelihood and impact of a range of political risks, it is first necessary to consider the vulnerability of the investment to a range of threats (issues and problems) posed by stakeholders considered in Step 2. In other words,

a political risk assessment asks what problems or issues could arise as a result of the investment's interaction with these stakeholders, and also considers whether the investment has adequate risk management processes in place to address those problems or issues. The weaker an investment's ability to manage political issues, the higher the probability (or likelihood) that those issues will have a negative impact on the investment.

Both the likelihood and the impact of the risks are examined so that steps may be taken to identify them as early as possible and then ideally to prevent them from occurring (reduce likelihood) or, failing that, to implement strategies to ensure that the consequences of the risk are as benign as possible for the investment (reduce impact).

The impact of political risk on companies in a particular country can include: changes to its fiscal or licence conditions leading to contract uncertainty; non-payment or delayed payment of fees or tax rebates outstanding; the imposition of disadvantageous currency controls leading to cash flow difficulties; adverse judicial rulings and corrupt or otherwise unfair tender awards undermining general business performance; and, at the extreme end, expropriation and nationalization. Inside and outside the country, this can spell wider reputational damage and lost shareholder value for parent companies, the imposition of fines and even international sanctions.

Political risk management is, therefore, in its most basic sense a strategy that ensures the avoidance of these kinds of outcomes.

Step 5: risk management

The final and ongoing stage of the process draws on the groundwork laid in the previous four steps. The various stakeholders analysed should be prioritized in terms of the level of relationship management they require. This should be based on their current attitude towards the project, the potential for that attitude to change in a meaningful way as a result of new developments with either the investment or its surrounding context, and the combined likelihood and impact of the specific political risks stemming from their behaviour to create problems for the project both currently and in the future.

Once the key political threats and risks have been identified and the stakeholders that may affect the investment's exposure to such risks have been closely considered, a framework political risk management strategy can be built. Those stakeholders whose objectives and motivations are in opposition to the investment will need to be closely and actively managed to achieve a greater area of mutual interest. Those whose objectives are closely aligned with the investment will need to be engaged and their shared objectives cemented. The importance of mutual self-interest cannot be overstated in this context: the company that seeks to 'get one over' on its host government when the playing field is tilted in its favour at one point during the lifespan of an investment project is invariably the same party that finds itself most enthusiastically pressurized whenever the balance of power shifts in the opposite direction. Ebbs and flows in commodity

prices regularly catalyse exactly this kind of tit-for-tat exchange between an extractives company and its host government.

The specifics of a political risk management strategy will always vary according to individual context: company, sector, geography and status of project. From the company perspective, community grievances with a mining project entering the production phase may involve conflict over persistent levels of fuel or equipment theft from sites and vehicles. However, resentment may be building among the community over a perceived reduction in employment opportunities, escalating environmental contamination, or the slow or non-delivery of anticipated social and physical infrastructure improvements such as new roads, power provision, hospitals and schools. Instead of attempting to address each problem in isolation, an integrated political risk management strategy would recognize that theft and protest problems are likely to stem directly from prevailing socio-economic conditions and a perception that the local community is not benefiting from the project as much as had been hoped or promised. A heavy-handed security-focused solution to the theft problem is therefore likely to exacerbate all of the issues being confronted.

Dialogue followed by demonstrable actions is key to achieving recognition and shared understanding of where jobs can be created. This may not be possible in the project itself, since positions may be too specialist; however, there may be employment-creation opportunities in the supply of services and logistics to the project's daily operations, where the infrastructure enhancement can be achieved to all parties' benefit in a cost-effective, sustainable and non-polluting, as well as job-creating, manner.

Similarly, at the national level, disputes over a project's fiscal contribution to its host country are also best addressed in a framework of collaboration rather than conflict. A solution that maximizes tax revenue by having the project run as efficiently and profitably as possible is in everyone's best interests, but may involve compromises and sacrifices on both sides. Similarly, investments that use as many local rather than foreign suppliers and partners as possible and add as much local value as possible through the refining, processing or manufacturing of raw materials unearthed from the country's soil achieve multiple positive outcomes in terms of greater fiscal income, job creation and local infrastructure enhancement.

Conclusion: the keys to effective political risk management

What unifies an effective political risk management strategy is precisely this long-term and multi-stakeholder view, employing a collection of integrated measures that will maximize the area of shared interest with as many of the most important stakeholders as possible, for as long as possible, regardless of fluctuations that may occur in either the circumstances of the project or its surrounding environment.

Accordingly, a communications plan that ensures regular dialogue with all stakeholders and explains what is being done to their benefit is critical to the

success of such a strategy. The optimum model for such a plan is one that is fully consultative and involves local stakeholders in discussions and decision making rather than just informing them constantly about what is being done for their benefit.

It is equally critical in this respect that the political risk management strategy is implemented alongside and in full coordination with – rather than isolation from or even conflict with – the project's public affairs, corporate social responsibility and community relations, security, legal affairs and local staff recruitment, retention and training programmes.

Last but not least, an effective and permanent monitoring function is crucial to a truly successful political risk management agenda. Such monitoring will provide constant visibility of changing circumstances and new opportunities that may affect the project risk profile, and will therefore require integration into the risk likelihood and impact reduction strategy. In addition to traditional 'intelligence' outlets such as the media and diplomatic communities, a project's own mobilized stakeholders – community groups, NGOs, workers' representation and so on – will often be the most effective allies and sources for such a monitoring capability.

NanoCentral®

[providing focussed expertise]

[risk management in emerging technologies]

NanoCentral is an alliance of leading organisations created to unlock the vast commercial and societal potential of nanomaterials. NanoCentral helps forge industry wide collaborations across markets and supply chains; and provides access to key enabling technologies, facilities and expertise.

Assured Nano

As a not-for-profit organisation, NanoCentral can offer significant benefits to organisations which may currently be put off by perceived high cost, risk or lack of knowledge of using nanomaterials. As world-class experts in nanomaterials technology, we can help you to overcome problems that you are already facing, or assist you to develop innovative bespoke solutions.

Backed by the Technology Strategy Board, the Regional Development Agency, One NorthEast, and the Centre for Process Innovation, NanoCentral is based in the traditional heart of the science and chemical sector on Teesside at the Wilton Centre.

NanoCentral can provide you access to technologies and expertise from our extensive Alliance of Providers to help you find solutions to the issues you have identified. NanoCentral can introduce you to potential partners to add expertise and capability to the development process. This part of the process is completely free of charge.

Nanocentral continually captures the emerging technologies from a wide range of sectors and makes these available to the emerging market. A key advantage of the NanoCentral offer is access to facilities to create and test these nanomaterial solutions in a cost-effective way. NanoCentral uniquely provides existing, potential manufacturers and users of nanomaterials single point access to an integrated and comprehensive set of nano-related capabilities that encompass:

- Development of underpinning science
- Synthesis
- Dispersion, functionalisation & formulation
- Application development
- Characterisation
- Safety, health and environment

The above steps in the supply chain have different risk profiles and are often in the hands of companies with radically different interpretations of risk management. To assist companies mitigate risk through this supply chain, NanoCentral has developed the AssuredNano Accreditation Scheme.

AssuredNano is designed to provide a clear signal to all stakeholders that nanotechnology and nanomaterial SHE (Safety, Health & Environment) is taken seriously by the business holding the Accreditation Mark and that the business is committed to ensuring that good current practice will continue to be applied.

AssuredNano is the first nanomaterial SHE Accreditation Scheme, which features annual Compliance Auditing. It also draws upon the technical expertise of one of the world's most respected authorities on nanomaterial toxicological risk and occupational medicine, the Institute of Occupational Medicine. The centrepiece of the AssuredNano Accreditation Scheme is a standard which considers all SHE aspects associated with a nanomaterial or a nano-enabled product throughout its lifetime. Uniquely, it does take a genuine cradle to grave approach.

AssuredNano differs from other nanomaterial SHE service offers in three ways

1. AssuredNano is the only nanomaterial SHE Accreditation Scheme that is all embracing, covering the entire range of nanomaterial SHE considerations relevant to a nanomaterial or a nano-enabled product from cradle to grave.
2. Underpinning the AssuredNano Accreditation Scheme is the technical expertise provided by one of the world's most respected authorities on nanomaterial SHE and occupational hygiene issues.
3. AssuredNano is the only Accreditation Scheme which will be annually audited for compliance, with a de-registration penalty for non-compliance.

The AssuredNano Accreditation Scheme provides a practical means of delivering the high level code of good corporate governance embodied within the NanoCode initiative

For more information on NanoCentral or AssuredNano, please get in touch with the team:
NanoCentral at the Centre for Process Innovation, Wilton Centre, Wilton, Redcar, TS10 4RF
E: steve.devine@nanocentral.eu
T: 01740 625 729 www.nanocentral.eu www.assurednano.com

1.7

Risk management in emerging technology areas: nanoparticles – a test case

Stephen Cash, NanoCentral

The overall environment in which innovation risk is managed may be considered by STEEP analysis in which the acronym reflects the social, technological, economic, environmental and political dimensions. This chapter focuses primarily on the technological, social, environmental and some political factors.

The innovation process in the UK

The innovation process is generally poorly understood but is the core process underpinning the emergence of new products and services. New products such as low-energy lighting or scratch-resistant touch screens don't come out of thin air. They are the end point of an often unrecognized innovation process. The UK is

extremely good at the starting point of the process, namely the science-based work, especially at the universities. The UK spends *circa* £3 billion per annum on basic research and is amongst the leading countries in filing patents and gaining Nobel prizes. However, the UK has a poor record in converting the science into technology and an even poorer record in translating that technology into marketable products. Typically, the process from science to market takes about seven years and for every £1 invested in basic research will require various parties to spend in total another £64 before the product is on the shelf.

The UK is weakest in the translational step that 'proves' the technology can be made to work at industrial scale. In the UK there are a few specialist organizations, such as the Centre for Process Innovation and the Welding Institute, that can assist in de-risking that step of the process. This compares to the 60-plus state-supported Fraunhofer institutes in Germany, the VTT institute in Finland and the likes of Battelle in the United States with its multibillion-dollar turnover. The use of such translational bodies helps reduce the risk (and costs) of scale-up. Governments and Regional Development Agencies (RDAs) in the UK have a role to play in helping the translation of publicly funded science into wealth-creating industry. Some RDAs, such as One North East, really do play an active role in helping to reduce the risk of entry for companies into these emerging markets.

The nanoparticles example

A useful example to explore is the use of nanoparticles by industry. The UK government in the early years of this century launched an initiative to help the UK benefit from the emerging field of nanotechnology.

Definition and applications of nanotechnology

Nanotechnology can be defined as: *The design, characterization, production and application of structures, devices and systems by controlled manipulation of size and shape at the nanometre scale (atomic, molecular and macromolecular scale) that produces structures, devices and systems with at least one novel/superior characteristic or property.*[1]

Just to get a sense of scale, a nanometre (nm) is one-thousand-millionth of a metre. For comparison, a red blood cell is approximately 7,000 nm wide, and a water molecule is almost 0.3 nm across. A human hair is 80,000 nm wide. People are interested in the nanoscale (which we define to be from 100 nm down to the size of atoms, approximately 0.2 nm) because it is at this scale that the properties of materials can be very different from those at a larger scale.

At the turn of the century, few nano-enabled or nanoscale products had reached market, but the hope was that intervention could help the UK gain a significant share of whatever market emerged. One part of the Micro and Nano Initiative, as it was known, was the attempt to fix the supply of nanoparticulate materials for British industry to use in the creation of new consumer products. The UK govern-

ment intervention in the nanoparticulate market is an interesting example of the unintended creation of an unquantified set of risks.

Nanoscale materials are products that have at least one dimension of 100 nanometres or below. They may be long thin tubes, angular crystals or round lumps. The materials that are around 30 nm or less are those of most interest to industry since they exhibit new or significantly changed properties compared to the bulk materials. Chemicals in bulk have well-defined properties and crucially have an associated materials safety data sheet (MSDS) that sets out the safety, toxicology, firefighting and handling data and associated procedures. One drum of acetone from one manufacturer is essentially the same, and can be risk-assessed as the same, when produced by another manufacturer. This is not the case for nanomaterials.

Risk factors in nanomaterials

The uncertainties and associated risks of nanomaterials are complicated by a number of factors. Even for a very benign material such as zinc oxide that is used in skin creams and suntan lotions there is a significant difference in its interaction with cells depending on method of manufacture, particle size distribution, morphology (whether it is long and thin or short and round), how it has been processed after synthesis and so on. In other words, all nanoparticles of zinc oxide are not created equal!

Discussions about the potential biological interactions between cells and carbon nanotubes (a favourite for the electronics and structural composite worlds) often revolve around whether the length of the fibre is right or wrong for the macrophage cells in the body to process and remove them from the body. Currently it is not possible to produce a credible MSDS for every nanomaterial.

Nanomaterials are forecast to play an increasingly crucial role in market sectors as diverse as pharmaceuticals, plastics, inks, coatings and electronics. Their use offers enormous potential for new product innovation, creating discernible differences. These will add value to brands, refresh products nearing the end of their life and create entirely new products to meet evolving needs. For manufacturers, nanomaterials can shorten the production process, save energy and raw materials and increase efficiency.

The UK government initiative

A particular part of this UK government intervention was the creation of an expert industrial alliance now know as NanoCentral. This was designed to fix a market failure in the supply chain for nanoparticulate materials. The supply chain from synthesis, dispersion and characterization of the nano-phase to formulated product was incomplete, had a high capital cost of entry and lacked some key processing steps. Government funding of capital assets at the semi-technical scale on an open-access basis greatly reduced the cost of entry for the smaller companies. At the same time a funded scheme called SAFENANO was set up to address some of the risks around toxicology and health and safety. SAFENANO is the portal for the

world-renowned Institute of Occupational Medicine (IOM) in Edinburgh. The IOM is arguably the world's expert on asbestos and issues relating to occupational hygiene and an independent authority on toxicology.

Products from emerging technologies are typically characterized by a shortage of life-cycle analysis data and safety and toxicology data. This is not surprising since the developer or entrepreneur is keen to push the product to market, even if it is a beta version, as quickly as possible. In markets that are regulated, eg pharmaceuticals and chemicals, the risk management process is well embedded and prescribes the data sets required to substantiate the safety or otherwise of the product. These data sets allow the creation of properly thought-out risk mitigation policies and an overall quantification of the risk profile.

However, the true commercialization of nanomaterials is being hampered by a number of issues, including the need to source a connected supply chain that covers all the process steps, concerns about health and safety, and a significant number of manufacturers unable to connect with the marketplace.

NanoCentral was set up in July 2006 to be the pivotal gateway for nanomaterials, enabling potential businesses looking to improve existing products and develop new products using nanomaterials to connect with a network of key technology providers. The aim is simple: to accelerate the safe commercial use of nanomaterials through a coordinated and reliable supply chain so that businesses can maximize profits. Backed by the Technology Strategy Board, the Regional Development Agency, One North East and the Centre for Process Innovation, NanoCentral is based in the traditional heart of the science and chemical sector on Teesside at the Wilton Centre.

The role of NanoCentral

As world-class experts in nanomaterials technology, NanoCentral can help to overcome problems that companies are already facing, or assist them to develop innovative bespoke solutions. NanoCentral can provide access to expertise, leading-edge technologies and facilities from the extensive alliance of providers and help companies find solutions to the issues already identified. NanoCentral can introduce companies to potential partners to add expertise and capability to the development process.

NanoCentral continually captures emerging technologies from a wide range of sectors and makes these available to the emerging market. A key advantage that NanoCentral offers is access to facilities to create and test these nanomaterial solutions in a cost-effective way.

NanoCentral uniquely provides existing and potential manufacturers and users of nanomaterials single-point access to an integrated and comprehensive set of nano-related capabilities that encompass:

- development of underpinning science;
- synthesis;
- dispersion, functionalization and formulation;

- application development;
- characterization;
- safety, health and environment.

These services can be related to each other in what is known as the nanomaterials supply chain. All steps in the supply chain have a different risk profile and are often in the hands of companies with radically different interpretations of risk management.

Despite science-fiction tales of self-replicating nano-machines reducing the planet to grey goo, there is no widespread public concern about nanotechnology. However, media interest and pressure group attention are understandable and a necessary part of the governance of science. Public debate on the balance between risks and benefits needs to take place sooner rather than later. As yet, there are not enough data about the effects of all the available engineered nanomaterials on the human body and the environment.

Managing risks in the nanomaterials area

It is the lack of hard data that makes the management of uncertainty and its subsequent quantification as risk so difficult. One consequence of the absence of well-defined risk management in the nano-area is that the insurance industry finds it hard to calculate its risk exposure, which tends to result in either no cover in the nano-area or higher corporate premiums.

The precautionary principle

First, let us consider the precautionary principle, often held up as the answer. One approach that is often cited loosely is the 'precautionary principle'. The industry response to this is that it would significantly stifle or block the beneficial development of the use of nanomaterials. The logical extension of the precautionary principle is to not handle anything until you have a full toxicological assessment and all test and lifetime data. A simple toxicological screen on a nanomaterial is likely to take a couple of years, cost at least £500,000 and need a significant number of animals. The full toxicology screen is often beyond the scope of the smaller companies, which tend to be the more innovative companies and are certainly the early adopters of the technology. Over time, it is probable that the data set will improve as state-funded and academic toxicology studies are completed and published. The EU is minded to legislate over the use of nanomaterials, and the US Food and Drug Administration (FDA) is considering what regulation would be appropriate. This is likely to force industry to take its management of risk more seriously, if only to avoid yet more poorly drafted and costly legislation.

There are real societal benefits to be gained by the safe development of nanomaterials, ranging from medicine, water and land clean-up to lighter, stronger composites. In the last couple of years the number of commercially available nano-enabled products has grown from a handful to multi-thousands of products in the consumer market.

To gain access to these benefits there needs to be a more flexible industrial-derived approach to managing the risk inherent in the creation and use of nanomaterials.

It was with this in mind that AssuredNano Ltd was created. It uses the types of approach developed in the chemical industry to quantify the risk profile. This is based on controlling exposure through the life cycle of the material right to final safe disposal.

Risk mitigation becomes increasingly difficult in most businesses that step out into new technologies. Often, scientific discovery is substantially in advance of a knowledge base that can support a robust risk analysis. The example here is from the wide field of nanotechnology, where concerns have been raised regarding the potential health and environmental impacts of engineered nanoparticles. Such concerns are quite understandable on an intuitive basis. However, real quantitative data on the effects of nanoparticles on human toxicology and the environment are minimal. Nevertheless, the voicing of legitimate risk concerns requires societal redress. The conundrum is how these concerns may be managed without resorting to a moratorium on nanotechnology development until such time as a toxicology and environmental research base can be established. Indeed, in a wider context in a rapidly developing technology, can the research base on which risk is assessed ever keep up to date with technological development?

Reaction to advances in risk understanding

A second dimension to the issue is the degree to which regulatory processes at state or international level can react to advances in risk understanding. One approach, perhaps presaged by the introduction of REACH in Europe, is to place the burden of creating the toxicology and environmental impact data and hence the risk analysis on the companies seeking to market the products. This is the so-called 'no data, no market' approach. Such an approach applied within a framework of principles rather than prescriptive regulatory legislation may afford a way forward. After all, companies have a legal responsibility to market only products deemed to be safe, and a company pursuing an unduly risky product release strategy would find itself uninsurable and hence unable to continue trading.

The application of principles allows the evolution of what constitutes good practice over time without the need continually to renew legislation. However, it does require modification of the mindset that assumes that industry will always seek to avoid being transparent about risk unless subject to legislation. Consideration would also need to be given as to how to prevent small companies, with limited resources, being competitively disadvantaged by larger organizations with a greater capacity to create the data required to open a market to a radically new product.

Providing stakeholder reassurance

Returning to the nanotechnology exemplar, a number of approaches have been taken to resolve the risk assessment conundrum and provide stakeholder reassurance. These range from those that concentrate on regulatory affairs, to those that

consider manufacturing risk assessment, to those that cover corporate governance aspects. However, until recently what has been absent is a coherent and integrated approach that looks at risk in a cradle-to-grave context. It has also been difficult to demonstrate that industry is treating potential consumer concerns with all seriousness and that the health and safety of people manufacturing and using such products are demonstrably safeguarded.

AssuredNano is designed to provide a clear signal to all stakeholders that nanotechnology and nanomaterial safety, health and environment (SHE) are taken seriously by the business holding the accreditation mark and that the business is committed to ensuring that good current practice will continue to be applied. AssuredNano is the first nanomaterial SHE accreditation scheme to feature annual compliance auditing. It also draws upon the technical expertise of one of the world's most respected authorities on nanomaterial toxicological risk and occupational medicine, the Institute of Occupational Medicine. The centrepiece of the AssuredNano accreditation scheme is a standard that considers all SHE aspects associated with a nanomaterial or a nano-enabled product throughout its lifetime. Uniquely, it does take a genuine cradle-to-grave approach.

In order to minimize bureaucracy, the standard is constructed as a 'bolt-on' addition to a business's pre-existing quality system, such as ISO 9000:2000. AssuredNano's purpose is to promote the demonstrable adoption of good current practice by those manufacturing, using or retailing nanomaterials or nanomaterial-containing products. As such, it will be progressively updated over three-yearly cycles to ensure that the good practice contained therein reflects continued advances in nanomaterial SHE knowledge. AssuredNano will deliver reassurance to other industrial partners in the supply chain, governmental agencies and the public in general that good current nanomaterial SHE practice is being employed by the business holding the accreditation mark.

The AssuredNano accreditation scheme

However, the key intention of the AssuredNano accreditation scheme is to ensure adoption of evolving good practice, as well as demonstration of an initial benchmark level of nanomaterial SHE compliance. To deliver this goal, it will be a requirement that a registered business is subject to an annual compliance audit. This will be no cosmetic feature: businesses failing to improve their practices, as well as those ceasing to maintain good current practice, will be liable to lose their AssuredNano accreditation mark.

As detailed previously, a plethora of risk initiatives are being pursued, most of which offer the prospect of recommendations in two or three years' time. A delay of this magnitude will, at best, seriously hamper the adoption of nano-enabled products. At worst it will ensure that competitive advantage in the field of nano-enabled products passes out of Europe to those geographies with a more proactive SHE approach.

AssuredNano differs from other nanomaterial SHE service offers in three respects:

1. AssuredNano is the only nanomaterial SHE accreditation scheme that is all-embracing, covering the entire range of nanomaterial SHE considerations relevant to a nanomaterial or a nano-enabled product from cradle to grave.
2. Underpinning the AssuredNano accreditation scheme is the technical expertise provided by one of the world's most respected authorities on nanomaterial SHE and occupational hygiene issues.
3. AssuredNano is the only accreditation scheme that will be annually audited for compliance, with a deregistration penalty for non-compliance.

The AssuredNano accreditation scheme standard is now available following beta testing in several high-profile UK organizations. In the EU there is a move to institute a high-level code as a statement of the corporate board regarding good governance of nano-issues (NanoCode). AssuredNano provides the teeth and the evidence of real compliance, proved through an annual on-site audit of compliance. The changes in the UK over corporate manslaughter also should help focus boards' minds over how to minimize risk and manage the related issues.

Conclusion

The contention behind this chapter is that companies have a duty to manage the risks inherent in their operations in a societally responsible way. That does not mean the stifling grip of the precautionary principle or the blunt sledgehammer of regulation. It means a pragmatic, logical and systematic application of common sense backed by procedures based on best current knowledge and practice.

The AssuredNano scheme shows that it is possible to put in place a management system that can provide and police a system of risk management even when the data set is thin or lacking. It is crucial that the scheme is a learning system that continually updates as new information becomes available. This type of pragmatic approach is extendable to products emerging from other technologies. The approach should help insurers quantify their risk more accurately.

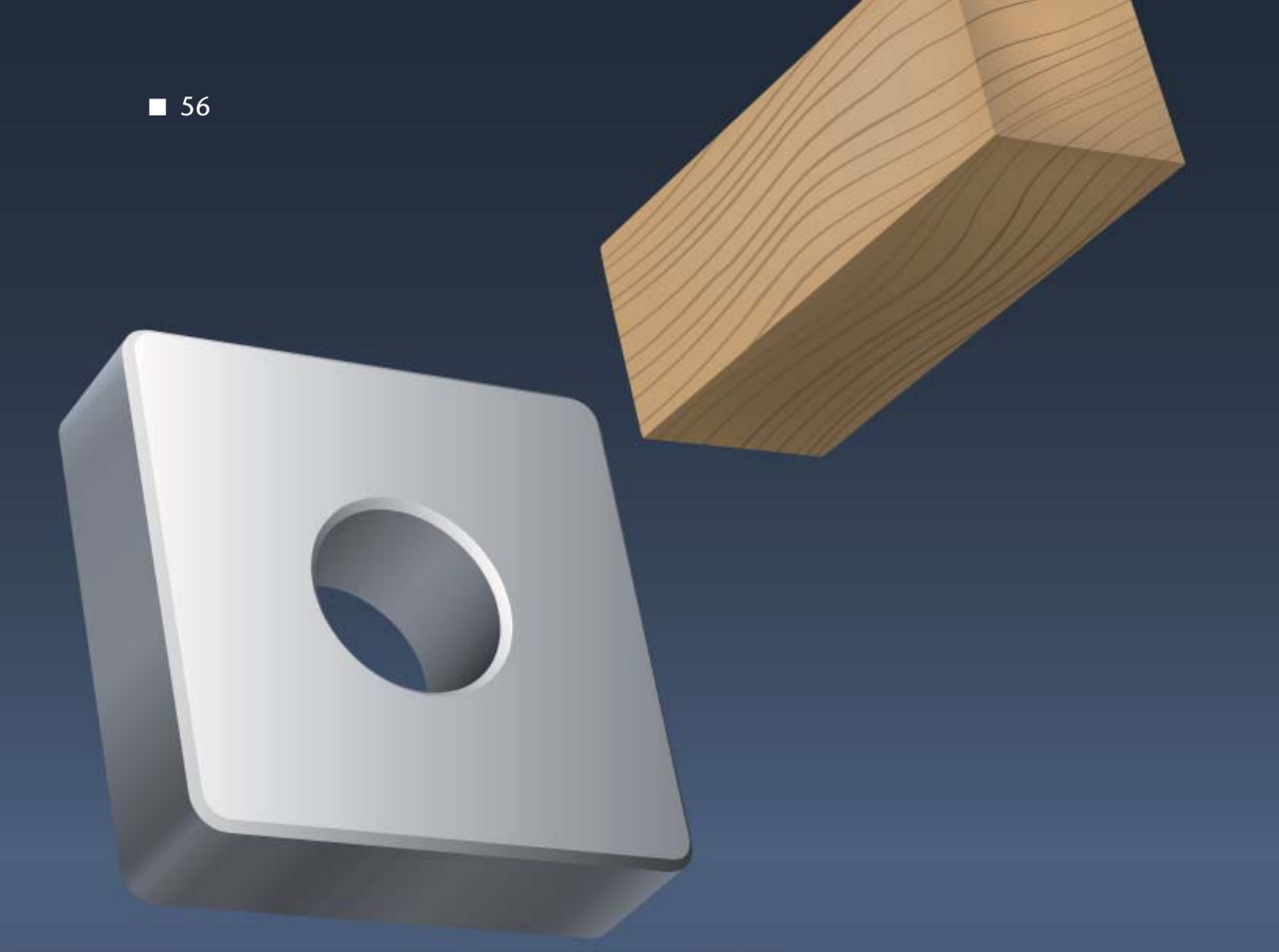
We can engage with the public over the benefits of implementing a new technology only if we can also provide assurance on the risks inherent in the new technology. The management of risk in an open way is the key to societal acceptance of emerging technologies.

Note

1. R Bawa, S Bawa, S Maebius, T Flynn and C Wei (2005) Protecting new ideas and inventions in nanomedicine with patents, *Nanomedicine: Nanotechnology, Biology and Medicine*, **1** (2), pp 150–58.

2

Insurance and Legal Liability Risks



For an integrated approach to risk and insurance management

01284 756565

towergate corporate

2.1

Taking a holistic approach to risk management and insurance

Martin Drury, Towergate Corporate

Introduction

It seems entirely logical that risk management would be a significant feature of any discussion about insurance, and vice versa. The two topics are talked about on a daily basis by insurers and insurance brokers, and there is regular discussion in the industry press regarding the obvious importance of risk management to the subject of insurance. Scratch the surface, however, and it is soon clear that there are various interpretations in the business world of how each influences the other, ranging from the notion that they are the same thing through to each being managed as a separate topic within the same business.

Therefore, the purpose of this chapter is to discuss some of the connections and influences that exist between risk management and insurance, and to understand how they could work as one to lower the total cost of risk within business.

Defining insurance and risk management

According to ISO Guide 73, the definition of risk management is 'coordinated activities to direct and control an organization with regard to risk'. This is a wide definition, which encompasses all aspects of risk including, by default, insurance.

But how does insurance manage risk? When thinking of risk transfer strategies, for instance, insurance immediately comes to mind, but what risk is actually transferred? For example, if a paint manufacturing company that mixes highly flammable solvents for use with its products decides to purchase insurance as a risk transfer strategy, is the company now immune from an explosion in the mixing plant? Of course not; an explosion will still cause damage and business interruption, but the company will be financially compensated for losses caused by the explosion (provided, of course, that all insurance contract terms and conditions are met). The point here really is to recognize that insurance is a financial risk management tool that compensates for losses incurred from other risk events.

Insurance has never been known to prevent a risk event occurring. The prevention role has become popularly known as 'risk management'. However, describing the preventive role as 'risk control' and the entire process (including insurance) as 'risk management', as illustrated in Figure 2.1.1, would be more accurate.

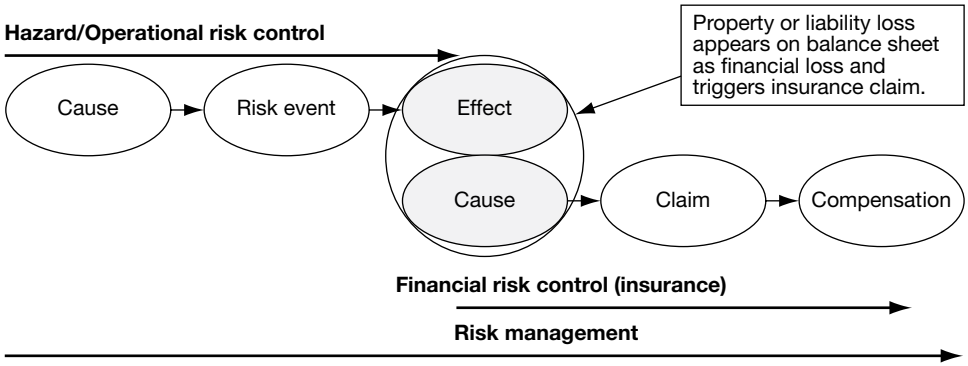


Figure 2.1.1 Progression of operational hazard risk to financial risk

Although there is an obvious and unavoidable link between risk management and insurance, they can also be seen as distinctly separate functions. The issue at hand is that the strategy and objectives of one may not be reflected in the other. The disconnection between risk management and insurance is most regularly demonstrated by the following common findings:

- businesses that have separate personnel or departments to undertake risk management functions and insurance buying functions, eg operations/safety director for the former and finance director for the latter (sometimes they communicate with each other, sometimes they don't);
- businesses whose risk register within their risk management system contains significantly different types and quantities of risks to those contained within their insurance risk schedule;

■ businesses that consider that insurance alone can be defined as risk management and vice versa.

Defining contexts

Context is an important factor when considering risk management issues, and there are a number of contexts in which the risk and insurance relationship can be viewed. For this chapter, two contexts come readily to mind, and both of these are looked at from the perspective of businesses actively managing risks and purchasing insurance.

The first context is one that could be headed as pure risk, as it is revolves around the interrelationships of risk management and insurance at a physical loss level. It's a reasonably well-worn path as a study topic, but not always that well practised, it would seem, in the wider business environment.

The second context could be headed as 'strategic', as it relates to the way in which both the risk management programme and the insurance programme can be influenced and complemented by the other to provide a comprehensive and efficient protection package suitable for the risk appetite of the business.

Again, this is not a new concept but has typically been the preserve of the big multinationals and plcs, although it can be just as relevant at mid-corporate level.

Context 1: 'pure' risk management

While it is clear that insurance does not prevent risk events, and to the extent that the risk cannot be mitigated by other means, insurance is the traditional means of transferring the financial consequence of a risk to one or more third parties. The theory is, then, that the insurance company will pay the bill for losses incurred.

While this is true to a certain extent (notwithstanding the many technical and legal reasons why it might not happen), there is the issue of uninsured losses to consider, and these can be substantial.

The Health and Safety Executive (HSE) make this point well in their accident iceberg diagram (Figure 2.1.2). Their research shows that between £8 and £36 of uninsured costs are incurred following an accident for every £1 of insurance premium spent, thus emphasizing the desirability of good risk management ahead of insurance.

The point regarding the uninsured elements of a loss is further underlined with regard to the business interruption element of the risk consequences. Research statistics published by the Department for Business, Enterprise and Regulatory Reform show that, even though insured, 80 per cent of businesses that suffer a major loss (for example, in a fire) either never restart or fail completely within a year. The commercial marketplace is unforgiving, and any threat to one business as a result of lost production will be quickly seized upon as an opportunity by other competing businesses. Although profits can be preserved for a substantial period by business interruption insurance, there is no guarantee that customers will be there when the business is up and running again.

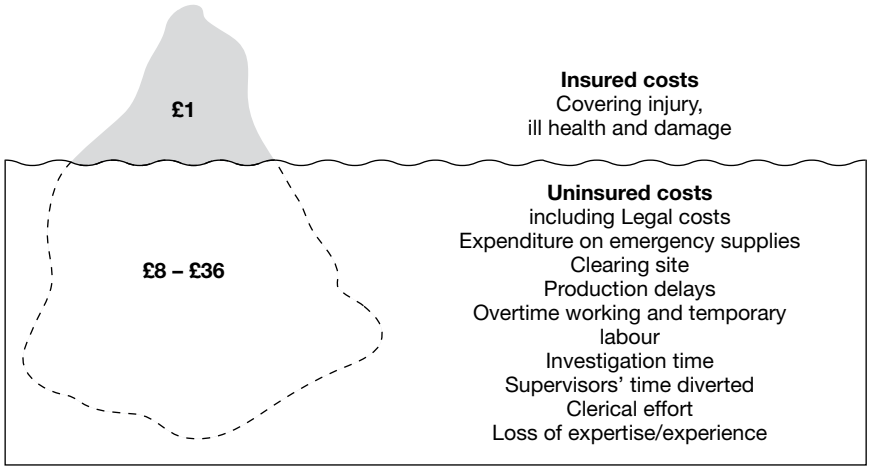


Figure 2.1.2 The accident iceberg
Adapted from the HSE model.

Good risk management initiatives in the areas of fire risk assessment, safety risk assessment and best-practice control measures, combined with a well-thought-out and communicated business continuity plan, will pay dividends on three counts. First, it will reduce the risk posed to the business by the hazards in question, especially taking into account all the associated non-insured costs as previously identified. Second, if, despite all best efforts of prevention, a significant risk event does occur, an effective business continuity plan will significantly reduce the impact on the business in a practical way that financial insurance compensation alone cannot provide (the compensation does however enable the plan to be executed). Third, a comprehensive risk management programme is a good negotiation tool that insurance brokers will be (or at least should be) keen to make use of when negotiating premium rates with insurers. There is no doubt that such good risk management looks very attractive to insurers, as of course it also reduces their own risk.

Just to relate this point to the earlier comments regarding the disconnection of risk management and insurance functions and/or personnel, if the insurance buyer is unaware of, or does not understand, the activities of the risk manager then the premium rates offered may well not reflect the actual risk.

Context 2: strategic risk and insurance management

One of the things that brokers find most commonly about insurance strategies is that there is often only the bare minimum of a strategy at all. A common strategy, understandably perhaps in the current economic climate, is lowest price, but one of the features of low-price premiums can often be policy wordings with exclusions, warranties and limits that in effect reduce, or even remove entirely, the necessary cover. Also, many insurance programmes are based on historical needs, with ad

hoc variations over a number of years that in turn become embedded into the insurance programme, making it inaccurate with regard to current risk exposures.

Competitive tendering for the insurance business is probably the most common strategy, but if the programme is wrong then the only achievement of this process is still the wrong insurance cover but (possibly) at a lower price. Even a so-called 'insurance programme review' rarely clarifies where actual risk and insured risk are uncoordinated, because the insurance reviewer frequently does not have access to the full analysis of the actual risk.

Therefore, the proposition is that, while insurance is a substantial component of a holistic risk management strategy, the optimum programme of covers cannot be obtained without utilizing other risk management practices. Ironically, the risk of inadequate insurance cover rarely features on business risk registers and, interestingly, failure to maintain adequate insurance cover has been an exclusion under directors' and officers' policies in recent times.

It is well understood that businesses need to take risks, as it is this risk taking that brings rewards for investors in excess of the standard risk-free rate of return and, of course, many of the risks that businesses are exposed to, such as marketplace and contract performance, are not insurable anyway. But, of the pure risk exposures that are insurable, there is still the question as to how much risk should be retained and how much should be insured.

This is a question that can be difficult to determine and unfortunately is often ignored. However, considering 'the theory of the firm' and duties to shareholders, it is crucial that the degree of risk to be taken by any business is determined and communicated to and understood by shareholders or stakeholders, as highlighted in the recent banking crisis.

In theory at least, we could have a situation where no assets or liabilities were insured. First, however, any business contemplating this course of action would need to have exceptional faith in its own internal risk management capabilities. Second, many perils, most notably at the moment those related to climate change, are not controllable by humans, so this would also be madness. Third, the law requires that certain insurances are obtained. At the other end of the scale, full insurance cover for each and every conceivable risk event regardless of degrees of exposure would not make any financial sense at all. Somewhere in between lies the optimum cover for each business.

Identifying and evaluating insurable risks

The natural starting place for any business wishing to manage its risks is to identify and assess the risks to which it is exposed.

While there are many risk management standards for practitioners to choose from, including the Institute of Risk Management (IRM) standard, the well-established Committee of Sponsoring Organizations (COSO) standard and the recent BS 31100 to name but three, the detailed procedures are outside the scope of this chapter. However, the basis of them all in the simplest of terms is to identify risk, evaluate it and decide how to treat it.

An important objective here is to capture risks from across all risk environments, eg by reference to the 7 environment model or section 2.1 (key risk drivers) of the IRM risk management standard. Traditional silo risk management approaches often fail to capture the significant risks that fall outside the defined silos.

With all identified risks recorded in a comprehensive risk register, each one can be analysed and evaluated and a treatment strategy defined. The analysis of the risk is crucial to ensuring that insurance cover is operative under the terms of the policy, ie relevant causes and circumstances of concern are covered in the policy wording.

Value at risk for property and materials is less straightforward than might be imagined, as balance sheet values may be written down to account for depreciation, land may be included in property valuations and so on. Actual reinstatement costs might be quite different to perceived values.

Liability risk can be equally difficult to value, as damages claims may vary considerably. Benchmarking with similar industries provides a reasonable expectation, but an analysis of all potential consequential third-party losses emanating from any risk event (similar to a 'failure modes and effects' analysis) will provide a more bespoke indication of the amount of insurance cover required.

The business continuity aspects of the risk register should indicate the levels of cover and indemnity period for business interruption cover. Business interruption risk is the potential loss of profit resulting from the reduction of turnover and increased cost of working as a consequence of a specified insured event, until such time as the turnover has been restored to its projected level or the selected indemnity period has been reached.

Using risk information

Traditional risk registers can be misleading with regard to risks that have been assessed as low, because, although likelihood may be substantially reduced by risk control measures, the impact component of the risk still may not be acceptable or tolerable to the business. Therefore, insurance cover still needs to be considered, based on the maximum possible impact. The reduction in likelihood is not without benefit, though, as this should be reflected in the premium rate charged by the insurer (provided that it is communicated to the insurer).

In all categories of insured risk, it cannot be emphasized enough that it is essential to check the actual identified business risk exposures against the contract wordings in the insurance policy. Unfortunately, the analysis within risk registers is often insufficient. The precise circumstances, including causes and effects of a possible risk event, need to be defined and reflected in the insurance policy wording to ensure cover as intended.

It is not unheard of to find that the risks of greatest concern to a business are the ones specifically excluded in the insurance contract. Nothing should be assumed. Typical assumptions are, for example, that public liability insurance will include all environmental pollution clean-up costs, whereas such costs are likely to be excluded unless the pollution is sudden and accidental and results in actual injury or damage, or that product liability insurance will include product recall costs,

whereas it frequently doesn't. Similarly, a business interruption policy covering loss of electrical supply may often be found to operate only if the fault occurs within a substation, hence leaving the business exposed to transmission line failures occurring elsewhere. However, insurance cover for each of these and other examples such as territorial limits is almost always available as an option provided that the need is identified and circumstances disclosed to the insurers.

Another advantage of cross-referencing specific identified risks to the insurance policy contract wording is that it is often found that the business in fact has no need for some insurance covers either in parts or as a policy in its entirety. In the aforementioned example of electricity supply failure, a business with its own standby generator may decide not to take such insurance, but, if a 'belt and braces' approach is opted for, the premium rate should reflect the greatly reduced likelihood of a claim occurring.

Appetite and total cost of risk considerations

Having determined the detail of risk exposures and potential loss values within the risk register it is logical that a business would want to consider its risk appetite policy so that this is reflected in the insurance buying programme.

Acceptance of the consequences of a risk in full or in part is a valid response, but this needs to be in line with the business's declared risk tolerance levels, which will be decided by the board of directors using a combination of the ability of the business to absorb losses and the attitude of the board (or, perhaps more correctly, the shareholders) towards risk. Whilst it is acknowledged here that risk tolerance may be established by a number of measures, in this instance the measure is financial loss.

Taking these factors into account, an insurance programme can be devised to cater for actual risk exposure (potential maximum loss) and provide cover consistent with the risk tolerance of the business. This may include exposure to a level of uninsured risk. Uninsured risk includes the deductible part of an insurance claim. Altering the level of deductible is a common method of retaining an element of risk within a business and thereby reducing the premium. A business with proven good risk management practices should have every reason to feel confident in having reasonably high deductibles and getting some return for its efforts by lowering its insurance premium.

However, just because a business can tolerate a set level of loss, it does not mean that it should take that risk if it can be transferred to an insurer at a substantially lower fixed rate. A lot will depend on the performance history of the business regarding losses, from which future likely losses can be extrapolated. A cost–benefit analysis of increased premium and reduced uninsured losses will identify the optimum level.

Another consideration is that the total cost of risk is made up of insurance premium, uninsured losses and the cost of risk control measures. This suggests that the allocation of resources to risk control must also be considered as a primary measure in conjunction with the optimum deductible levels. This aspect of a holis-

tic approach to risk management is a key consideration and is being accepted by many leading insurers to the extent that they are willing to divert premium income back into risk control measures for the business, as ultimately this reduces risk for the insurer and reduces the total cost of risk for the business.

In summary

Risk registers can be usefully expanded to form the basis of, and include, the relevant insurance arrangements and detail. Insurance policies initiated without such reference to accurate risk registers are less likely either to provide the required cover in the required circumstances or to reflect the risk appetite and tolerance of the business. The total cost of risk will not be maintained at its optimum level.

The expertise to insure from build to boardroom

Environmental Liability
Architects & Engineers
Construction
Property & Business Interruption
Employers' Liability
Public Liability
Directors & Officers
Professional Indemnity

Whether buying a site, designing a building, constructing an office block, or running a business, you need specialist insurance cover you can rely on. Our global experience combined with local knowledge and a strong focus on client service can support you at every stage from planning to ongoing operations.

Expertise. Commitment. Strength.
Just a few of the reasons why XL Insurance is a market of choice.

+44 (0) 20 7933 7000
www.xlinsurance.com

The XL Insurance companies have one or more of the following ratings: A (Excellent) by A.M Best, A (Strong) by Standard & Poor's.

XL INSURANCE

2.2

The dangers of ignoring environmental liabilities

Simon White, XL Insurance

Introduction

Stricter and more onerous environmental regulation has moved companies' exposures to environmental liabilities up the risk agenda. Many businesses purchase specialist environmental insurance to protect their balance sheet against the potential financial fallout of a pollution event. Environmental insurance is no longer a niche product relevant only to the most serious potential polluters, but has become an important element of a company's overall risk assessment.

This chapter will outline the rules and potential liabilities for companies under the European Environmental Liability Directive and explain why the traditional cover such as property or general liability insurance has proven insufficient for this specialist market.

Making the polluter pay

Over the last few decades companies have started to clean up their act, in line with changing social and political attitudes towards environmental pollution. Since its humble beginnings in the 1970s the modern environmental movement has always

highlighted the impact of major pollution incidents to increase awareness. Public pressure to hold polluters accountable for their actions has tended to rise following a catastrophic event. Pressure groups like Greenpeace and Friends of the Earth have also used global conferences, such as the 1992 UN Earth Summit in Rio de Janeiro, to motivate politicians into passing tougher environmental laws.

Table 2.2.1 Key events influencing public opinion

	Key events
1962	*Silent Spring* published, seen as helping launch the environmental movement.
1976	Seveso, Italy: explosion at chemical plant results in dioxin contamination of surrounding area.
1980	Lekkerkerk, Netherlands: toxic contamination under housing estate leads Dutch government to establish programme to clean up contamination.
1986	Basel, Switzerland: contaminated water pollutes Rhine, leading to European Commission proposing a liability system for remedying environmental damage.
1987	Brundtland Report, *Our Common Future*, coined the phrase 'sustainable development'.
1989	Alaska, United States: oil tanker *Exxon Valdez* spills 10.8 million US gallons of crude oil into the sea.
1992	UN Conference on Environment and Development in Rio de Janeiro introduces the 'polluter pays' principle.
1998	Aznalcollar, Spain: escape of about 6.5 million cubic metres of toxic waste from tailings dam at Boliden Ltd's lead-zinc mine.
1999	Britanny, France: spill from oil tanker *Erika* causes widespread damage to coast.
2004	The Environmental Liability Directive enters into force.

Many see the public outrage following the sinking of the oil tanker *Erika* in December 1999 as a key event in motivating public opinion towards the so-called 'polluter pays' principle. The *Erika* sank in a heavy storm off the French coast, spilling thousands of tons of oil into the Bay of Biscay as it went down. Over 400 kilometres of coastline were affected by crude oil, killing tens of thousands of birds. In this case, Total, which had chartered the *Erika*, not only ended up paying more than €200 million towards an extensive clean-up operation, but, in a landmark ruling, was also fined €375,000 for the ecological loss 'resulting from the damage caused to the environment'. In addition, Total was ordered to compensate nearly 100 parties affected by the pollution, including fishermen, hoteliers and bird protection associations.

The Environmental Liability Directive

This 'polluter pays' principle is at the core of the latest European environmental legislation, the Environmental Liability Directive (ELD). The Directive takes environmental laws to the next level, leading to potentially expensive clean-up costs for

polluters. This strengthening of the 'polluter pays' principle, with its consequent clean-up costs after an incident, introduces a significant liability for companies. As a protection against this risk, it is not good enough anymore to rely on the existing standard property or general liability insurance, hoping it will cover a pollution incident.

The ELD changes the way companies deal with pollution. Under the Directive, for instance, polluters are required to take immediate steps to prevent damage to the environment and to notify the enforcing authority of a potential incident. Non-compliance could, in the worst case, lead to a criminal prosecution, a risk no company director would want to face. This requirement alone has increased the volume of notifications to the regulator in a number of EU countries that have implemented the Directive.

The Directive also requires authorities to enforce the 'polluter pays' principle, compelling a clean-up and possible restoration of the polluted area, paid for by the polluter. This includes:

- *Primary remediation.* Restoration of the natural resource to its baseline condition, that is, its condition before the environmental damage occurred.
- *Compensatory remediation.* Certain natural habitats and species are especially protected and, if damaged, there may be a requirement for compensation to the regulator in the form of a material action or financial payment.
- *Complementary remediation.* This may be required if the polluted area cannot be brought back to its baseline condition following a clean-up. Remediation could, for instance, involve acquiring new land and creating a complementary habitat from scratch.

Wide remit

Despite the best endeavours of companies to operate environmental management systems and invest in maintenance of site infrastructure, the potential still exists for accidents, human error or machine malfunctions to result in pollution.

Pollution incidents might not happen every day, and most people think of an event as being a catastrophic failure, such as a fire and explosion, or accidental damage to a pipe or storage vessel. In reality, the majority of pollution incidents are caused by a small drip from a tank or pipe, or a number of releases that individually might cause no harm but in accumulation could be harmful. Sometimes a significant environmental liability will not be known until it is too late.

Like other EU member states, the UK has extended the remit of special natural habitats requiring protection to include the 5,000 sites of special scientific interest (SSSI) in England and Wales. Consequently, many companies will have operations in relatively close proximity to one of these specially protected natural habitats, requiring extra (and more expensive) clean-up if damaged.

Importantly, the Directive applies not only to pollution incidents but also where damage has been caused to the environment, further extending a polluter's liability. For instance, companies could be held liable for causing damage

by flooding an SSSI. Even if the water itself was not polluted and the site is drained quickly, compensation is needed for any damage to plants and animals on the site.

Further to this, local conservation organizations, animal welfare groups or non-government organizations (NGOs) also have the right to ask the authorities to investigate potential polluters, should they feel the initial response by the authorities was inadequate. In countries that have implemented the ELD, we have seen NGOs making use of this right, especially where there is a history of local campaigning.

The cost of cleaning up

Two decades ago companies would just have cleaned up the pollution and might only receive a fine in serious cases. The main costs paid by the polluter were to compensate third parties for damage resulting from the pollution.

The concept of complementary remediation, introduced by the ELD, is relatively new in the UK and Europe. It has been described as giving 'rights to nature' or a way of compensating special protected nature for any loss of biodiversity following a pollution incident (see Figure 2.2.1).

We can get a good idea about the costs for this type of remediation work from the US concept of Natural Resources Damage (NRD). An example from the United States involved the rupture of a pipe at an oil-processing facility, resulting in around 22,000 litres of waste oil entering a river used for recreational purposes with a sensitive ecosystem. In this example the emergency response included containing and recovering the oil. Over 100 workers spent several weeks on this initial response and remediation activity. Nearly 16 miles of riverbank had been affected, and nearly 100 oil-soaked birds needed cleaning. An additional number of birds died as a result of the oil.

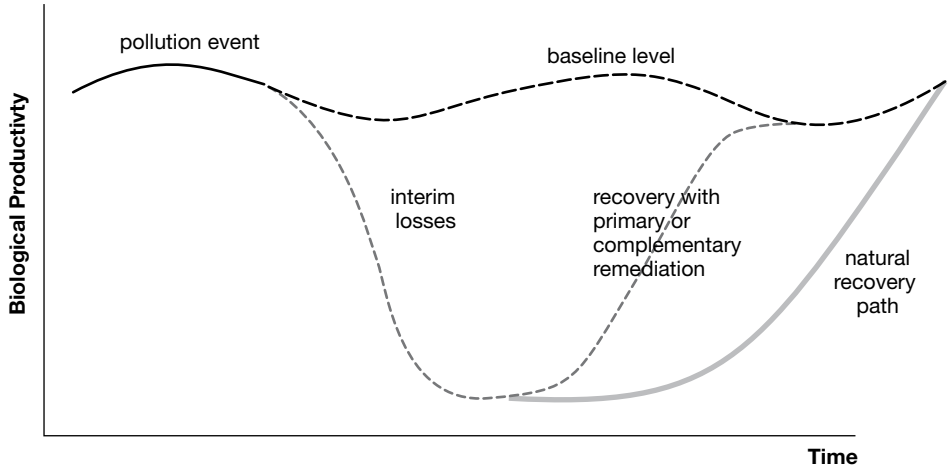


Figure 2.2.1 Restoring nature to its baseline

Following the clean-up, the polluter and its insurer hired an NRD expert to conduct a detailed site remedial investigation, which involved reviewing and categorizing the ecological damage. Based on this assessment, the affected areas along the riverbank required either further cleaning or actual removal. The shoreline banks required flushing, and the extensive cleaning process needed to be constantly monitored. The ultimate ecological restoration included the replanting of reed beds and other vegetation along the river.

The total cost for the emergency response, the subsequent pollution and NRD assessments and characterizations, the actual remediation itself, the ecological and species restoration and rehabilitation (similar to the ELD's 'primary remediation' and 'complementary remediation') and the legal costs is estimated at around US$2.5 million. On top of the above actions aimed at restoring nature to its baseline condition, the NRD concept equally assesses interim loss to the environment as a result of the pollution incident. The claim for NRD (compensatory remediation) was expected to be in excess of US$250,000.

Some firms still believe that their General Liability (GL) policies cover a significant proportion of their environmental risk. However, since the 1990s, GL policies have generally been restricted to 'sudden and accidental' events, still leaving some confusion as to what, in terms of environmental liabilities, the GL form does cover. In most cases the GL policy will not respond to a gradual pollution condition or first-party clean-up of soil and groundwater, as Figure 2.2.2 illustrates. In addition, there is considerable uncertainty as to whether such policies would respond to statutory liabilities following intervention by an environmental regulator where there had been no claim by a third party, eg the pollution of groundwater resulting in a clean-up notice from an environmental agency.

In the UK, this issue was brought to light by a 2006 court case that ruled that a company's GL policy did not cover off-site clean-up costs arising from a sudden and accidental event.

Coverage available…	**Gradual release**	**1st Party Cleanup**	**Regulatory Notice**	**Biodiversity Damage**
GENERAL LIABILITY POLICY	No	No	No	No
PROPERTY POLICY	No	No	No	No
ENVIRONMENTAL POLICY	Yes	Yes	Yes	Yes

Figure 2.2.2 Insurance coverage

The Bartoline case

In May 2003, a fire at the premises of Bartoline Limited, a manufacturer of adhesives, packed solvents and woodcare products, resulted in firefighting foam and chemicals polluting two watercourses. The UK Environment Agency carried out emergency clean-up work, for which it invoiced Bartoline over £620,000. In addition, the Environment Agency required the company to carry out further remedial work at a cost of nearly £150,000.

Bartoline's insurer agreed to pay some claims resulting from the fire under its GL policy but not for the clean-up costs. The policy covered 'legal liability for damages' and it was argued that the clean-up costs did not fall within that definition.

In the resulting court case the English High Court ruled in favour of the insurance company. The judge said that, in looking at the insurer's wording, the term 'damages' referred to civil liability and not statutory liability. The court considered statutory liabilities to operate as debts. As the clean-up costs invoiced to Bartoline were a statutory liability stemming from the Water Resources Act 1991, Bartoline was therefore not covered by its general liability policy.

Financial provision

The EU encourages the uptake of a form of financial provision to pay for the expected increase in environmental clean-up costs under the Directive. A few member states are even making financial provisions for clean-up mandatory, something that is anticipated to be reviewed on an EU-wide basis over the next few years.

In response to the Directive, the insurance market has developed a range of products providing cover for all liabilities that may arise as a consequence of the ELD. Environmental policies combine third-party liability and first-party property coverage, on- and off-site clean-up costs, legal defence and technical expenses for sudden and gradual pollution conditions. The insurance is seen as an effective way to protect a company's balance sheet and, in some cases, can incorporate cover for first-party business interruption and additional costs of working following the pollution condition.

Environmental claims are notoriously complex and expensive to settle, and it may take some time before the full costs of liabilities arising under the ELD come to light. Companies need to remain proactive in their exposures and liabilities to ensure they have the right protection in place to match these risks. As environmental legislation becomes ever stricter and pollution more expensive to clean up, risk managers will realize that a firm's environmental liability becomes a business risk they can't afford to ignore.

Putting your risk management needs at the centre of our world.

At HSBC Insurance Brokers we strive to provide our clients with the confidence and certainty to pursue their objectives. As one of the largest insurance broking organisations in the world, HSBC Insurance Brokers has the depth of knowledge to analyse complex situations from multiple perspectives and develop innovative solutions that proactively meet the specific needs of our clients.

The Intelligent Alternative

Call: +44 (0)20 7661 2050
Email: insurancebrokers@hsbc.com
Web: www.insurancebrokers.hsbc.com

HSBC Insurance

2.3

Health and safety compliance

Andrew Templeton, Corporate Customer Group, HSBC Insurance Brokers Ltd

Setting the scene

Good morning. I understand you are here to carry out the health and safety inspection. Excellent. We are very safety conscious at Totally Deluded Ltd and are fully up to date and compliant with current legislation and take the safety of our employees and visitors very seriously.

It shouldn't take you long, but unfortunately I have got to go to another meeting, so can I leave you in the capable hands of our production foreman? He is just repairing a machine that keeps breaking down and will be about half an hour, so you might as well make a start on your own.

If you need to see a copy of our health and safety policy, it's on the shelf over there. Just wipe off the dust. It's so good that we haven't looked at it for a few years. Just be careful when you walk around the factory, though; those forklift drivers are a law unto themselves. Oh, and if you go into the boiler room, be a bit careful, as our odd-job man is just removing some asbestos from some of the boiler pipework to make us compliant with the Asbestos Regulations. He's got a bad cough at the moment and gets a bit grumpy if you get in his way.

Unbelievable? Well, not really. This is still a familiar story, and even in these days of greater health and safety awareness this scenario is still common with many businesses.

Bureaucracy gone mad or sound business practice? Well, although recent figures would seem to suggest that the number of people killed at work in Britain actually dropped in 2008, provisional statistics recently published by the Health and Safety Executive still show that, between 1 April 2008 and 31 March 2009, 180 people were killed at work, corresponding to a fatal injury rate of 0.6 per 100,000 employees. This figure is still far too high, prompting Natasha Freeman, the President of the Institution of Occupational Safety and Health, to say:

> These figures show the true need for health and safety in this country. It shows that health and safety is not just mindless bureaucracy, brought in to make life difficult, or prevent us enjoying our lives. It's about preventing true tragedy that destroys lives. Each worker killed in an accident leaves hundreds, even thousands, of people mourning the needless loss of a loved one, friend or colleague.

Legal background

There is a plethora of legislation applicable to health, safety and welfare in the UK, a good deal of which has originated in Brussels since the UK has become a member of the European Union (EU). It is impossible in a chapter such as this to cover all relevant health and safety legislation. However, the key legislation in the UK and the bedrock for the majority of current health and safety law is the Health and Safety at Work Act 1974 (HSWA), the Management of Health and Safety at Work Regulations 1999 (MHSWR) and the associated Approved Code of Practice (ACOP).

The HSWA sets out the general duties of employers to their employees, of employers to non-employees and of employees to colleagues and visitors in the workplace. The Act states that employers should, so far as is reasonably practicable, ensure the health, safety and welfare of their employees in the workplace. In particular, this duty extends to:

- the provision and maintenance of plant and equipment and safe systems of work;
- arrangements for ensuring safety and the absence of risks to health in the use, handling, storage and transport of articles and substances;
- provision of information, instruction, training and supervision to ensure employees' health and safety at work;
- the maintenance of a workplace that is safe and without risk and the provision and maintenance of a safe means of access and egress;
- the provision of a safe working environment that is without risks to health and adequate in terms of facilities and welfare arrangements.

Whilst most employers are in the main conversant with the need to maintain a safe workplace and safe working practices, many are still failing miserably, as the

aforementioned statistics would seem to indicate. Management will often paint a rosy picture when sitting around a meeting table, but when you get to the reality of the shop floor you often find a very different picture. Unsafe working practices, inadequate machine guarding and unsuitable workplace transport arrangements, including forklift drivers trying to emulate Jenson Button, are commonplace.

An employer also has a similar duty, so far as is reasonably practicable, not to expose non-employees to undue risks. Employees themselves have a duty to take reasonable care to ensure the health and safety of themselves and others and to comply with any management policy aimed at meeting the employer's legal duties.

The HSWA also imposes a duty on employers with five or more employees to compile and record a health and safety policy and to bring this to the attention of those employees. Unfortunately, whilst most employers have a health and safety policy of sorts, this is generally insufficient and does not include a statement of intent signed and dated by the most senior person in the organization or responsibilities and arrangements sections. It is not uncommon for an employer to pay an external consultant a small fortune to compile a health and safety policy and, like Totally Deluded Ltd, put it away on a shelf to gather dust. In order to comply with legislation it is essential that the policy is a live document that is constantly monitored and reviewed.

The MHSWR became law in the UK in 1993 following an EC directive and were updated in 1999. These regulations reinforced and amended the requirements of the HSWA and in many ways redefined the duties of employers and employees.

One of the key requirements of the MHSWR is for employers to make a suitable and sufficient assessment of the risks to the health and safety of employees whilst they are at work and to non-employees who may be affected by their activities. It is also a requirement that where the employer has five or more employees it must record the significant findings of the assessment and any group of its employees identified by the assessment as being especially at risk.

This is an area where employers constantly fail to comply with legislation. Either they do not have any risk assessments, or what assessments they do have are not suitable and sufficient or are rarely reviewed to reflect current activities and working practices. Many health and safety prosecutions brought by the enforcing authorities are due to the lack of or insufficient and unsuitable risk assessments. It is essential that employers compile adequate risk assessments and assessments that will stand up in a court of law. They should regularly review all risk assessments to establish that they are being undertaken in a methodical way and that they cover the full range of business activities.

Many employers are also still in contravention of more recent legislation such as the Control of Asbestos at Work Regulations 2002, the Fire Safety Reform Order 2006 and the new Noise at Work Regulations introduced in 2006, to name but a few.

The Control of Asbestos at Work Regulations 2002 and the Health and Safety Executive Guidance Note MDHS 100 relate to non-domestic premises. These regulations require confirmation of the absence of asbestos-containing materials or evidence of an asbestos management plan. The plan should include the type of

asbestos involved, where it is located, the condition of the material, the inspection routine, and the timescale for removal or remedial works. Unfortunately, whilst compliance with these regulations was required by May 2004, many companies are still in contravention of the regulations and do not have an asbestos management plan or they have a plan but it has not been reviewed and is out of date. The maximum penalties for non-compliance are an unlimited fine and/or up to two years' imprisonment.

Fire in the workplace is still a major risk, with arson still the biggest cause of fire in the UK. The Fire Safety Order came into force in April 2006 and was introduced under the Regulatory Reform Order, with the aim to 'simplify, rationalize and consolidate existing legislation'. Previous fire legislation was repealed, and one of the key things to come out of this new piece of legislation is the fact that the fire authority will no longer issue fire certificates; each company is now responsible for its own fire safety and needs to organize a fire risk assessment of its workplace. It would seem that there are still many employers that have not completed fire risk assessments, are therefore are not compliant with this legislation and are leaving themselves open to prosecution.

The new Noise at Work Regulations were introduced in 2006 and require employers to prevent where possible or reduce the risks to health and safety from exposure to noise in the workplace. These new regulations reduced the daily or weekly exposure action value to a lower exposure action value of 80 dB(A), an upper exposure value of 85 dB(A) and an exposure limit value of 87 dB(A). Once again, many employers are still not complying with this revised legislation and still need to appoint a competent person to carry out a risk assessment to establish which employees are exposed and to ascertain the need for hearing protection, ear protection zones and the reduction of noise exposure.

Finally, results of the second annual British Safety Council (BSC) survey indicated that, whilst 95 per cent of managers thought they knew what to do to make their workplace legally safe, 26 per cent were unaware of key pieces of recent legislation such as the Corporate Manslaughter and Corporate Homicide Act 2007 and the Health and Safety (Offences) Act 2008. These Acts will be covered later in this chapter.

They were also unaware of the Institute of Directors Guidance for Directors, which was published in October 2007 by the Institute of Directors (IoD) in collaboration with the Health and Safety Commission (HSC). Essentially, directors in the UK have compiled their own commonsense health and safety guidelines to remind directors of their responsibilities to lead the way on health and safety and ensure that policies and practices are in place to make health and safety integral to their culture and business values.

Health and safety in a recession

The results of the second annual survey by the BSC revealed that one in 10 employees have concerns about raising health and safety concerns during the recession. The BSC feel that this survey indicates that the recession is affecting health and

safety in the workplace, which could ultimately threaten people's lives. One in 12 employees also state that they were under pressure from management to take risks with employees' safety as a cost-cutting measure.

It can be seen from earlier in this chapter that the number of deaths in the workplace in 2008 would appear to be down on the previous year's figures. However, the Health and Safety Executive have suggested that evidence from previous downturns seems to point to the fact that injury rates actually fall during a recession, mainly as a result of fewer new, inexperienced workers being employed, less work being conducted in the workplace and the proportion of employees operating long hours falling as demand declines. Employers must not therefore be misguided by these figures and lose a sense of direction. It is very tempting for companies to reduce health and safety budgets during this period and to cut down on expenditure in essential areas such as education and training. However, they must look to the long term, to the time when the economy improves, the worst of the recession is over, demand is buoyant and the numbers of employees in the workplace are up once again. Areas such as education and training will be critical during this period.

It is also essential during the period of a recession, when turnover and profit may be at their lowest ebb, that employers do not incur the unnecessary costs associated with accidents in the workplace owing to the short-sighted decision to cut back on health and safety.

Other relevant legislation

In this chapter we have looked at health and safety compliance only in relation to current legislation, ie from a criminal law perspective. The rights a person has for recompense under civil law, mainly through the tort of negligence, should also be borne in mind. A successful action against a company for negligence can be very damaging and harmful to a company's image as a caring employer, particularly in the moralistic world in which we live.

Businesses these days face a complex array of health and safety and environmental laws and responsibilities, and the minds of many employers have become more focused since the introduction of the Corporate Manslaughter and Corporate Homicide Act 2007, which came into force in 2008.

Under this Act an offence is committed if, in the event of a death, there have been failings by an organization's senior management that are a significant element in any gross breach of the relevant duty of care owed by the organization to the deceased person. In the event of a conviction, the maximum penalty is a fine of unlimited magnitude; additionally, the court can make a publicity order requiring the company to publish details of its conviction and fine. Remedial or improvement notices may also be imposed.

Failure to comply with the requirements of health and safety law in general can have serious consequences for both individuals and organizations. The sanctions for failure to comply can include fines, imprisonment and disqualification.

The Health and Safety (Offences) Act 2008 came into force on 16 January 2009, and the effect of this Act was to raise the maximum fine that may be imposed in the

lower courts to £20,000 for most health and safety offences. The Act also made a custodial sentence an option for more health and safety offences in both the lower and the higher courts, and made it possible to try certain offences in either the lower or the higher courts that previously could be tried only in the lower courts.

Conclusion

It is imperative in these difficult economic times that employers have a strong embedded safety culture driven from the very top and with the requisite buy-in from employees, particularly those at the sharp end. Employers such as Totally Deluded Ltd should constantly review their practices and procedures to ensure they are fully in compliance with their legal, financial and moral obligations and do not leave themselves open to unplanned-for and needless fines or even the possibility of a custodial sentence. In today's competitive business market, where the credit crunch and recession have forced companies to review their costs, it is essential that resilient management procedures are in place to avoid any unnecessary expenditure associated with poor health and safety management.

The importance of maintaining good public relations, consumer goodwill and, where appropriate, shareholders' confidence cannot be overestimated. The corporate identity of an organization and brand protection are becoming more and more important, because corporate identity is a highly valuable piece of intellectual property.

In 2007 a survey carried out by Business Continuity Management, supported by the Cabinet Office and Continuity Forum, identified that 17 per cent of managers blamed health and safety incidents for business disruption (up from 13 per cent in the previous year). The same research, which was carried out with 1,257 public and private sector managers, also highlighted the fact that almost half (49 per cent) perceive 'damage to brand' as a major threat to their business.

In summary, therefore, compliance with health and safety responsibilities is a legal, financial and moral necessity that is sound business practice and certainly should not be misconstrued as bureaucratic nonsense to which employers can merely pay lip service.

The information and opinions contained in this chapter are not intended to be a comprehensive study, nor to provide legal or broking advice, and should not be relied on or treated as a substitute for specific advice concerning individual situations. References to legislation, court cases and their effects are merely provided as an overview and reflect the law and practice at the time of publishing. Specific advice should always be sought on individual requirements, and it is always necessary to read the contractual documentation issued by underwriters for full details of the product and cover provided.

2.4

The role of professional indemnity insurance in managing business risk

Daniel Rouse, Field Fisher Waterhouse LLP

Introduction

Until the middle of the 20th century, the advice of professional advisers was treated with a degree of respect bordering in many cases on the reverential. The professional status of the adviser was sufficient in most clients' minds to allay any concern that losses incurred may have been the result of defective advice. In the rare instances where clients were more assertive and disputes did arise, they were more often than not settled by a reluctant reduction of fees or some other token gesture by the magnanimous adviser.

In the latter half of the century the cultural landscape changed beyond recognition, owing in no small part to a rapidly developing body of tort case law with such cases as Hedley Byrne *v* Heller & Partners [1963], which held that an adviser could be held liable for negligent statements that caused the party relying on it economic loss, and that this liability was not dependent on any contractual relationship between the parties.

The volume of litigation in the field in recent years has been such that professional indemnity insurance (PII) should be a central plank in the risk management strategy of any business that offers specialist advice. It is predicted by many that the economic storm that we have endured in recent times will only engender even more court actions as businesses look to recoup losses they have suffered and where professional advisers are regarded as the archetype 'deep pocket' defendant. In such circumstances it is timely to revisit some underlying principles and consider some basic steps that businesses can take to make sure that they have the right protection.

What exactly is PII?

At the broadest level, PII is liability insurance that indemnifies a business in the event that a third party claims to have suffered a loss as a result of an error, act or omission on the part of someone for whom the business is legally responsible. Depending on the wording of the policy, PII may also offer protection in respect of, for example, the unintentional infringement of others' copyrights, the loss of data or documents, breach of statutory terms under the Sale of Goods Act 1979 and Supply of Goods and Services Act 1982, defamation, or liability arising from the theft of a client's money. The insurance typically covers paying out on the claim or the legal costs of defending the claim, depending on the insurer's views of the merits of the individual case. In exchange for such cover, which will be up to certain specified monetary limits, the insured business will be charged a premium. The cover almost invariably runs annually on a 'claims-made' basis, a term that is considered in more detail below.

Who needs it?

Many businesses that offer professional advice are required by their regulators to obtain PII. The Financial Services Authority (FSA) for instance requires, among others, financial advisers and mortgage intermediaries to obtain PII cover, while the Solicitors Regulation Authority (SRA) imposes similar obligations on law firms. However, many businesses that offer specialist advice – from IT consultants to advertising agencies – are not obliged to have such cover, but would be well advised to ensure that they are protected. The rapid growth of the information technology sector in particular over the last decade has led to a huge increase in claims against those acting in the field: the development of outsourcing, for example, has been the source of a large number of complaints over the past few years, while the recent proliferation of blogs and other user-generated content raises obvious concerns for internet service providers (ISPs) relating to potential claims for defamation and malicious falsehood.

Why have it?

Insurance is a fundamental tool in risk management. Most economic actors are risk-averse and prefer the certainty of known small losses (in the case of insurance,

the losses equate to premium) to the possibility of exposure to a much more substantial loss. This is the case even if projections indicate that in a given period the expenditure in premiums is likely to exceed that in claims. The difference between the two is effectively the price a business is willing to pay to satisfy its risk-averse preferences and, of course, explains the profitability of the insurance industry. However, insurance offers advantages beyond 'hard' economic factors: many clients will expect businesses offering specialist advice to have PII in place as a basic prerequisite for doing business with them, and those without it are likely to find themselves at a significant disadvantage in obtaining business.

Clearly, even the risk-averse will wish to keep the premiums they pay for any given level of cover as low as possible. In order to consider the ways in which they can do this it is necessary briefly to review the factors that determine the level of premium charged by insurers.

Premium

In determining the level of premium, insurers will typically have regard to the following considerations:

1. The number of insurers in the market. All other things being equal, the greater the supply of insurers (the capacity of the market) the lower the price for the cover.
2. The profession involved and indeed, in many instances, the specific niche within the profession. In relation to solicitors, for instance, the premium charged for coverage of conveyancers has traditionally been high, reflecting the volume of claims associated with that particular field of practice.
3. The underwriting and risk profile of the individual business.

There is very little that businesses can do to affect the first two factors, but the third is one over which businesses should be capable of exercising a high degree of control. Clearly the previous claims profile of a business will be of considerable interest to the potential insurer, and businesses that have experienced large claims will do well to take the time and effort to explain the circumstances surrounding claims and the systems that have been put in place to prevent, or minimize the effects of, any recurrences. However, in determining the level of risk an individual business poses, sophisticated insurers will take into account a number of additional factors. These will of course depend on the nature of the business seeking insurance, but a number of near universal considerations can be identified, including the following: the qualifications of staff, the systems of staff monitoring and training deployed, the complaints structure in place, the existence or not of an effective written risk management policy, and any accreditation recognized by the particular business sector. This may all sound fairly obvious, but many businesses that have robust risk management systems in place fail to communicate the components of the system effectively to insurers and brokers, with the result that they do not

receive cover at the premium they should. Indeed, brokers play a vital role in securing the necessary PII coverage for business, and it is to their role we now turn.

The role of the broker

Insurers seldom deal directly with the businesses for which they are providing cover; rather the insurer–insured relationship is normally conducted through intermediaries known as brokers.

In law, brokers act as agents for the insured, which means that they owe the insured fiduciary duties (ie to act in the utmost good faith, not to place themselves in a position where their own interests conflict with their duty and not to act to their own advantage without the fully informed consent of the insured). Brokers are required to use reasonable endeavours to obtain insurance on the best possible terms. In Standard Life Assurance *v* Oak Dedicated Ltd and Aon Limited [2008], Tomlinson J stated that a broker must:

1. discover the requirements of the client;
2. match risks with coverage; and
3. arrange insurance appropriately.

If, for example, it is made known to the broker by the insured that there is a critical deadline by which the insurance must be secured, there will be a duty on the broker to ensure that quotes from insurers are obtained and presented in a timely manner.

As well as the legal obligations that brokers owe, it is prudent for the insured to attempt to agree with brokers that they will provide a number of additional services. After all, brokers will normally take a proportion of the premium paid by the insured as commission and this is factored into the level of premium insurers charge insureds, so it makes sense to make the most of what brokers have to offer. It is brokers who will take policy proposals to insurers, so it is important to know the markets to which they have access and that they will be approaching. Brokers should have a detailed knowledge of the contemporary PII market for the relevant specialist, including information relating to the reputation, suitability and solvency of possible insurers. Some insurers will offer risk management support to assist in preventing claims arising in the first place, and it is worth finding out from the broker if it has access to such markets. It is often also wise to instruct the broker to obtain a range of limits (discussed further below) from possible markets so that the prevailing relationship between cost and risk can be identified and levels of cover can be adjusted, depending on the rates on offer.

The usual position is that the insured must disclose to the insurer all facts material to an insurer's appraisal of the risks that are known or deemed to be known by the insured but are neither known nor deemed to be known by the insurer. This is important because a breach, however innocent, of this duty by the insured will entitle the insurer to avoid the contract as long as the insurer can show that the non-disclosure induced it to provide the cover on the relevant terms. The broker should

have a full understanding of what constitutes 'material facts' for the relevant business sector, and this should be fully explored with the broker, as it cannot be assumed all such facts will be elicited by the policy proposal form.

On a practical level, it is sensible to agree that the broker will advise on the retention and maintenance of insurance documentation, keep all relevant records relating to the insurance arrangements and pursue claims recoveries on the insured's behalf. In order to consider other issues that a competent broker should be able to assist with, we need to briefly review some of the other main components of a typical PII policy.

Indemnity limits and the excess

As with other forms of insurance cover, PII typically involves an excess, which the insured pays, and a limit, which defines the insurer's maximum monetary liability. The limit will normally be expressed in the policy as the aggregate cost of all claims within the period of cover of the policy. An obvious problem with aggregation is that a large claim can substantially diminish or even totally wipe out the limit within the first month of the insurance year. It may be possible to reinstate the limit upon payment of an additional premium, but if a claim has been made that has exhausted the limit it may be very difficult to convince the insurer that it should provide any reinstatements. Clearly, this leaves the insured in a potentially precarious position, all the more so as the broker would be under a duty to disclose the loss to any other insurer subsequently approached to provide cover. It is critical therefore, if a business chooses (or is only offered) aggregate cover, that it ensures, in conjunction with the broker, that the indemnity limit is sufficient.

The excess is the first amount of every claim that is not covered by the insurance and that must therefore be borne by the insured. Care must be taken, however, as the definition of a claim may well have a substantial impact on the burden that remains on the insured. For example, if one negligent act leads to a hundred claims of relatively low value, is the intention that the excess should apply to each claimant's action against the insured or that it should apply only once in respect of the totality of the claims? Historically, the problem has been that insurers have regarded words such as 'cause', 'claim' and 'event' as synonymous, although case law has established that these words do not in fact have the same meaning. Again, businesses should work with their broker to ensure that their PII policy is as clearly and unambiguously worded as possible in this regard so that the ambit of the cover is readily understood.

Claims

Policies will almost invariably be on a claims-made basis. This provides cover for claims made during the period of insurance only, which means that a claim might be made against a policy written in the current year in respect of a negligent act that could have occurred many years previously. Accordingly, insurers are likely to be

very interested in the nature and standard of a business's risk management practices in the past, and these should be fully explained to the broker so that he or she is able to fully apprise the insurer of the position. Alternatively, the insurer may wish to include a retroactive date in the policy to exclude claims from acts of negligence done any time preceding that date, though any such exclusion should of course be reflected in a lower premium being charged.

The obverse consequence of a claims-made policy is that, if the policy lapses and is not renewed, there is no protection in place for any claims that may arise thereafter. This highlights the fact that PII should be considered a long-term commitment as part of a business's risk management strategy and not simply a 'one-off' for the purposes of, for example, satisfying the conditions of a contract.

A claim is generally notifiable to a broker under a PII policy when the business first becomes aware of circumstances that could lead to a claim against it, and this could be anything from a letter of complaint to receipt of a court claim form. Indeed, the definition of 'circumstances' has been the source of many disputes between insurers and insureds, so it is important that the policy wording is as clear as possible about what constitutes a notifiable event, to avoid any later uncertainty. Businesses should also bear in mind that issues surrounding prompt notification to insurers are more likely to arise in an economic downturn, when redundancies and additional pressures upon employees to perform (and thus conceal mistakes) are likely to result in delays in reporting claims to insurers.

Conclusions

PII should play a central role in the risk management strategy of any business that offers specialist advice and should no longer be seen as a necessity solely for the 'traditional' professions such as accountancy and the law. The importance of such insurance is only accentuated in the current period of economic uncertainty when all the signs are that litigation, which is historically counter-cyclical, is on the rise. It is critical therefore, now more than ever, that businesses have a basic understanding of the product and the steps that they can take to obtain cheaper and more effective cover.

2.5

Brand and reputation management: how the law of defamation can help

Rhys Griffiths, Field Fisher Waterhouse LLP

Introduction

It is a cliché that it takes 20 years to build a reputation and five minutes to ruin it, but clichés are usually based on truth. Rumour, gossip and simple factual errors can have a calamitous effect on the reputation of an individual or business. The ubiquity of the internet has made it simple to spread a factually incorrect comment, and the ripples, through adoption by bloggers and other authors, can mean a rumour is 'out there' instantly and impossible to put back in the bottle.

Reputational damage can have a severe economic impact (eg on share price or earning capacity), it can affect whole industries (eg lobbying by industry bodies) and it can cause great distress. Defamatory information can be spread innocently or maliciously; it can be spread by journalists, bloggers, competitors, would-be investors and others. It often needs to be handled urgently and emphatically – preferably before publication.

It is often thought that a defamation claim is something that only celebrities are drawn to in order to prevent the tabloids from publishing some scurrilous rumour

or other. However, it is of wider application than that, and it may properly be used to protect the reputation of a business against damage caused by the circulation of unfounded allegations.

This chapter will give an overview of the laws of defamation in order to explain how they may be used to protect the corporate brand and its reputation. This will involve considering what is defamation, what are the available defences, what remedies are available, what is the court procedure and how the position is different with regard to online defamation.

What is defamation?

There is no single legal definition for what is and is not defamatory. Generally speaking, a defamatory statement is a publication to a third party of an untrue imputation about someone's reputation that would tend to discredit that person, undermine that person's reputation in the eyes of right-thinking members of society generally, cause that person to be shunned or avoided, or expose him or her to hatred, ridicule or contempt.

One of the first points for consideration is the proper meaning of the words complained about. The law recognizes two types of meaning – the natural and ordinary meaning of the words and the innuendo meaning. The natural and ordinary meaning is, as it suggests, the meaning that a reasonable reader would give to the words. This is not restricted simply to the literal meaning of the words, and it will also include any inference that may reasonably be drawn from the words. The innuendo meaning concerns an alternative meaning, which may reasonably be understood by 'reading between the lines', or else a meaning that is innocent on its face but defamatory if the reader is in possession of some special knowledge.

Curiously, an insult, or mere vulgar abuse, is not defamatory. This is because mere vulgar abuse is likely to be taken as just that – an insult – and so the substance of the statement is not something that would be taken seriously so as to lower that person's reputation.

There are two forms of defamation – libel and slander. Libel occurs where the defamatory statement is made in some permanent form, the classic example being publication of a defamatory statement in a newspaper. Slander, on the other hand, occurs where the defamatory statement is made in some temporary or transient form, for example where a defamatory statement is made orally. The legal consequence of this distinction lies in the fact that an action for slander requires proof that the defamatory statement has actually caused the claimant damage, except in a limited set of circumstances where such damage is presumed to exist (for example, saying that someone is guilty of a criminal offence).

If it can be established that the statement is defamatory, then the next question to consider is whether the publisher has any available defences.

Justification

The defence of justification is to say that the defamatory statement is true. If this can be proved, then it is a complete defence to a defamation action. In order to

succeed, the defendant must be able to prove that the meaning of the defamatory statement (as alleged by the claimant) is true.

Fair comment

It is a defence to a defamation claim to say that the defamatory statement was a fair comment on a matter of public interest and that it was published without any malice (that is, with an honest belief in the truth of the statement). The reason for this is that where a matter is such as to affect people at large, so that they may legitimately be interested in what is going on, then everyone should be entitled to make fair comment. It is important to understand that this defence will only apply to 'comment' or 'opinions' passed by the defendant. It will not apply to any assertions of fact made by the defendant; in that case, it is the defence of justification that will apply, ie that the facts are true.

Privilege

There are two types of privilege defences available – absolute privilege and qualified privilege. If either can be established, then that provides a defence to a claim in defamation even if the words complained about are plainly defamatory and cannot be justified. The rationale behind the privilege defence is recognition that, in some instances, it is necessary for people to be able to say what they like and without the threat of a defamation claim if they happen to get it wrong.

The first form of privilege defence is absolute privilege. The list of what falls within this category is fairly detailed, but it includes matters such as statements made in the course of parliamentary proceedings, statements made during court proceedings, statements of some public officials and fair and accurate reports of parliamentary and judicial proceedings.

The other form of privilege defence is qualified privilege. Broadly speaking, this protects statements made by a person who has a duty or interest in making the statement (legal, social or moral) to a person who has a corresponding duty or interest in receiving the statement. One example where the defence might be said to apply is where a former employer gives an employee reference to a new employer, or statements made between shareholders of a company. Importantly, however, the defence of qualified privilege will be defeated if it can be shown that the statement was made maliciously.

What is the relevant court procedure and what remedies are available if you win your case?

Before a claim is issued at court, the parties ought to follow the Pre-Action Protocol for Defamation Claims. This sets out a pre-claim procedure that the parties must follow in order to try to settle the case. It begins with a letter of claim from the claimant, which sets out the complaint and the remedy sought. The defendant

then has to respond to this letter with its case, and the parties should then try to settle the matter. If there is no settlement or if the matter is particularly urgent (eg where a newspaper article has yet to be published) then the claimant may wish to issue a court claim for relief.

Claims for defamation are usually heard in the High Court. The claimant has a right for the claim to be heard by a jury, although the court may order the trial to take place by judge alone if the case requires a detailed analysis of documents or finances or if the case involves technical, legal or scientific issues.

The claimant is entitled to seek damages and/or an injunction in relation to a defamatory statement. The damages will be quantified by an assessment of that which is necessary in order to reflect the damage that has been caused to the claimant's reputation and the hurt feelings caused by the defendant's publication and to vindicate the claimant's reputation.

The claimant may also wish to seek an injunction to prevent the publication in the first place or else to stop a republication of that which has already occurred. The first type of injunction, known as a 'pre-publication' injunction, is very rare. The courts are reluctant to interfere with the right to free speech and, provided that the defendant indicates an intention to claim the defence of justification, an injunction will not be granted unless it can be demonstrated that the defendant is acting in bad faith or that the defence of justification will inevitably fail.

Special concerns regarding the internet

The dawn of the internet and its blogs and chat rooms means that defamatory statements can now be made by anyone, anonymously, to the world at large and at the touch of a button. How, therefore, do the ancient laws of defamation work in this context?

The initial answer is short – they apply equally to defamatory statements made online as to, say, articles in a newspaper. However, two practical considerations are worthy of special mention. Are the website hosts liable for defamatory comments made by users of blogs or bulletin boards? Is there anything that can be done when web users post defamatory comments anonymously?

Liability of website hosts

The general rule in English law is that an innocent disseminator of defamatory statements (ie those who did not originally publish, author or edit the statements) are not liable for those defamatory statements. So, if an individual gives a newspaper to another, totally unaware of its content, he or she will not be liable for any defamatory stories within that newspaper.

The position is the same with website hosts – provided that they did not publish, author or edit the defamatory statement, then they will not be liable. The liability will remain with the original poster of the comments. However, the position does change once a complaint is made to the website host. At that point, the website host's liability is triggered, and it will become jointly liable for any defamatory

statements contained in the particular post. For this reason, website hosts are well advised to adopt a 'notice and take down' procedure, whereby they automatically remove (or review, at the very least) defamatory statements made on their website by third parties once they have been notified of those posts.

Liability of anonymous website users

As has been described above, website users may post defamatory comments anonymously, or under a user name that does not give away their identity. Moreover, many websites do not require users to go through a verified registration process before they can post messages and so, at first glance, there is no way of knowing the identity of these users. This is material because, as has been said, it is only they who are initially liable for the statements that they post (the website host becomes liable only upon notification). Moreover, to really cut out the attacks at source, it is the user who ought to be pursued and, if necessary, injuncted to prevent any further posts.

All is not lost. Many websites keep a log of the IP addresses of the computers that access the website. From this, it is possible to obtain the IP address of the computer that was used to post a particular defamatory message. This IP address can be used to ascertain the identity of the internet service provider (ISP) that grants access to the user to the internet, who can then be asked to identify the relevant individual (whose details will have been verified by the ISP so that they can take payment). The website host and the ISP will both require a court order for disclosure to be obtained before they are prepared to divulge the IP address and personal details of the user, as they are bound by the confidentiality provision of the Data Protection Act and Human Rights Act. However, they will not typically oppose any such application.

Conclusion

It is a general misconception that the laws of defamation exist only to protect the images of the rich and famous. They are of wider application than that and may properly be used to protect the reputation of a business against damage caused by the circulation of unfounded allegations. They can be used to correct and to alter intended publications and then as a tool for obtaining vindication when the publisher steps over the line.

2.6

Software escrow – an effective tool for managing risk and new business opportunities

Stephan Peters, Deposix Software Escrow GmbH

Introduction

Option A

Observant readers who are not yet familiar with escrow may ask themselves: 'How can something that supposedly mitigates risks at the same time enable new business opportunities?' This question drills right down to the heart of this particular tool, which always serves two parties and at the same time offers both the benefit of risk mitigation and the benefit of new business opportunity to the parties involved. This chapter, in plain words, will describe how software and technology escrow work and the benefits they offer, in particular in light of the recent economic crisis.

Deposix
software
escrow

We hold the key to protect your IP – and your investments in IT

Deposix — professional Risk Management & Escrow Services

We protect your intellectual property (IP) and your investments in IT through specialized Software and Technology Escrow. Manage your risk in a professional way and let the experts handle your valuable IP - we are looking forward to serving both your local and your global escrow needs!

Our offering

Expert escrow standard contract: based on our broad experience, we help You adjust the agreements according to your specific needs.

Complete contract management process: we take over responsibility for the entire escrow lifecycle.

Technical verification: Deposix automatically conducts initial verifications of every deposit received; for clients seeking further risk reduction, complementary verification services are available.

Audit trail protection: Deposix will accept, review, time stamp, and document all deposits, thereby creating a secure audit trail of the technology's development.

We ensure that your escrow agreements are done right, with the utmost care, in a quick and efficient manner.

We provide tailor-made Escrow Solutions for

- Licensees
- Developers
- IT and IP Attorneys
- Technology Investors

Do you want to know more about our Risk Management services?
We can help you evaluate whether an escrow agreement would be beneficial for your specific situation. Our standard contracts and a list of references are available upon request.

For further information, please contact:
Katharina.Hertzog@deposix.com

Infanteriestrasse 11a
D-80797 Munich
Tel. +49 (89) 9901-3654

www.deposix.com

Option B

We have all heard about cases in which the financial or other difficulties of a supplier have severely affected the ordering customer. Typical examples often refer to original equipment manufacturers (OEMs) and analyse the supply chains of, for example, the automotive or pharmaceutical industry. In most of these examples, the failure of the supplier of a specific component is critical to the following process chain. The stories typically describe in great detail how long the whole production and output of the OEM were halted for and how this caused huge financial losses. 'That's an old hat,' you might say, 'OEMs have been addressing the issue for a long time. And we all know that commonly promoted risk strategies to avoid such a situation are optimizing inventory management and multi-sourcing'. You are right – as long as it comes to OEMs and physical goods in the production chain. But what about non-physical value chains without the option of stockpiling? Or when the goods are specialized software for which multi-sourcing does not make sense or is not even available? In such a case, software escrow is the solution for all the parties involved. Please read on…

What can go wrong – negative examples and risky situations

Imagine a large licensee like a bank that had commissioned some very complex and important software, eg its central credit-scoring tool, from an external developer. The development, including specifications, all necessary testing, debugging and the international pilots, had been lengthy and costly. Now that the bank is ready to reap the first benefits from its investment, the licensor goes bankrupt owing to some other big project and is wound up. The licensor is therefore no longer able to deliver the agreed maintenance support (continued roll-out, prolonged bug fixing and development of additional functionalities). Even though the bank would have the internal know-how and resources to take over these tasks from the licensor, it does not have the means to do so since it does not own a copy of the underlying software source code. The bank would face the tough decision of either continuing to use its central scoring tool 'as-is', or starting all over again by looking for a new supplier.

In a slightly modified example, a large licensee works closely together with the licensor and has the know-how, resources and a complete copy of the source code plus development environment available. This time, though, the trustee appointed to the licensee under insolvency proceedings intervenes and forbids the usage of the source code by the bank because of a missing licence for continued development. Here the bank would face the option of negotiating from a weak position with the trustee for additional licence fees, to use the software 'as-is' (as above) or to start all over again.

In a further example, a medium-sized fashion company licenses a system for its store management from an external licensor that originally developed the software and also made individual adaptations for the licensee. Then the licensor gets bought

by a main competitor of the fashion company. In addition to the very irritating 'know-how drain' to the competitor, which can now access parts of its particular know-how, the licensee also depends on this competitor to provide future maintenance for its store management system – or else face the known options of 'as-is' usage or starting over again.

As a fourth example, we consider a venture capital (VC) company that has to close down one of its portfolio companies owing to its failure to be economically viable. Nevertheless, the start-up had developed some very valuable software technology, which unfortunately had not been secured. Since the team of developers is upset about the close down and refuses to help the investor further, the source code of the technology is inevitably lost. Any potential partial recovery of the original investment in the start-up by exploiting the technology at hand has gone astray. In an even worse scenario, the team of developers takes along the source code of the VC's technology and founds another company with similar focus that then continues to exploit the market momentum that had been created with the original investor's money. Any attempt by the investor to stop that 'unfriendly' exploitation is doomed to fail owing to a lack of proper documentation of the technology in question.

These examples could be extended easily to various other industries, markets or fields of technology, in particular against the background of the recent economic turmoil, which spilt from the real estate market to banking and subsequently to various other industries. All the instances described above have one thing in common: the risk could have been mitigated significantly or even avoided altogether by using a professional escrow agreement tailored to the specific situation.

What can go right – positive examples and opportunities gained

This time a young and agile but small software development company is challenging a more established competitor. The incumbent's software products are mature and known to work but outdated from a technological point of view and lack leading-edge functionality. The young developer faces the typical concerns of potential licensees on the reliability and financial viability of the company, its current size and a missing track record. At the same time, the licensor strives to protect its leading edge and keeps the technology (ie the source code) tightly locked up. To overcome this seeming conflict of interest, the small software company proactively offers a software escrow agreement along with its licence contracts to all potential customers. This agreement foresees a handover of the source code to the licensees in the event that the licensor defaults on maintenance or any other of its contractual obligations. This way, potential concerns about the size or age of the developer are overcome and the licensor opens up new business opportunities for itself that otherwise would have been unavailable.

In the same example, when shifting the perspective to the licensees, companies in need of software applications open up additional options of potential suppliers for themselves by exactly the same means: an escrow agreement may permit addi-

tional, better-suited opportunities when identifying viable software solutions and suppliers for their various business needs that otherwise would be ruled out because of the concerns mentioned above.

When looking beyond the two parties involved directly in an escrow agreement – the licensor and the licensee – one soon comes across a number of external advisers that may also have a stake in the planned licence transaction: lawyers, consultants, auditors, etc. Any of these professionals could potentially facilitate the deal by suggesting an escrow agreement to either of the two main parties, thereby creating apparent value, which would benefit their own cause and reputation. In other words, having escrow in their professional toolbox helps advisers to create potential new business opportunities for their clients.

Escrow explained

So how exactly can you mitigate certain risks and open up additional business opportunities by using escrow? To gain a better understanding, we will first identify some basics concepts.

Software or technology escrow is a service offered by a trustee or a neutral third party (often a professional escrow agent), who receives, for example, the source code of a software application from its developer and who keeps it in custody for and in the name of the licensee. A source code generally provides access to all the know-how and intelligence incorporated into a given software application. At the same time, the source code is needed to fix any bugs or to develop new functionalities within the software.

The same principle applies for any other form of intellectual property (IP), often of a technical nature, that a licensor strives to protect (ie keep secret) but that a licensee would need, in the event that the licensor defaults on supply or maintenance. Examples for technology escrow would be drawings and diagrams for (and/or samples of) electronic circuit boards, chemical formulae or production processes, or detailed specifications and supplier information for complex machines. For the sake of convenience, for the remainder of this chapter we will stick to the most relevant field of escrow, software applications.

Definition of source code

When programmers design software, they break down a planned new functionality (eg 'adding a new customer record to the bank's central database') by writing a series of specific instructions for the computer. For this, they may use any of the manifold existing programming languages. The result is the so-called source code, and anyone capable of 'reading' it, ie understanding the instructions in that programming language, could extract the specialized know-how and expertise that the programmers put into it (hence the

effort to keep it secret). Next, the programmers 'translate' the source code into machine-readable code called object code. This process is also called 'compilation' and as a result creates the executable programs (so-called '*.exe' files) that run on our computers. For any subsequent change to the software (either bug fixing or the add-on of new functionality), the original source code needs to be modified and the process of compilation repeated. Without the source code, the software running at the licensee's facilities could be used only on an as-is basis.

The licensor strives to protect the IP that went into the software. The typical instruments available for protecting IP, such as copyright protection or patents, have several severe shortcomings for software – among them the fact that the source code needs to be disclosed.[1] The particular know-how – often considered to be the most valuable asset of software companies – could possibly be extracted and reused in a number of creative and legal ways. The result would mean taking unjustifiable risks, with potentially dire implications for the vast majority of all existing developers. Consequently, most licensors will never allow their source code to be disclosed, either to the general public or to specific customers.

So while licensors have every reason to keep their source code secret, what is the position of the customer, the licensee? From the licensee's perspective, risk management is just as crucial. The licensee is a mere user and fully depends on the licensor in order to exploit both the software's immediate benefit and its long-term potential. The issues at hand here are bug fixing, maintenance, and development of new features. Often enough, licensees have to invest up to seven- or eight-digit euro sums in new software and its indispensable implementation process into an existing IT landscape. Typical costs include the regular licence and maintenance fees and further charges for individual adaptations, interface programming, additional or new hardware plus surrounding IT infrastructure, time and effort to analyse and adapt obsolete or incompatible internal business processes, and training for employees. Therefore, licensees have a strong interest in mitigating the risks involved and in protecting their investments in IT in the case of their licensors defaulting on maintenance or other critical deliverables.

Practical guideline: when to use software escrow from the licensee's perspective

Software escrow should be considered when any of the following questions is answered with a 'yes':

Does the software administer or operate with critical processes and/or data? ☐

Would a short-term replacement of the software lead to significant costs?	☐
Can maintenance of the software not be guaranteed 100 per cent?	☐
Is compliance with one's own contractual obligations vis-à-vis customers or partners dependent on the software at hand?	☐
Does the investment in the overall project exceed €50,000?	☐

Considering the different perspectives of licensor and licensee, the inherent conflict of interest between developer and licensee becomes apparent. Whilst the licensor prefers to keep the source code secret and not to disclose it to anyone, the licensee seeks to get hold of the source code as backup for a potential situation in which the licensor defaults on obligations. Both sides have legitimate interests to limit the risks involved for them. However, if both sides insist, they would never sign a licence agreement. The detriment would be loss of potential revenue and reputation for the licensor and abandonment of potential benefits offered by acquiring the functionality of the software for the licensee.

Depending on when, within the buying process, the parties start addressing this conflict of interest, a very costly situation could arise for both parties. The quarrel over the source code has been recorded as an insurmountable stumbling block in more than one case in the past.

Software escrow as the solution to this conflict creates a three-party constellation in which the escrow agent serves as trustee and holds the IP in custody (see Figure 2.6.1 – 'The software escrow triangle'). In contrast to a notary or other legal services firm, which typically serves as trustee in similar situations, the escrow agent has the competency to understand and evaluate the software from a technical point of view. Further, the escrow organization holds the internal processes ready, for example, to accommodate regular updates or the particular safety requirements.

As a vehicle to software escrow, a three-party escrow agreement is put in place, complementing the bilateral licence (or development, or maintenance) contract between licensor and licensee. Based on their expertise and experience, escrow agents typically adapt their standard agreement to the needs of licensor and licensee. Once the specific release conditions – which could trigger the disclosure of the source code to the licensee as beneficiary – are agreed and the escrow agreement is finalized, the software developer hands over the source code to the independent escrow agent. The agent verifies the content from a technical point of view and then transfers it safely into its specialized storage. From that point onwards, the agent ensures the quality and safety of the source code through regular maintenance and adherence to a strict contract management process and provides the licensee with access to the source code in the event that one of the predefined release conditions occurs.

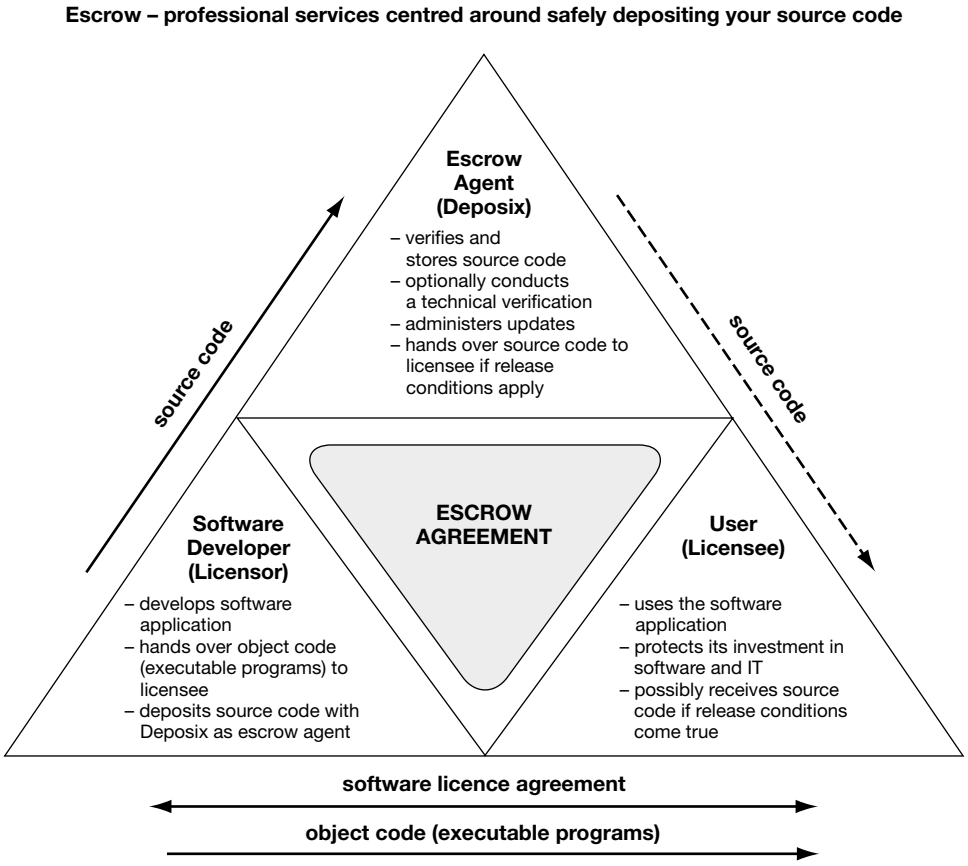


Figure 2.6.1 The software escrow triangle

Six typical release conditions

1. Bankruptcy of the licensor or termination of business activity.
2. Licensor opening a case for insolvency protection.
3. Default on maintenance.
4. Decision to end the life cycle of the software.
5. Loss of critical know-how (key programmers leaving the developer, 'brain drain').
6. Change-of-control clause (eg competitors of licensees taking over the licensor).

Risk and opportunity management with software escrow

The licensee's perspective

A structured analysis of potential risks from a licensee's perspective would have to include a look at its industry and the specific type of technology or software in use. However, on a more abstract level, using a software application critical to its core business exposes the licensee to general IT and operational risks. The most relevant with respect to escrow, as mentioned before, is dependency on the source code and thus the developer. When the licensor defaults on its contractual obligations in support and maintenance, one or several IT systems and the related operational processes are affected. Since we are assuming mission-critical software, this default also implies some specific business or market risk. Related to the first example cited above, the bank's credit-scoring system, the business risk would be the lack of ability to score new credit applications and thus to acquire new business.

Using software escrow would mitigate or eliminate the above-mentioned risks; moreover, it could result in additional business opportunities. With respect to the credit-scoring application in our example, the bank potentially would have had additional options in choosing a supplier. Typical contractor and software selection processes evaluate among other things the standing of suppliers and often look at criteria like size (revenue, number of employees), age, balance sheet total, reference customers or similar factors. These criteria are only so-called secondary criteria, as the goal is always to try to derive a statement about the reliability of the products or services offered by the licensor. By using escrow, the risk of default is mitigated independently of these criteria, and the potential result is an increased solution base from which to choose. In other words, the bank may place more emphasis on factors like functional fit, technological feasibility, level of service offered or price of an application, rather than decide primarily based on size or assumed standing of the supplier.

The licensor's perspective

The licensor's perspective could be presented in a similar way, but as the converse of the licensee's perspective. As discussed before, the owner of an IP such as software has very good reasons for thoroughly protecting the underlying source code, but at the same time cannot ignore the needs and wishes of the (potential) customers for securing their investment in that particular technology and for mitigating the various risk types involved. If licensors did not address these needs, they themselves would face potential reputation and business risks, since customers would possibly look for more suitable alternatives in the market. By using a professionally administered escrow agreement, licensors address their own risks (IP, market, reputation, etc) and open up new business opportunities by appealing to those customers who would otherwise look elsewhere.

The venture capitalist's perspective

VCs or other firms managing their stakes in technology companies are facing certain risks with respect to the IP incorporated in their investment portfolios. Often enough, the technology developed with the support of, or entirely based on, their funding is very volatile and at the same time represents the only tangible asset that exists. If portfolio firms fail for whatever reason, the VCs need to write down investments and bear the associated business risk. If, in cases with existing know-how and IP, these are lost completely and written off to zero, it might severely affect the VCs' reputation in light of their financial backers, the original investors. These investors entrust their money to the VCs, who are responsible for professional asset management. Unnecessary loss of an asset would risk damaging the trust and ability to raise future funds. On the other hand, VCs might open up new business opportunities by securing tangible assets of individual firms with an escrow agreement, since the IP could possible be reused, either by transferring them to other portfolio firms or by selling them off to an external party.

The adviser's perspective

And last but not least, the manifold advisers like lawyers, auditors or other consultants who work for and in the name of the main parties (ie licensors, licensees or investors) could use escrow as one instrument in their expert toolbox. Since many clients by now know about escrow, they might expect the adviser to know about it as well. In any case, professional aides can demonstrate their specialized aptitude to their clients by 'pulling out' and recommending escrow from their toolkit whenever needed, thereby creating additional value. For the lawyer, a typical situation could arise when working on a licence contract or other key agreement – possibly involving IP – for his or her clients. For an auditor, it could arise under any circumstance related to financing or balance sheet optimization or due diligence. For a consultant – depending on the specialization – it could arise under circumstances ranging from giving advice on general risk management to helping with a procurement process (ie a software or supplier selection) to working on hands-on IT implementation. Whenever escrow is mentioned by the adviser, he or she will further his or her own professional reputation, thereby building the grounds for additional assignments in the future.

One final aspect of software escrow that should be mentioned here is based on its general characteristic of reducing risks for its licensees. These beneficiaries – be they normal market participants or investors – often use external financing and specific insurance coverage for their normal conduct of business. The cost of this financing and insurance coverage, among other things, is typically based on a rating or screening of the applying company, and institutions lending money or insuring risks use or compile these in the process. In addition, banks or insurance companies have regulatory requirements like Basel II or Solvency II, which among other things analyse operational risks. All these frameworks try to quantify various different factors with the goal of putting a value (or from an applicant's perspective a price tag) to a potential deal. Naturally, anything that reduces risks will lead to

lower costs. As shown above, software escrow contracts help to reduce various risk types, and therefore users may benefit from reduced costs for financing or insurance coverage where needed.

Tables 2.6.1 and 2.6.2 briefly summarize the potential risk types addressed by software and technology escrow as well as potential business opportunities opened up by using escrow, both distinguishing the different target groups.

Conclusion

The recent worldwide economic downturn caused by the crisis in the real estate market and the banking and financial industry has demonstrated once more in an impressive way that the stability of the overall marketplace, and in particular of individual firms or suppliers, is relative. As always, the proper management of risks and proactively seeking new opportunities are inevitable for protecting assets and securing the long-term survival of any market participant. In this context, this chapter has made the case that software escrow is a valuable tool for both objectives, effective risk management and opening up new business opportunities.

Table 2.6.1 Risk types addressed by software and technology escrow, by potential target group

	Target group			
Risk type addressed	Licensees	Licensors	Investors, VCs	Advisers (lawyers, consultants, auditors, etc)
IT risk	X			
Operational risk	X			
IP risk		X	X	
Business/market risk	X	X	X	X
Reputation risk	X	X	X	X

Table 2.6.2 Potential business opportunities arising from escrow usage, by target group

	Target group			
Additional opportunities gained	Licensees	Licensors	Investors, VCs	Advisers (lawyers, consultants, auditors, etc)
Additional deals/business		X		X
Improved reputation		X	X	X
More business options/suppliers	X			
Improved financial rating	X	X	X	

The key benefits of software or technology escrow for the two main parties to a licence transaction are protecting IP for the licensor and securing investments in IT or other technology for the licensee, thereby mitigating key risks and facilitating deal closure. Further potential beneficiaries are various types of advisers to the two parties (lawyers, consultants, auditors and so on), who improve their own service and professional aptitude and create additional value for their clients, and any kind of investors who may improve the rating and/or exploitation of their portfolio's assets.

Finally, software escrow – which originated in the United States some 30 years ago – is slowly but steadily making its way across Europe and the rest of the globe and is becoming a commonly accepted best practice for business continuity.

Note

1. *Shortcomings of copyright and patent protection for IP in software.* The most intuitive step would be to rely on copyright protection and, in addition, to file a patent for the software. Yet it is not that easy. While copyright protection and patents for software are generally available across most industrialized jurisdictions, typically only certain parts of today's comprehensive applications stand a chance of reaching the intended shelter. Copyright protection protects specific lines of code from being copied. This means that one can take no action against another code written independently that achieves the same effects. Patents for computer-implemented inventions offer a broader protection for a product or process regardless of the software language they are written in. Patents can be obtained generally for novel software-based inventions that, for example, guide a satellite in orbit, or manage more telephone calls through narrower bandwidth, or make a computer run faster through more efficient memory usage. But any competitors who find a different way to achieve the same objective, perhaps even a better way, will not have to explain themselves to the patent holder. Furthermore – and this is true for other forms of tangible IP such as text, music or videos as well – software is an electronic and thus a very volatile good. Nowadays, there are very few physical restrictions on its dissemination. And as often, unfortunately, being right and getting one's rights are two very different animals.

2.7

Corporate manslaughter: the new landscape

Rhys Griffiths, Field Fisher Waterhouse LLP

Introduction

On 23 April 2009, the Crown Prosecution Service brought the first action under the new Corporate Manslaughter and Corporate Homicide Act 2007 when it charged the Gloucester-based company Cotswold Geotechnical Holdings Limited. The charges relate to the death of one of its employees, a junior geologist named Alexander Wright, aged 27, who died on a building site near Stroud, Gloucestershire. The site had been excavated for a survey and, on 5 September 2008, Mr Wright was collecting soil samples in a pit when the sides collapsed and crushed him to death. The company, an engineering consultancy, is charged with corporate manslaughter and for breaching provisions of the Health and Safety at Work Act 1974 (the HSWA 1974). Paul Eaton, a director of the company, is also charged with gross negligence manslaughter and for breaching the HSWA 1974. If found guilty, the company could face an unlimited fine and Mr Eaton could face a sentence of life imprisonment.

When the case comes to trial, it will attract much interest given that it is the first case under the new Act. It will be interesting to see how the new law will be applied in practice and whether it will lead to the predicted increase in prosecutions for corporate manslaughter. This chapter will consider the workings of the

new Act and the steps that all businesses ought to take in order to ensure that they are not susceptible for prosecution under the new Act.

Why the Act has been introduced

The old law of corporate manslaughter was such that it could not be used successfully to prosecute large organizations. This was much publicized by the collapse of the corporate manslaughter prosecution of P&O European Ferries following the Zeebrugge ferry disaster in 1987 and, more recently, by the collapse of various corporate manslaughter prosecutions following rail disasters such as the case against Balfour Beatty following the Hatfield train disaster of 17 October 2000.

The inadequacy of the old law led to Parliament enacting the new Corporate Manslaughter and Corporate Homicide Act, which came into force on 6 April 2008. The Act abolishes the old law and creates a new offence of corporate manslaughter. It is said to be designed to secure, in a wider range of cases, a conviction for a specific, serious criminal offence that properly reflects the gravity and consequences of the conduct involved. It is intended to be an additional means of enforcement by the authorities of proper health and safety standards, and so organizations may still be prosecuted for breaches of health and safety laws as an alternative, or in addition, to the new offence.

The old law provided that a company would be guilty of corporate manslaughter if its 'directing mind' had been grossly negligent and that had caused a person's death (known as the 'identification principle'). For the purposes of the old law, the 'directing mind' was typically a director or senior manager and so only if he or she was liable of gross negligence manslaughter would the company also be liable.

The old law resulted in only six convictions of small organizations in a 13-year period. This is because it was always impossible to find an individual of sufficient seniority to have been grossly negligent. Large companies tend to have complex management structures, whose directors and senior management are not typically involved in the health and safety decision making that caused the death. Indeed, the old law effectively encouraged the delegation of health and safety duties away from the board in an effort to remove the possibility of a 'directing mind' being grossly negligent in respect of those duties. As Mr Justice Scott Baker put it so forcefully in his judgment in the case concerning the 1997 Southall train crash:

> There are many who say that the present state of the law is unsatisfactory and that the present obstacle to prosecuting large corporations for manslaughter should be removed. However, if the law is to be changed it is up to Parliament to do so. The Law Commission recommended legislation over three years ago but nothing has been forthcoming. There is little purpose in the Law Commission making recommendations if they are to be allowed to lie for years on a shelf gathering dust.

The new offence of corporate manslaughter

The new offence abolishes the identification principle and moves liability away from individual fault to a more global view of how the organization has arranged itself. An organization will be guilty of the new offence if the way in which its activities are managed or organized: 1) amounts to a gross breach of a relevant duty of care owed by the organization to the deceased; and 2) that causes a person's death. However, there remains a residual element of the identification principle because, in order to secure a conviction, the prosecution must also prove that the way in which the organization's activities were managed or organized by its senior management was a substantial element in the failure described above. These elements of the offence are explored in more detail below.

The Act applies to companies, local authorities, specified public bodies, police forces, and partnerships, trade unions or employers' associations that are also employers. The new offence will not apply to individuals, and neither does the Act create any other new form of individual liability. However, it is important to note that an individual may still be guilty of individual manslaughter if he or she has acted in a way that amounts to gross negligence.

Trial will be by jury. If found guilty, an organization may be subject to:

1. an unlimited fine;
2. a remedial order; and/or
3. a publicity order.

The government is in the process of drawing up guidelines for punishment under the new Act but, in its initial consultation, it made clear that it thought the starting level for a fine ought to be 5 per cent of the organization's turnover. If there were mitigating factors then the recommendation was that the fine should be decreased to 2.5 per cent of turnover, whilst if there were aggravating factors then the recommendation was that the fine ought to increase to around 10 per cent of turnover. Clearly, therefore, the Act will have some bite.

The remedial order is, as it suggests, an order by the court to compel an organization to remedy a particular failing within its administration. This is aimed at 'correcting' a failure in an organization's health and safety system so as to ensure that there are no more fatalities caused by that same failure.

Finally, the publicity order will enable the court to compel an organization to publicize details about the conviction, including a full account of the facts of the fatality and also the sentence received. In many ways, this could prove to be more damaging for the organization than any fine imposed. This part of the Act is not yet in force, pending further consultation as to how it will be applied.

Although no doubt obvious, it must be stressed that the new Act creates a criminal offence; to be found guilty means punishment – the rationale of orders against an organization found guilty is not to compensate those affected but to use punishment as a deterrent.

The first stage: a gross breach of a relevant duty of care?

The first stage of the offence requires a finding that the organization has managed or organized its activities in a way that amounts to a gross breach of a duty of care owed by the organization to the deceased. There are two elements to this. Firstly, the organization must have owed one of the following duties of care to the deceased under the ordinary law of negligence:

1. a duty as an employer;
2. a duty as occupier of premises; or
3. a duty owed in connection with the supply of goods and services, the carrying on of construction or maintenance operations, the carrying on of any other activity on a commercial basis, or the use or keeping of any plant, vehicle or other thing.

The second element of this stage of the offence is that the breach of the duty of care must be gross, that is, conduct that falls far below what can reasonably be expected of the organization in the circumstances. In order to decide this question, the jury may consider any relevant matter, but in particular they must consider whether the organization has failed to comply with any health and safety legislation, the seriousness of that failure and how much of a risk of death that failure posed. The jury may also consider the safety culture of the organization and whether that is likely to have encouraged the failure to comply with, or a tolerance of the breach of, health and safety legislation. The jury may also consider any health and safety guidance issued by a responsible body that relates to the alleged breach.

The second stage: the senior managers

The new offence also includes a requirement that the way in which the organization was managed or organized by the senior management was a substantial element in the breach of the duty of care by the organization. So who are the senior management? The Act provides that the senior management are those who play significant roles in: 1) the making of decisions about how the whole or a substantial part of the organization's activities are to be managed or organized; or 2) the actual managing or organizing of the whole or a substantial part of those activities. Essentially, both strategic and operational managers will be considered to be senior managers. This very much links into the importance that the new Act places upon 'the safety culture' within an organization.

The principal aim of the new Act is to focus liability on the systems of work adopted by the organization and to move away from individual fault, which was why the old law could not be applied to large organizations. Nevertheless, there remains the need to prove some fault on the part of senior management, because their conduct must have been a substantial element in the gross breach of the duty

of care by the organization. As Gerry Sutcliffe, Parliamentary Under-Secretary of State for the Home Office, said during a Standing Committee debate, 'the question will be whether the organization overall was negligent, and it is difficult to see how the organization overall could be guilty if the senior management were diligent in their approach to health and safety'.

Ramifications of the new Act

There will undoubtedly be more corporate manslaughter convictions under the new Act. Previous cases, such as the prosecution against P&O European Ferries, failed because of the impossibility of finding a 'directing mind' with the requisite degree of culpability, despite the organization as a whole having been described in Lord Justice Sheen's inquiry as having a 'disease of sloppiness'. The new Act is intended to secure convictions in such cases, as its focus is on the management and organization of the organization as a whole, which will directly involve analysing how the board has managed or organized those activities given that it is ultimately responsible for the administration of the organization.

An indication of the potential increase in prosecutions under the new law is given by Michael Welham in his book *Corporate Killing*.[1] In 2000, the Health and Safety Executive (HSE) evaluated the number of potential corporate killing cases under the new draft bill (as it then was). It reviewed 52 cases that were prosecuted by the HSE between 1996 and 1998 and assessed whether, if the Act had been in force at that time, the cases would have been submitted for prosecution for corporate manslaughter. Of the 52 cases reviewed, the HSE concluded that 21 would have been elevated from health and safety charges to corporate manslaughter charges.

How to prepare for the new Act

All organizations can and should take action to minimize the risk of liability under the new Act. This is particularly crucial because of the stringent punishments likely to be imposed by the courts following conviction. The modern approach to safety is well illustrated by the following extract from the Baker report, which was produced following the tragic accident at BP's Texas City refinery in March 2005, which resulted in 15 deaths and more than 170 injuries: 'A positive safety culture is important for good process safety performance… leadership from the top of the company, starting with the Board and going down, is essential.'

The new law will reflect the Baker report, as its focus is on failures by the organization to manage or organize itself properly. The individuals who have responsibility for such management and organization are the board, and so it is imperative that safety systems and cultures are board driven. A full board member must be given responsibility for safety, which should be a standing item at all board meetings. The relevant board member must seek to ensure that the organization has in place robust health and safety systems. In particular, he or she ought to

be considering the effectiveness of the organization's systems for identifying and managing risks to its employees and individuals not in its employment. Such systems must be in writing and reviewed at appropriate intervals. Moreover, the board member ought to receive direct reports of safety concerns, which should then be given high priority. Essentially, the following issues ought to be addressed and reviewed in a systematic way:

- How effective are your health and safety systems?
- Are you taking all reasonably practicable steps to reduce the risk of accidents?
- Are your systems rigorously followed or are breaches tolerated?
- Are you complying with all health and safety legislation that is relevant to your organization?
- What are the health and safety attitudes, policies, systems or accepted practices within your organization?
- Who are your senior management?
- In addition, whilst not a preventative step, one should ensure that your insurance cover will meet the defence costs of a corporate manslaughter prosecution.

Whilst these questions may be difficult and time-consuming to answer, there will be a huge desire to make the Corporate Manslaughter Act work and to secure convictions where the old law failed to do so. A full and proper consideration of the issues set out above will minimize the risk of accidents and also liability under the new Act following such accidents. Now is the time for action.

Note

1. M Welham (2002) *Corporate Killing*, Tolley, Devizes.

2.8

Conducting internal investigations

Alexandra Underwood, Field Fisher Waterhouse LLP

Introduction

If you have a suspicion that a colleague or employee is engaged in unlawful or improper practices, it is human nature to want to find out whether your suspicion is well founded and to investigate. In some cases, directors may also have a duty to investigate suspicious circumstances or behaviours in order to comply with their obligations under the Companies Act 2006 or the requirements of the company's regulator.

The investigation is an information- and evidence-gathering exercise, which will inform your decisions on how to take matters forward and what further steps need to be taken to protect the assets of the company. The assets in question might be intangible, such as the reputation of the company, or physical assets, such as the money in the company's bank account. In either case, the information obtained in the course of the investigation may be used to rectify the asset position, to identify areas in the risk controls that need to be improved to prevent similar problems arising in the future or simply to punish the wrongdoers and obtain financial compensation for loss suffered by the company. Often the objective may not be clear until interim or final conclusions have been reached, but, whatever the objective or objectives, some care is needed in the conduct of the investigation not only

to avoid the pitfalls that lie in the way of an investigator but also to ensure that the product of the investigation can be used in the way that was envisaged when it was begun.

Duties to investigate

A director of a company has a duty under section 172 of the Companies Act 2006 to act in a way that he or she considers promotes the success of the company for the benefit of its members having regard to (amongst other things): 1) the long-term consequences of any decision; and 2) the desirability of the company maintaining high standards of business conduct.

Considering these factors, there is an argument that a failure to exercise zero tolerance on certain behaviours that harm the company in the long term may amount to a breach by directors of their duties to the company. For example, if directors were to turn a blind eye to an instance of fraud they may breach more than their duty to protect the assets of the company. They may have contributed to the creation of a culture that will have long-term consequences for the company and for society as a whole. For this reason, it is suggested that directors have a duty to take reasonable steps for the prevention and detection of fraud and should exercise zero tolerance when instances of fraud are detected.

Further, there may be a duty to report suspicions of fraud under the Proceeds of Crime Act (POCA). Under POCA a failure to report a suspicion of money laundering in the regulated sector carries a sanction of up to five years in prison or a fine. A suspicion may be defined as a possibility that is more than fanciful that the relevant facts exist.

Similarly, directors must not turn a blind eye to regulatory breaches by employees, because to do so would expose the company to sanction by the regulator and risk the company's reputation. In the case of companies operating in the financial services market there is a general duty on the company and on the authorized persons within the company to report breaches of certain principles set out in the Financial Services and Markets Act 2000 to the Financial Services Authority (FSA).

Where an employer suspects an employee of misconduct it will need to substantiate its suspicion by carrying out an investigation before confronting the employee with the evidence obtained. The investigation must comply with the principles of fairness set out in the Employee Relations Act 1996, case law relating to unfair dismissal and the ACAS Code of Conduct on Disciplinary and Grievance Procedures. The requirement for an investigation to take place prior to any disciplinary action is critical if an employer is to ensure it does not fall foul of either the Burchell principles or the ACAS Code. The case of British Home Stores Limited *v* Burchell [1978] IRLR 379 is authority for the principle that, to establish fairness in a conduct dismissal case, an employer must be able to establish that, at the time of dismissal, it had a reasonable belief in the employee's guilt based on a reasonable amount of investigation.

In the employment context, it will often be the case that, during the investigation, perfectly plausible explanations emerge and the disciplinary process is discon-

tinued without a hearing. This is why it is of vital importance that, even in cases of apparently 'obvious guilt', the employer should always investigate rather than launch straight into a disciplinary hearing or (worse) go straight to dismissal.

Common pitfalls

Many investigations will by their nature need to be carried out in secret. In disciplinary proceedings secrecy is required to ensure that the investigation itself does not damage the reputation of the individual under investigation and amount to a constructive dismissal. In cases where you are investigating a potential fraud the element of surprise is required to ensure that the fraudster does not have the opportunity to dissipate assets obtained by fraudulent means or with the proceeds of fraud. An investigation may also need to be conducted in secret to prevent the destruction of evidence by those involved in the wrongdoing.

Monitoring

Investigations can involve the surreptitious monitoring of communications including e-mails and telephone calls, and it is important that this activity is carried out in accordance with the law. The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the monitoring if it involves the 'interception of a communication in the course of transmission'. Examples of the types of monitoring systems that will be caught include the recording of telephone conversations and systems that block e-mails and make some of the content (for example, an offending phrase) available to another person. It is generally accepted that opening e-mails that have already been opened by the intended recipient will not constitute an interception under RIPA. RIPA criminalizes the interception of telephone calls and e-mails without a warrant. However, communications can be lawfully intercepted under RIPA by obtaining consent. Section 3(1) of RIPA provides that the lawful interception of communications can take place if the interceptor has reasonable grounds for believing that both the sender and the recipient have consented to the interception.

Employers should ensure that contracts of employment and internet use policies contain a clause providing the required consent to monitor all communications. This will facilitate the investigation by permitting the employer to monitor internal e-mails and telephone exchanges. However, it is more problematic to monitor telephone calls and e-mails with the outside world, where it will be difficult for the employer to show that it has reasonable grounds to believe that both the sender and the recipient have consented to the interception. If the business of the company is predominantly conducted over the telephone, the company should consider putting in place a recorded message to the caller informing him or her that the telephone call may be monitored. E-mail exchanges may be monitored if the foot of company e-mails informs the recipient that continued communication by e-mail will be taken as consent to monitoring.

The effect of RIPA is ameliorated by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. The Telecommunications Regulations, as they are commonly known, provide for circumstances where, in a business context, it is lawful to intercept communications without consent.

To establish the existence of facts relevant to the business, businesses may monitor or record communications without consent in order to:

- ascertain compliance with the regulatory or self-regulatory practices or procedures relevant to the business;
- ascertain or demonstrate standards that are or ought to be achieved by means of persons using the system;
- prevent or detect crime;
- investigate or detect the unauthorized use of the telecommunications system;
- ensure the effective operation of the system.

Regulation 3, Telecommunications Regulations

The Telecommunications Regulations also authorize businesses to monitor but not record without consent for the purposes of: 1) determining whether the communications are relevant to the business; and 2) monitoring communications to a confidential anonymous counselling or support helpline (Regulation 3, Telecommunications Regulations).

The apparently broad grounds for lawful interception without consent are restricted by the requirement that the interception must be effected solely for the purposes of monitoring (or keeping a record of) communications that are relevant to the business as defined in Regulation 2(6), Telecommunications Regulations.

The Supplementary Guidance distinguishes between monitoring that is carried out partly to gain access to the contents of personal communications that do not relate to the business (which is not allowed) and monitoring that only incidentally and unavoidably involves access to personal communications (which is allowed). RIPA on the other hand provides justification for the interception based on the contents of the communication, which begs the question of how the employer will know for sure until it has opened the e-mail or listened to the telephone call whether it is entitled to do so.

In light of this limitation, the best advice to employers is that they should err on the side of caution. If an e-mail is clearly personal do not open it without very good reason. An example of such a reason would be where the employer suspected that a criminal offence had been, or was being, committed.

To take advantage of the Telecommunications Regulations, the employer must also have made all reasonable efforts to inform all parties who may use the telecommunications system that interception may take place (Regulation 3(2), Telecommunications Regulations). Again, it is particularly important to ensure that information is given to third parties (for example, within an e-mail disclaimer) as well as to workers themselves (in an electronic communications policy).

Tipping off

With all covert investigations it is important not to tip off the suspected wrongdoer. If the subject becomes aware of an ongoing investigation, there is a real risk that valuable evidence will be destroyed or made more difficult to uncover and that assets will be dissipated. Tipping off may occur simply by moving papers on a subject's desk or disturbing some item of furniture or by leaving a trace on someone's computer that shows that their files have been accessed by someone other than themselves. When conducting a search of someone's office it is sensible to take photographs of the room before anything is moved so that everything can be put back in the right place at the end of the search. It is also a good idea to employ a specialist locksmith who can access locked filing cabinets and drawers without breaking the locks. Ideally, investigations of this nature should be conducted under the supervision of an independent expert investigator who will carefully record the source of any evidence found and preserve the evidence in sealed bags, which show how the evidence has been dealt with since it was recovered. If the investigation leads to a criminal prosecution, the integrity of the evidence will be essential if it is to be used as evidence in the proceedings.

It is also possible for evidence to be destroyed for ever if the investigation is not carried out carefully and by individuals who know what they are doing. For example, a well-meaning IT technician may be able to access and review the subject's e-mails remotely but in the process of reviewing the e-mails may destroy important metadata stored on the electronic file. Such metadata will include the date when the file was last accessed or modified. Once lost, this information may never be recovered. For this reason, we suggest that, if you want to examine a subject's computer as part of an investigation, you employ an expert in computer forensics who can take a mirror image of the data on a computer hard drive without disturbing the data held on the computer in any way. The forensic expert can also help you review the data recovered with the use of a filtering system and list of agreed key words. Again, the integrity of the data recovered by a forensic specialist should enable you to use the data in both civil and criminal proceedings if required.

Reputational damage to the subject of the investigation

It is important to remain conscious in the course of an investigation that your suspicions of fraudulent or wrongful activity may be unfounded, or that one or more of the suspected offenders may be innocent. It is therefore essential that you do not do anything in the course of the investigation that might lead to a claim from an employee in an employment tribunal for constructive dismissal. To avoid such a claim you should be careful not to make allegations against individuals in the course of your investigation that cannot be substantiated by evidence. You should keep to a minimum those who are aware of the investigation and the suspicion that a particular employee may be involved.

The Data Protection Act 1998

No chapter on internal investigations would be complete without a reference to the provisions of the Data Protection Act 1998 (DPA), but equally the provisions and interpretation of the Act could and do fill entire tomes. There is a limit to the amount that can usefully be covered in this chapter. Consequently, we do not attempt to provide a comprehensive summary of the relevant principles. Instead, we highlight some of the key provisions of the DPA to give you an idea of the issues you should consider when conducting an investigation.

The DPA applies to the 'processing' of 'personal data', both of which are very widely defined. This means that practically any business operating in the UK that holds information about individuals, whether employees, customers or anyone else, is affected by the DPA. Further, since breach of data protection laws can result in criminal as well as civil liability, not to mention adverse publicity, which increasingly is the likely result of non-compliance, no organization can afford to ignore its data protection obligations.

Not only does the DPA apply to many different types of data and a wide range of processing activities, but it also imposes a number of stringent obligations on data controllers to ensure that data is processed properly. This is because it is recognized that improper use of data can have a serious adverse effect on the life of the individual concerned.

In order to process data in compliance with the DPA, you have to establish one of the preconditions to legitimate processing. The Act lists certain conditions under Schedule 2 for the processing of personal data and sensitive personal data. Personal information is considered to be fairly processed only if at least one of the six conditions is met. One of the conditions for the processing of any personal data is that the data subject has given his or her consent to the processing.

Companies should have in place policies and employment terms and conditions or manuals that establish consent to processing of all e-mails and other data sources on the company's systems for the purposes of investigations for fraud detection and prevention, regulatory compliance and disciplinary purposes. But be aware that the Information Commissioner has a general distaste (as evidenced in his Guidance) to consent forming the only basis of processing. He prefers entities to establish a further distinct basis. This may be because consent can be contrived, not informed, and may be withdrawn.

In order to process sensitive personal data, the Act requires that, in addition to satisfying one of the ordinary processing conditions in Schedule 2, the data controller must also fulfil one of the extra conditions in Schedule 3 to the Act.

Paragraph 6 of Schedule 3 establishes data processing 'necessary for the purposes of establishing, exercising or defending legal rights' as a valid purpose enabling data controllers to process 'sensitive personal data', which includes data concerning the subject's commission or alleged commission of an offence. You will need to consider with your advisers whether there is a strong argument that the investigation you are conducting is a necessary element of 'defending legal rights'.

The Data Protection (Processing of Sensitive Personal Data) Order 2000 adds further clarification by allowing processing that:

- is in the substantial public interest;
- is necessary for the purposes of the prevention or detection of any unlawful act (or failure to act); and
- must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.

It is important to consider data protection issues carefully and to take advice from your lawyers. The Act does allow scope for the processing of data in a properly constructed investigation when there is a genuine suspicion of fraud or regulatory breaches.

Blagging

Companies cannot be blasé about the source of the information that they may receive in the course of an investigation. They certainly cannot say that they don't want to know about the means by which it was obtained. Indeed it is strongly arguable that there is a positive obligation to give clear instructions and remain vigilant.

Section 55 of the DPA makes it a criminal offence knowingly or recklessly to obtain, disclose or procure the disclosure of personal data or information without the consent of the data controller.

In the event that you or your lawyer instructs an enquiry agent it is essential that it is made clear to the agent that his or her investigations must be carried out in compliance with the law. There is nothing in section 55(1) of the Act that limits liability for an offence to persons who obtain personal data or information directly from the source. Therefore, persons who obtain the information along a chain of transfer of data or who might ultimately benefit from obtaining it are also liable. Breach of section 55 is a criminal offence.

The risk to you of instructing the investigators who breach section 55 of the DPA are clear and were highlighted in the case of Hughes *v* Carratu International Plc [2006] EWHC 1791 (QB). First, there will be a considerable risk of serious embarrassment in having to explain why the enquiry agent's illegal actions have exposed the company to a messy investigation about breaches of the DPA, with the risk of criminal liability. Second, there will be an equal risk of embarrassment (at the very least) in any criminal prosecution if the victim of the illegal investigation applies to exclude all the evidence obtained by the enquiry agents, even legitimately, to avoid polluting the court with either directly tainted evidence or evidence that may have been obtained as a result of a 'chain of enquiry' from tainted evidence. Civil courts tend to be more relaxed in that there is no doctrine about fruits of the poison tree, but illegally obtained evidence is still not admissible and will attract severe criticism from a judge.

Another lesson is to be learnt from the case of Dubai Aluminium Co Ltd *v* Al Alawi & Ors. Normally, evidence obtained for the purposes of litigation attracts

legal professional privilege. However, in this case, the judge held that criminal and fraudulent conduct for the purposes of acquiring evidence in or for litigation resulted in any documents generated by or reporting on such conduct that were relevant to the issues in the case falling outside the legitimate area of legal professional privilege, and therefore they could be inspected by the other party.

Conclusion

If an investigation is poorly managed it can result in the loss of evidence, the dissipation of assets, the loss of privilege and even criminal liability. It is important to get it right, and therefore we conclude this chapter with some top tips for managing the risk associated with conducting an investigation:

- Assemble the investigation team and consider carefully who will need to be involved in the investigation, including human resources and a senior decision maker.
- Consider including expert advisers in the team from the outset, including investigators and lawyers.
- Use your expert advisers to preserve evidence and assist you with interviewing witnesses.
- Have in place an agreed communications strategy for when the investigation comes out into the open. This will minimize speculation and gossip, which can be harmful to the company's reputation.

3

Defining and Managing Intellectual Property Risks

Patents
Utility Models
Designs
Trademarks
Domain names
Legal
IPR strategies
Search and watch services

www.berggren.fi

Tampereen Patenttitoimisto is a member of The Berggren Group which is a leading intellectual property agency in Finland. We offer high-quality and individual services in all domestic and international IPR matters, with a strong expertise in European issues. Our experts are at your service in patent, trademark and design matters as well as IP strategy analysis and planning, litigation and infringement cases. Our experience and business development provide a winning combination of depth of knowledge and breadth of service models which can be tailored to any requirements and operational structures you may have.

TAMPEREEN PATENTTITOIMISTO

TURUN PATENTTITOIMISTO

BERGGREN

3.1

Risky patents

Kim Simelius, Tampereen Patenttitoimisto Oy

Patents are a form of intellectual gamble, where a game may last a decade and novices may end up having their company as the stake against their will. Everyone knows gambling is risky – but equally well some skill in playing the game may help in reducing the risk and improving the probability of a good outcome. Playing the patent game requires a lot of skill in different areas, and as with a game of cards you can never know which card will come up next. Or can you?

There are different kinds of risks in patents. Some relate to applying for and owning patents, as patents may have a very different value depending on a number of things. Some of the risks relate to development of technology and even the development of society. There are different kinds of risks arising from the fact that other companies typically own patents that may be relevant to the products of your own company. Most of the patent risks are dependent on time and place. The risk related to a patent application that has just been filed is different in nature from the risk related to a mature patent that was granted years earlier. Patents are national rights, so the risks are also dependent on the country where you look at the situation.

In such a complex setting, it is clear that striking a balance between risks related to patents and the ability to manage that risk is not an easy task. So let us look at the cards in this game!

Risks in creating patents

Companies apply for patents and own a portfolio of patents for many reasons. Some companies have a so-called defensive portfolio that typically has resulted from patenting inventions made by the R&D department. Somewhat later, as the company considers using the patent asset, it becomes necessary to own patents that other companies need. An extreme end to this development is companies that concentrate on owning and extracting value from patents.

The risks in applying for a patent start right from the point when there is an invention. The invention may look very promising in terms of patent value, but in fact it may be already known or even turn out to be technologically of low value. Owing to the vast amount of information related to every technology, filing patent applications for already known or technologically low-value inventions is commonplace. In this sense, investing in patent filing carries a high risk.

When the patent application for an invention is filed, a long and costly journey towards a valuable patent begins. On this journey, it is possible to make various mistakes in prosecuting the application towards a patent. One may give in too easily to the arguments of a patent examiner, and end up with a patent having a very narrow scope of protection that nobody will ever infringe. On the other hand, it is possible, and in some technical areas even likely, that the granted patent has a scope that is too wide in light of existing prior art that was missed in the examination. Such patents may not stand in court, or they may fall in an opposition procedure after the grant. During prosecution, the scope of the patent application may change away from the original technical idea. Planning and managing the investment of possibly tens of thousands of euros per patent family thus become important, as well as using the right partners, who understand the technology thoroughly.

Following the developments in business and technology closely is crucial in ensuring the value of the patent portfolio. It often happens that a company files patent applications on those technologies that it develops itself, but fails to see that the resulting patents are not relevant for the mainstream technology. The opposite is also possible, especially under financial pressure: to avoid cost, a company may abandon patents and patent applications too early before they become relevant for a highly popular technology. To make things even more difficult, the fact that patents are national rights requires the company to predict the development of business and technology in different countries over a span of 20 years. Failure to have patents in the right countries can happen very easily.

Even after the grant of a patent, things can go wrong. Owing to the complexity of technology or the lack of understanding of the patent portfolio, a company may not find customers for its patents and technology. This may happen merely because of a lack of resources or skill in finding the customer. Even a change in the political environment and the local laws may affect the value of patents, owing to their long lifetime of 20 years. Extracting the value from patents requires a lot of skill.

Owning patents is definitely a gamble – and jokers come along rarely. It is therefore understandable that a company, having developed a risky asset, will want a return on the investment by using the patents against other companies.

Risks from patents of other companies

It greatly helps to know who owns the patents that may be a threat to your business. It is of little use worrying about the thousands of patents that are out there unless you know whether they are truly relevant and whether the owner of the patents is ready and willing to use them against you. As with the company's own patents, there are many uncertainties related to patents owned by others.

There are different kinds of harm that patents of other companies can cause, and different ways of ending up in harm's way. At the least, patents can take time to analyse, and knowledge of and concern about patents may slow down development of new products. In a more serious setting, it may become necessary to make changes to products or even stop selling potentially infringing goods. Ultimately, a court of law may order an injunction and may award significant damages to the patent owner.

Since the risks from infringing other companies' patents can be significant, it is necessary to understand these risks and also be able to avoid and manage them. Reacting to materialized risks needs to be driven in a systematic manner as well.

There are different aspects to the risk from patents owned by others. Obviously, the quality of the patents affects the risk greatly: poor patents are not likely to hold up in court and therefore are of little risk other than nuisance. The aggregation of patents into patent portfolios is another aspect. It is more difficult to remove a threat from a portfolio of 10 patents than it is to fight off a single patent.

Yet another fundamental aspect of patent risk is the technology it relates to. Some technologies are simpler than others in terms of detecting infringement, and in some technologies avoiding infringement may be relatively easy while in others it is close to impossible or may take a very long time.

The quality, portfolio and technology aspects of patent risk are more or less static and fairly objective factors. The aspects relating to the ownership of the patents and the countries that are in question can be highly dynamic and unpredictable factors.

Sometimes the owner of the patents that are relevant to the business is a company that is completely unaware of the relevance of the patents or even the existence of your company. In such a situation, the patent risk is minimal. At other times, the owner may be a company that is highly litigious and will seek compensation for any possible use of its patent rights. Naturally, the risk from the patents of the aggressive company is significant, almost regardless of the true value of the patents.

The relationship between companies also affects patent risk. The patent owner may be a competitor, or it may be in an adjacent field of business. A complicated situation may arise when the owner of the patents is a customer or a supplier, or there exists some other business relationship between the companies.

Some unpredictability comes from the country aspect: different countries may have very different legal proceedings, and the legal system may or may not favour a domestic patent owner. Naturally, language is one aspect of the country factor. How's your Chinese?

Developing and using technology are definitely a gamble, and having an ace up your sleeve is often welcome. An ace can be up-to-date knowledge, or it can be excellent ability to mitigate risks.

Managing risks related to patents

Having valid knowledge of the patent landscape and what exists already is key to being able to manage the risks related to patents. It helps both in steering the patent investment and in dealing with the risks from other companies' patents.

In patent filing, there should be no file-and-forget attitude. The reasoning why a patent application is filed needs to be solid and it needs to stay with the patent application throughout its lifetime. The prosecution of a patent application into a patent needs to be carried out by people who thoroughly understand the technology related to the patent application. In addition to good knowledge of individual patents, the management of the whole patent portfolio needs to be executed on the basis of the business needs of the company in a strategic manner.

In reducing the risk from other companies' patents, tracking what the other companies are doing regarding their patents is absolutely necessary. The companies that could pose a risk need to be identified, and the threat from these companies then needs to be mitigated. When surprises happen, dealing with issues quickly and decisively is often the winning strategy. At the heart of successful patent risk mitigation are two things: understanding the technology and understanding the business. What is most important, however, is choosing the right tools, eg avoiding a single patent, getting a licence and developing one's own portfolio of patents have different characteristics in respect of the time it takes to employ them and the different risks against which they work. A company needs to be in a good long-term position by having a solid patent portfolio, and it needs to have an agile capability to defend against other companies.

Not owning patents or ignoring the risk from other companies' patents is definitely a gamble. It's like cheating in a card game and not being ready to get caught.

Summary

Everything related to patents is risky, whether you create patents, own patents or defend yourself against patents by others. Understanding the nature of the different risks and knowing the facts are necessary for safer business. Or would you like to gamble?

3.2

Managing through the downturn: intellectual property optimization

Matthew Hogg, Liberty International Underwriters and Fredrik Motzfeldt, Marsh Ltd

Introduction

Businesses worldwide have struggled as the global economy has gone nowhere fast. Commodity prices are comparatively low, unemployment figures have been setting records and there has been a global contraction in trade as a result of the financial crisis. In unprecedented times such as these, where property values have fallen, interest rates shrivelled and retail price indexes have dived below zero, not all are optimistic of 'green shoots'. The financial powerhouses are still showing caution in their release of capital to struggling companies, which might also enable the speculative purchases that could enhance shareholder value.

All of this is undoubtedly bad news for companies that carry too much debt and have weak business models, as evidenced by the recent bankruptcy of hundreds of companies across Europe. But what impact will the recession have on well-managed companies with sound finances? Can they remain resilient, and emerge from the downturn with their human and capital resources in place to enable growth in the future?

Most will seek to ride out the storm by reducing costs to protect their bottom line. This response is sound, but it would be wise to avoid rushing into decisions about where and when to make cuts. It would also be wise to re-examine the strengths and weaknesses of a company in order to press home any competitive advantage and maximize revenue opportunities. Many companies own assets that they have not had valued, leveraged or fully exploited. Nor are the exclusive rights to these assets enforced in a systematic way. These assets are a company's intellectual property (IP).

Intellectual property in a downturn

Intellectual property encompasses an array of creations of the mind. Whether such creations are truly 'intellectual' is often up for debate, although predominantly, and not exclusively, such creations have a commercial value. Intellectual property rights (IPR) are national rights, often directed by regional or global regulation. They exist to harness the economic value and progressive understanding of intellectual property for the good of society at large, and to encourage further development through the provision of personal property rights, granted to the creators, so enabling them potentially to profit from their efforts. Intellectual property rights are predominant in all major economies and include patents, trademarks and copyrights amongst others.

Intellectual property is significantly affected by the state of the economy. As with other assets, where cash is in short supply the value of IP can depreciate. If market principles are to be applied to the valuation of IP then clearly there are fewer buyers, with less expendable cash to splash on such assets. Likewise, as market demand leads to price cutting of products and services so the component parts of such, including the IP, are pared back in value.

It is also easy to see how market conditions can lead to less R&D expenditure when companies reduce on expenses that do not see immediate returns on investment. IP development and innovation can then often be cut or ceased entirely. The cutting of costs can also see a reduction in applications for intellectual property rights to governmental bodies. History has shown deterioration in the demand for IPR in times of depression or recession. In the United States, during the Great Depression, it was calculated that patent applications declined by 37 per cent between 1929 and 1933 and did not recover completely until 1965, despite the industrial drive of the war periods.[1]

Interestingly, unusual patterns can already be seen from the impact of the current global recession. The World Intellectual Property Organization in analysing patent applications has seen a general decline overall, with countries such as the United States (14 per cent), the UK (12 per cent) and Japan (15 per cent) showing a decline in 2008, although some countries appear to be bucking the trend, eg China has a 19 per cent increase.[2] Sectoral impacts are also likely to be seen if one were to contrast the financial health of the automotive industry to that of the pharmaceutical industry at present, both being heavy patent filers.

Yet experience has also shown, importantly, that some companies pay heed to the importance of intellectual property rights in such times.[3] As property rights, IPRs can be traded, licensed, monetized and otherwise exploited, with the ability to capture extremely valuable revenue streams. In economic downturns there is often seen a latent increase in the amount of IP litigation between companies that are fighting over the potential revenue streams attached to such IP and its control of their market, or to ascertain a level playing field for competition. With everyone struggling to obtain their budgeted revenue figures and market share, tolerance of others' transgression of money-spinning assets is reduced.

Recent research from a leading law firm suggested that more than one-third of the world's leading IP-owning companies (38 per cent) have indicated an increased willingness to take competitors to court in a bid to protect their IP rights during the downturn. Also 30 per cent of companies will increase their use of IP assets in the current economic climate, for example through measures such as licensing and joint ventures.[4] Similarly, a recent report on risk in the communications, media and technology sector showed 30 per cent of participants believing that risks associated with IP will be significant throughout 2009 and 2010.[5]

Intellectual property forms a critical component in the value proposition of a company. It is often a key differentiator that brings customers to the business in addition to providing efficiencies in manufacturing or providing services. Whilst rarely considered in great detail from a risk management perspective, it is a critical element to the success of the company, whether it is as a direct (licensing income) or indirect (products and services) money-spinner. IP is critical to the 'value chain' of a business and should be given the same consideration as other assets and core materials that are required for the continuation of business as a component of the supply chain.

During an economic downturn, old risks are magnified and new threats emerge, so the potential adverse impact increases. It is essential to understand the key points of vulnerability within the value chain. Business continuity management has traditionally focused on a company's internal systems, or occasionally immediate upstream dependencies, such as the manufacturer that supplies the parts used in a company's factory. These are certainly important, but the value chain must be examined from end to end – downstream as well as upstream. This involves an appreciation of the role of IP and IPR in the business, but also in that of a competitor, a supplier, a customer and all partners.

IP that is created by a company but rarely or never used, owing to change in strategy or simply incidental creation, has a potential value that can be unlocked. Given the current climate it makes more sense to appreciate the entirety of intellectual property dependencies within the business and to explore the opportunities that these unique assets can bring.

Optimization of intellectual property

Companies across a wide array of industries are increasingly implementing intellectual property optimization programmes. The onset of the economic downturn has created a steep increase in entities searching for approaches to increase cash

flows and raise capital. While companies have varying approaches to do this, for most companies IP optimization can take the form of a number of actions:

- licensing IP to third parties;
- sale of IP;
- IP protection and enforcement measures;
- IP royalty audits;
- borrowing against the value of IP;
- monetization and securitization of IP;
- setting up IP investment holding companies (IHC);
- charitable donation of IP;
- improved IP strategy;
- supply chain diagnostics;
- enhanced management and control of existing and future IP;
- risk transfer.

In simple terms, there can be three steps to optimizing IP within the business: review it, prioritize it and strategize it. The strategy that evolves from this process will depend upon the appetite of the business, its financial status and its place in the market amongst other things. There may be no right or wrong answers, but what is important is to have a strategy to optimize the risk and reward associated with intellectual property.

1. Review it

Many companies still do not work hard enough to review their existing intellectual property. First steps might include establishing a comprehensive list of all the IP assets that are held by the company, including assets other than IPR such as brands, know-how, confidential information and trade secrets. The status (active or inactive, etc) and expiration of all such assets should be understood, as well as the scope of any rights, the protection they give and the geographic footprint of all IP. At this point it also makes sense to gauge the minimum costs associated with the maintenance of the intellectual property, renewing any rights, and the legal or marketing costs associated with promoting and securing this portfolio of IP.

During the process of review it is important to examine how IP is currently managed within the company. Is responsibility given to any one individual to exploit the IP, such as a chief intellectual property officer (CPO), or divided amongst legal, marketing and finance functions? What authority do individuals have with regard to promoting, managing and exploiting IP? How is accountability for IP handled at a senior level or even at a board level? What policies are in place to manage IP throughout the business both down to and up from a grass-roots level?

Does the company have an internally developed or off-the-shelf programme that is used to track and collate IP? It is important to examine procedures to protect any internally generated IP from misappropriation, loss, or public distribution prior to the acquisition of the appropriate intellectual property rights.

Gillhams // Solicitors

Gillhams Solicitors specialise in providing legal advice on technology and intellectual property protection.

Our solicitors include qualified and experienced software engineers. As members of the British Computer Society, we understand technology and focus on legal issues. We believe that obtaining legal advice should not require training your solicitors on the subject matter upon which they are required to advise.

We advise large national companies on intellectual property rights and their nexus in commercial transactions and disputes.

Specialist technology legal advice at cost-effective rates in the United Kingdom and Europe.

Lexcel Accredited.
Quality Assured Legal Services.

INTELLECTUAL PROPERTY
INFORMATION TECHNOLOGY
REGULATORY COMPLIANCE
PROCUREMENT
DISPUTES & LITIGATION
CONTRACT ADVICE

Gillhams // Solicitors

Second Floor
47 Fleet Street
London EC4Y 1BJ

T +44 (0) 20 7353 2732
F +44 (0) 20 7490 2733
www.gillhams.com
solicitors@gillhams.com

An understanding of the IP supply chain has been previously mentioned, and measures should therefore be put in place to minimize disruptions to it. The interdependencies between partners, and suppliers particularly, can raise challenging IP issues to consider. Understanding the IP required for the business to operate is critical. Only when the comprehensive review of all IP, IP strategies, if any, and the measurement of success of such strategies is completed can a company safely move on to stage two of the process.

2. Prioritize it

In order to prioritize IP within an organization, it is firstly paramount that the strategy of the company is clear with regard to the products, services and markets with which it wishes to be involved. While the development of certain IP can sometimes radically influence the strategy of a company, or a shift in market demand might position non-core IP as more influential upon the strategy of the business, the overall direction and objectives of the company should then be clearly supported by the IP. Every business has varying appetite and objectives, which the IP should be positioned to enhance.

Once the due diligence has been conducted as part of the initial review phase, the next step is to prioritize the IP based on values, the nature of the IP, and the competitive landscape. By conducting a high-level market valuation analysis to ascertain which IP categories may have significant value, and thus should be the focus of more in-depth management, the process can move with more speed. In many industries (eg pharmaceutical, automotive, technology), the prioritization of patents, based on value and exposure to risk, makes most sense, whilst in other industries it may be brands and trademarks that are paramount (retail, consumer goods), or copyrights (media). The valuation is also to be based on the future income-generating capabilities of the asset, bearing in mind the competitive landscape, any available market pricing for comparable assets, the remaining economic life of the IP, and the risks associated with the IP.

The valuation, in simple terms, must obviously consider quantitative factors such as costs, revenue value, asset value and cash flow value. However, a number of qualitative factors may form the valuation, such as brand enhancement, compliance and strategy. Once fair market values are estimated, the IP can be categorized based on value, exposure to risk and optimization opportunities. The idea is that now senior management can establish the priorities upon which to allocate time, management attention, resources and capital.

3. Strategize it

This is a tough time for chief financial officers. As the global economy has deteriorated, so the pressure increases to develop strategies for making the best use of capital and reducing the potential impact of volatile markets. The process of IP optimization is predominantly encouraged to ensure efficient use of IP assets and then to further protect the value they generate to the business. However, a

by-product of such an approach can lead to the transformation of a company's intellectual property from a cost centre to an income-generating and/or leveragable asset that can lead to the enhancement of existing cash flows. As the process is executed, it may maximize existing IP arrangements, monetize IP in new ways or even unlock ideas for new IP.

As mentioned, IP strategy will influence and be influenced by the overall strategy of the business. Many of the questions asked during the review process can now also be addressed, predominantly around determining the role of accountability for IP and the management systems required to gather information. As a better picture of the entire scope of IP retained by the business is gathered, and the dependencies upon key IP or the existence of non-core IP is discovered, then strategies can be designed around unlocking further potential or minimizing harm. Some of the strategies are discussed below:

- *IP supply chain diagnostics.* It may make sense to spend considerable effort in the appreciation of all intellectual property critical to the supply chain of the business. The objective is to identify all dependencies and skills required to maintain the operation of the supply chain, to ensure appropriate resources are in place to continue to deliver and maximize the IP, and to ensure IP is appropriately protected to provide greater supply chain resilience.

  The diagnostic should also enable better business and financial decision making by moving from an instinct-based approach to a knowledge- and information-based approach to understanding risk. Decisions that effectively and efficiently allocate scarce resources towards IP risk mitigation efforts can also be achieved. Other benefits include:
  - gaining a better understanding of key IP risk exposures and enabling the company to quantify the potential financial impact of those risks to the business;
  - using the quantification of risk as an input for IP risk management investment decisions: acceptance, mitigation and/or transfer;
  - recommending an IP risk management plan that is built upon a sound and measurable business case;
  - providing recommendations to reduce key IP risk exposures and developing a road map for implementing those recommendations.

  It would be expected that part of the revenue gains uncovered during the optimization efforts can be allocated to fund the enhanced IP risk management, which would result in improved returns and resilience without incremental expense.
- *Risk transfer.* Much has been written on the subject of intellectual property insurance, and there have been considerable developments in this space over the last few years.[6] The IP risks now covered by insurance, and indeed intangible assets in a broader sense, have expanded to include reputation and open source issues.[7] The traditional insurances providing coverage for legal expenses in defending an IP claim and any resulting damage award or settlement from that litigation are now also supported by insurances to indemnify liability under

contractual representations and warranties, or litigation expenses in enforcement actions. Furthermore, coverage is now available to insure the value of intellectual property much like a traditional property or business interruption insurance cover. This is another risk management tool when seeking to protect the value of licensing income, R&D expenditure, IP portfolio transactions and monetization and securitization deals.

- *Management/protection.* In addition to supply chain diagnostics for IP and the continuing efforts of a business's lawyers to establish policy for IP treatment, IPR achievement and assertion against competitors, there are many other tools available to enhance IP optimization. The prevention of counterfeiting and piracy may need to be examined, where there is no easy way of ascertaining the infringer or in obtaining damages. Such activity can be achieved with forensic investigators, and ensuring vendor integrity through the due diligence of suppliers and distributors is good practice. Again, valuation experts can assist in determining the losses suffered during the operation of the business and are able to calculate the damages caused for litigation purposes if required.
- *Monetization.* A robust IP monetization programme can improve cash flow, reduce costs, and provide additional sources of capital, all potentially providing increases in shareholder value. When the understanding of what IP is under the control of the business is clear, value-accretive opportunities to sell or license IP, borrow money against the IP and review existing licence relationships (IP royalty audits) become possible.

  For many entities, the inability to raise capital to produce a scalable product is a hurdle to recognizing the value of IP, while for other businesses many IP assets are 'dormant' and non-core to the daily operations of their market, but nonetheless could provide benefits to another party. In either case, a sale or licence of the IP is a viable solution for recognizing and maximizing the value of IP.

  In some instances, organizations may be able to utilize their IP as collateral for borrowing, as the rights to the IP are utilized to secure debt. For many IP-centric companies without significant levels of tangible assets to use as collateral, their IP – whilst often overlooked for lending purposes – has a discernible value that should be considered to assist in securing debt capital. One of the most vital aspects of any transaction utilizing IP as collateral is an understanding of the fair market value of the IP, as it is a key driver in the amount and terms of the loan.

  The availability of financial partners who might be interested in such deals, or even more complicated securitization deals, has decreased with the downturn commensurate with a more conservative approach to lending and investment. However, opportunities still exist for the right deal.

Conclusions

The global economy has pushed many companies to the brink of survival and challenged business leaders not only to examine their expenses, vulnerabilities and operational structures but also to seek opportunities within the business that have

not been seen before. During the process of driving efficiency from all of a business's assets and costs, the role and scope of intellectual property should not be overlooked. A holistic approach to appreciating the IP assets retained, all IP dependencies and the value of IP to the business will lead to an optimized programme for protecting the business, driving informed commercial decision making and potentially unlocking those vital revenue streams.

Notes

1. Francis Gurry, Director General, World Intellectual Property Organization, speaking at Global Financial Crisis and Economic Outlook: Global Think Tank Summit, Beijing, 3 July 2009.
2. Francis Gurry, Director General, World Intellectual Property Organization, speaking at Global Financial Crisis and Economic Outlook: Global Think Tank Summit, Beijing, 3 July 2009.
3. See, for example, B Williamson and M Myers (2009) 'IP in a downturn', *IP Review*, CPA Global, May.
4. See Freshfields Bruckhaus Deringer, June 2009, http://www.freshfields.com/news/mediareleases/mediarelease.asp?id=1835.
5. Marsh, Communications, Media and Technology Industry Research Report, June 2009.
6. See, for example, M Hogg (2007) 'IP insurance', in *The Handbook of European Intellectual Property Management*, ed A Jolly and J Philpott, Kogan Page, London.
7. For a deeper examination of IP risks, reputation risk, IP risk management practice and insurance, see M Hogg (2005) 'Intangible assets, risk management and insurance: bringing all minds together,' in *Risk Management and Innovation in Japan, Britain and the United States*, ed R Taplin, Routledge, London.

3.3

Securing the investments in your brand

Ari-Pekka Launne, Kolster Oy Ab

If you plan to make a profit in business, it is no longer enough simply to bring your product to the market. Your brand competes with other brands and you invest lots of money in it. Your products may be copied, and your brand is constantly under attack. With a carefully planned IP strategy you can back up your business strategies and secure the maximum benefit from your investments.

The changing brand landscape

The modern world and the new methods of communication and transport have resulted in more and more companies facing the need to go global. It is no longer a question of how to do it but a huge challenge with multiple risks. To survive, companies must pay close attention to the changes in the environment, to demand and to new innovations. The amount of information available is massive, and much effort will be required to winnow out the unnecessary.

In the good old days the main focus of companies regarding their IP was on the registration of the rights, mainly intended to secure the companies' options to use the technologies they had developed, as well as marks and designs of their own. As the market was more local, a system based on territorial protec-

tion was sufficient. Coexisting rights in different countries did not affect businesses in the way they now do. Now, globalization is a fact, and new thinking is needed.

New risks have evolved, and the remedies available are not always efficient. In fact, it appears that companies must put more and more effort into minimizing the risks beforehand instead of relying on action when it is needed. Although not all risks can be completely ruled out with planning, however carefully one plans, a lot can be done to avoid certain situations in which companies in the global market may easily find themselves.

To be able to develop an effective IP strategy, it helps if one understands the life span of the rights as well as the life span of the product. The similarities are obvious. In principle, there are three phases, and each of them plays a role in the overall success. These phases are planning, securing and follow-up. In the following, each is discussed in more detail.

The planning or pre-registration phase

The old saying 'Well begun is half-done' gives advice that applies to the protection of IP rights and also brands. Most companies are familiar with conducting searches and investigations to reveal bars against the use or registration of their marks, to secure their freedom to operate and to help them in foreseeing risks related to certain market areas. With globalization, these actions are becoming more and more important and should therefore be routine for all serious players.

Therefore, the next step to be taken in this phase should be straightforward. It is simply setting up a framework for carrying out these searches and investigations in an integrated and timely manner, and looking for the information regarded as necessary. The needs of companies vary depending on several things, resulting in the individualization of the planning phase for each company. This is why advice on these matters also needs to be on an individual basis.

It is necessary to understand that the planning or pre-registration phase relates not only to the registration of rights but also to all matters relevant to the IP of the company. Naturally, when discussing, for example, the registration of a single trademark in a limited number of countries, some planning is needed; but, when considering the whole IP strategy of the company, wider insight is needed. Therefore, the following questions need to be addressed:

- Decisions on attitude towards others: competitors, imitators, copycats, infringers; to be an active or passive player; to avoid infringing others or to act in the grey zone? If necessary, can this attitude vary depending on the other party, and if so how?
- Geographical issues, relating to the planned market areas and the company's position in that market: where to register, where to enforce, where to attack others and where to defend the company's own rights.
- Registration systems, relating to the different possibilities for obtaining protection for IP: when to apply for national registrations; when to use

international registration systems; how to combine the different forms of IP to maximize the protection; and how to avoid unnecessary registrations and costs.
- Working processes and actions in the pre-registration and registration phase of a single right: when to search; what to search for; how to put to use the results; optional ways of trying to overcome bars that have been revealed; and when to drop the case and start with another.
- Working processes in the enforcement and maintenance of the rights.
- Who makes the decisions: a person, a department (just to name two possibilities); in-house or outsourcing?
- Budget issues relating to IPR. These go hand in hand with the overall IP strategy, but it is worth paying some attention to these matters as well in the course of making decisions on the above issues.

Once these questions have been addressed, the company is well on its way to concluding the task of creating an IP strategy. While it may have taken some time and effort to prepare, and while it may need to be amended from time to time, it will surely make life easier for those responsible for these matters. Experience has shown that both working hours and money can be saved later when this phase has been completed with care.

If possible, it would be a good idea to have this IP strategy in writing, preferably as a company handbook to IP-related issues. First of all, assembling such a manual means that things need to be considered more carefully. It is also easier to insist that the IP strategy and the accompanying processes are followed by personnel when such a manual is available. New technical possibilities to have this document available, for example on the company intranet, make updating easy and facilitate distribution to those involved.

Securing the rights

As mentioned above, when plans are clear and the guidelines that were set up are followed, the actual registration of rights does not seem to be too complicated. After all, in a case where the company uses a network of attorneys, the majority of work done in this phase is made up of sending instructions and receiving reports. Since such procedures are clear, other kinds of unnecessary communication can be avoided, which of course means saving money.

It is, of course, essential that the company itself also keeps records on its IP activity. Depending on the partners chosen and the number of attorneys involved, as well as on decisions relating to the responsible bodies in the registration phase, it may be inevitable that no one is aware of each and every registration or application. This is a risk and may result in the subsequent loss of rights and complications. To decrease this risk it is necessary to choose a limited number of persons to be in charge (preferably one) and to create a network that supports efforts to manage the portfolios.

Once again, the needs and practices of companies will be different depending on the size of the company, the amount of their IP and the chosen strategy. Therefore the practices that are found to work should be put in use and those that do not should be developed further or disregarded.

Follow-up and enforcement

The third phase is likely to be the trickiest. It can be divided into subcategories as follows:

- actions needed to keep the registrations valid and in force: this may include not only payment of the annual fees or renewal fees but also proper use of the marks;
- watching the registers so as to be able to take action against competitors and third-party applications in time, to avoid limitations to the company's own IP and, possibly, to collect information on competitors or potential competitors;
- actions against copying and counterfeiting;
- actions against infringements of the company's own IP;
- actions to defend the company's rights when accused of infringement and to open more space for its IP by clearing bars against use or registration (cancellation actions, counterclaims);
- entering into agreements relating to the use and registration of IP with others;
- actions needed to maintain and enforce such agreements;
- educating and increasing the awareness of employees in IP-related issues and company policies;
- collecting information and feedback useful for amending strategies when needed.

When working on global business one soon discovers that, in spite of all needs and efforts to harmonize the laws, rules and regulations that have an effect on IP, there are a number of variations on this simple theme. This calls for constant updating of information on what kind of evidence is needed in individual cases, what is generally accepted and what is particular to a certain country or area. It is quite common that companies do not prepare themselves in this respect but tend to begin the collecting of evidence only at the time of actual need. While this is understandable, and may be even the most convenient way of doing it (since one might never actually need to do it), in many cases it proves to be the cause of failure in actions and results in limitations to or, in the worst case, complete loss of rights. This risk too can be decreased by planning and being consistent in sticking to the plans.

Special attention should be paid to using local aid and specialists in foreign jurisdictions to be able to enforce the company's IP in full. While it involves more costs, at the same time it secures skills and know-how on the legislation and procedures of that particular country. Risks in choosing a local representative can be

decreased by networking with those who have a good reputation and have been recommended by trusted sources.

And the other way around…

One cannot completely avoid situations in which legal advice and the help of lawyers are needed, however carefully one tries to build a strategy to allow operations without the interference of others. The competition sometimes calls for action against competitors, and some competitors may be more eager than others to attack for the least of reasons. In such cases, a company may find itself being the defendant, even if it did everything according to the book. Luckily, good planning will help in this case too.

Actions brought on the basis of non-use can be met with confidence if material supporting one's case has been collected in time. In these cases, the risk is managed by regularly giving out information on usage to the public, as well as documenting the use by collecting leaflets and advertisement material from time to time. When acting globally, this also needs to be done globally. The wider the market area, the more material is needed to cover it. As stated above, it is easy to note in this case too that such collecting of evidence may be an extremely hard task if done only in the case of immediate need.

To lessen the risks of being sued for infringement of the rights of other parties, one needs to be well aware of what rights others might have. Once again, searches and investigations are needed and may also reveal information that is useful in other respects, such as spotting changes in the strategies of competitors or identifying new possible competitors.

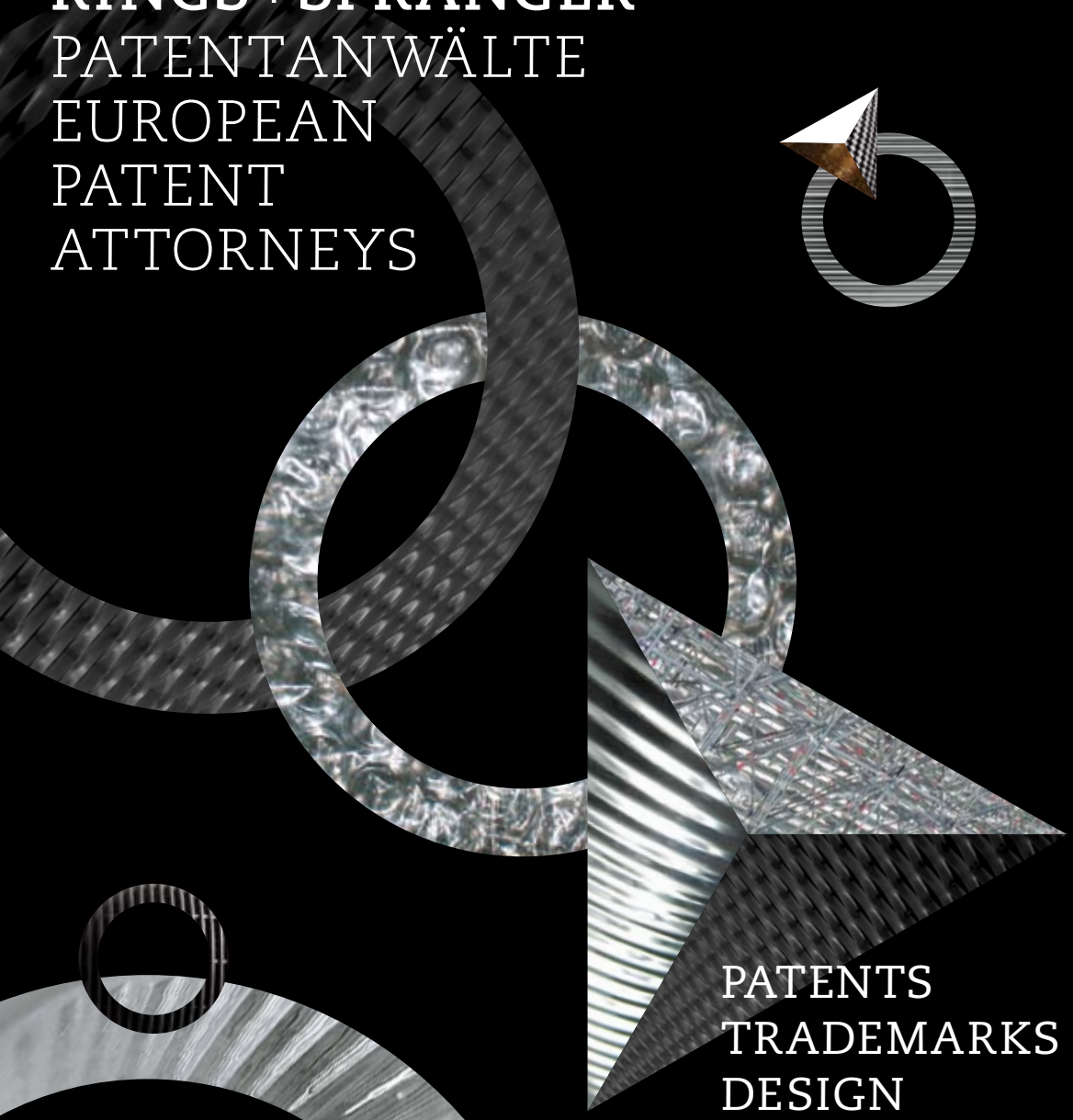
If and when disputes arise, the resolutions come to play an important part in the life of the company. These may be judgments, decisions of administrative bodies or settlement agreements. They may limit the future possibilities to expand the scope of protection, geographical scope of actions or use of some rights in a particular respect. All the same, effort should be put into following these and to implement the stipulations in everyday activities – to avoid being in breach of them and thus liable for damages or compensation. At the same time, these kinds of documents are equally valuable as certificates of registration, as they may indeed define some rights and obligations that otherwise would not be recognized or that would be unsafe, to say the least.

Conclusions

There are always risks that a company faces in the course of business, and some of these relate closely to IP. These risks should never be underestimated or downgraded. They depend on the company's field of activity, the geographical issues, the nature of the risks or the competition and so on, but the risks are always there. Companies must do what they can to avoid the risks and do the best they can to control the situation when the risks become reality.

Careful planning of a company's IP strategy, consistent securing of its rights by registrations, and available supplementary means to enforce those rights against competitors and other players in the field will result in the best outcome. This all means constant work. It may seem endless, but it will pay back in the form of helping the company to maintain the high value of its brand.

RINGS+SPRANGER
PATENTANWÄLTE
EUROPEAN
PATENT
ATTORNEYS



PATENTS
TRADEMARKS
DESIGN

RINGS+SPRANGER
PATENTANWÄLTE
EUROPEAN
PATENT ATTORNEYS

RAUCHSTRASSE 8
81679 MÜNCHEN
GERMANY

TEL +49(0)89/90 77 823-0
FAX +49(0)89/90 77 823-22

INFO@RS-PATENT.DE
WWW.RS-PATENT.DE

Register of German Partner Companies:
PR 735, County Court Munich

3.4

Patent infringement and non-validity risks: opportunities and dangers in the context of intellectual property risk management

Rolf Rings, Rings & Spranger

Introduction

The strategic management of intellectual property (IP) and in particular patent matters has become a crucial issue for the success of modern innovative companies. Patents and patent portfolios can have a considerable economic value for companies in a more and more globalized and competitive business world. On the other hand, there are many risks arising from patent rights for start-up companies as well as for international firms starting business in new areas. This

chapter focuses on evaluating the potential risks and opportunities in patent matters through operative and strategic risk management measures in intellectual property management.

Patent rights as opportunities and obstacles in business

Patents provide the proprietor of a patent with a timely limited monopoly to use the patented technology. This exclusivity of use of innovations for at most 20 years from the date of filing a patent application is in some areas a highly valuable asset for technology-driven companies. The possible earnings from the competitive advantage are the main purpose of developing and filing patents for the proprietor. For competitors and third parties, on the other hand, a strong patent portfolio of one company is a high risk when their own products may inadvertently fall under patented technologies and a patent infringement suit by the patentee is likely.[1]

Patent infringement proceedings may easily cost from a few hundred thousand euros to several million euros. Therefore, it is very important to consider and mitigate the patent infringement risk as far as possible. The patent proprietor, having good knowledge of infringing products by competitors, is faced with an also not inconsiderable risk of possible non-validity of its patent rights. If it is decided to file a lawsuit for patent infringement in one country, most certainly an opposition or nullity suit will be filed by the accused infringer in response to the lawsuit, and at the end of the process, if the patent office has not found all pertinent prior art documents, the patent will possibly be found to be invalid. In such a case, after revocation of the patent, the patent proprietor filing a lawsuit for patent infringement is also liable for the costs of the proceedings and the adversary party's attorney costs.[2] But, if the patent proprietor has done proper searches and taken necessary risk management measures, such a patent conflict may offer an opportunity for the innovative firm to make profits over quite a long term – either by using the monopoly itself or by earning licence fees. With a maximum patent duration of 20 years, a company can make considerable profits from patents. Therefore, it is an important management challenge to file patents correctly and to protect key patents for very important products and business areas. On the other side, a company's management will have to do everything possible in today's intellectual asset-driven business world to avoid an infringement of patents owned by other enterprises. Possibilities and management measures to reduce such risks arising from patent rights will be discussed in the sections that follow. Most statements can be taken to apply also to other intellectual property assets, such as utility models, trademarks, copyrights or design patents. However, we will concentrate here on utility patents.

Patent infringement risks

Companies doing business in patent-active countries and product areas have to be more and more diligent when introducing new products in the market. Every year,

an increasing number of patent applications are filed with the patent offices. In 2008, for example, the European Patent Office (EPO) received 63,013 new European patent applications and, together with the international Patent Convention Treaty (PCT) patent applications entering the regional phase before the EPO, the total number of new EPO patent applications filed in 2008 was 146,561. Although not all of these patent applications will pass the examination proceedings successfully and result in granted patents,[3] this large number of patent filings already shows that more and more companies are trying to monopolize certain technological areas. For technological companies and especially start-up companies, it is therefore very important first to know the relevant patent rights with which the products may come into conflict and then to develop and file their own patent applications on new subject matters regarding their own products in order to minimize potential patent risks and to increase the possibility of negotiation in the case of such conflicts.

The following patent-related risks may arise in patent infringement situations if one company threatens another company with a patent infringement lawsuit, when companies do not correctly consider beforehand and evaluate patent rights of third parties before launching new products:

- costs of patent clearing;
- patent litigation costs (attorneys' fees, court fees);
- payment of damages to the party succeeding in patent litigation proceedings;
- loss of market share due to a 'patent infringer' image;
- costs of design-around solutions.

Effective risk management of companies has to deal with these patent infringement risks. Even though only a minor number of patents and patent conflicts will lead to infringement and validity litigation, in which the adversary party tries to invalidate the patent, the potential risks of patent infringement situations are very high and, for small and medium-sized companies (SME), often an obstacle to entry into new areas or even to starting their own patent filings. For an average or relatively low value of litigation today of €500,000, the costs of the patent infringement and nullity proceedings can easily amount to €96,670.[4] It is therefore highly advisable to take any possible risk-reducing measures in patent matters before the launch of new products. A number of operative and strategic measures for patent infringement risk minimization are given below.

Patent non-validity risks

On the other hand, even examined patents when re-examined are often shown not to be valid, not within the broad scope of protection as granted by patent offices, or not valid over the prior art. For example, if the patent examiner did not find all pertinent prior art documents[5] when carrying out the patent search, there can be a situation in which the patent proprietor uses its patent aggressively in the first instance, but in the end loses the patent and has to bear the litigation costs, because the re-examination of

the patented subject matter in opposition proceedings before the patent office or nullity proceedings in court showed finally that the patent was not valid.

After the grant of a patent, third parties and companies confronted by the patent owner with patent infringement threats may file an opposition with the patent office within a certain time limit. German patents may be opposed within three months from the date of publication of the notice of the patent being granted, and European patents may be attacked with a centralized European opposition for all the present 36 member states of the EPO (July 2008) within nine months from publication of the grant.[6] After expiry of the opposition deadlines, patents may only be attacked and re-examined in respect of their validity or non-validity by filing a so-called nullity action either with a specialized court (Germany) or in the context of an infringement proceedings with the infringement court (eg in the UK or in France). In order to reduce the risk of non-validity, a patent proprietor can conduct its own prior art searches before filing either a patent or an infringement lawsuit. Further measures for minimizing this kind of business risk, such as validity opinions elaborated by patent experts or patent attorneys, are discussed below.

From a business point of view, the non-validity risk seems to be less critical than the patent infringement risk discussed previously.[7] In Germany, for example, in cases of the non-validity of a patent, the patent proprietor does not have to refund any licence payments made by licensees before the revocation of the patent. Furthermore, the costs of opposition proceedings normally do not have to be paid by the losing party. Rather, each party has to bear its own attorney's costs and office fees in patent office opposition proceedings. The largest risk component for the patentee in the case of invalidity threats is the loss of the patent right and its blocking position. If the patent was a highly valuable asset, the legal and financial loss may be considerable.

IP risk management measures for reducing infringement and non-validity risks

There are several effective management tools and measures to mitigate patent-related business risks. In this respect, a management executive will usually rely on external services and external expert knowledge provided by patent law firms and technically specialized patent attorneys, but a basic knowledge of possible IP risk issues is nevertheless important for company success.

Patent risk-related measures in IP management are, on the one hand, defensive measures in the sense that preventive steps are taken to reduce possible patent-related risks in the future. On the other hand, there are more offensive patent risk management measures, which will in most cases be employed in cases where a patent risk scenario, such as a patent infringement threat, has already occurred. A summary of the various defensive and offensive risk management measures is provided in Table 3.4.1.

Defensive IP risk management

Examples of preventive IP risk tools are clearance opinions, prior art searches, patent validity opinions, patent audits and patent watch systems. A clearance opinion is an expert opinion, usually provided by specialized intellectual property attorneys or patent attorneys, in which the freedom to operate for a specific product is examined and evaluated in view of third-party patent rights granted in the product-related field. The basis for such clearance opinions is a search for valid patents in relevant territories (eg in Europe and in the United States), which will normally concentrate on the most important competitors in the respective business area. Nevertheless, more and more patents are filed and owned by non-producing companies or licensing pools, so that a broad search for third-party patent rights is recommended. In a second step, the patent attorney will check the legal status of the found patents. The product and technology will then be evaluated from the point of view of a possible infringement or non-infringement of these patents. The result of such a clearance opinion is an assessment of the infringement probability for a specific product (before the product launch), so that management executives can decide whether to take the risk or whether to search for other possible solutions, such as cross-licensing with the owner of the patent rights or a product design-around.

Another defensive patent risk management measure is the provision of so-called prior art searches. If, for example, the clearance opinion showed that a certain number of competitor patents might lead to a patent infringement conflict, the company can search for prior art documents in patent databases in order to find documents that will invalidate the patent and that will be used in cases where the patent proprietor actually threatens an infringement lawsuit after the product launch. The aim of prior art searches is either to destroy patents of competitors or to prepare the filing of a company's own IP rights. For example, if such a prior art search shows that the product contains new and inventive subject matter, which can be the basis for a patent application, the filing of such an application is highly recommended in order not only to secure the company's own freedom to operate but also to establish a basis for negotiation in a possible future patent conflict.

On the basis of prior art searches, patent attorneys can draft so-called validity opinions regarding specific patent rights. A validity opinion contains pro and contra arguments regarding the validity of a patent application or a granted patent. The validity may be questionable if there are many prior published documents for similar technologies or even a prior use by actual products in the market, which destroy the novelty or the inventive step of one or more claims of the patent or patent application. Validity opinions as a defensive patent risk management tool are also used in order to support and prepare litigation based on non-examined IP rights, such as utility models. It is very important to mitigate the risk of invalidity of such a utility model before filing an infringement suit or even before sending a warning letter to alleged or actual infringers of the utility model.

A more business-related defensive patent risk management tool is the so-called patent audit: in patent audits, the patent portfolio (patents, patent applications, etc) of a company or of a business section of a company is reviewed in detail in order to determine the strengths or weaknesses of the company's IP portfolio. Patent audits include not only the documentation of all patent rights, but also the determination of the legal status (filed application, granted patent, dependent patent, independent patent, etc) and an evaluation of the importance of each single patent. Patents covering technology that is used in core products of a company, for example, are more valuable for the business than patent applications regarding minor improvements or technology that is not even used by the company. These patent audits are often established in the context of so-called due diligence searches to prepare the sale of a business unit or to prepare an acquisition. Finally, so-called patent watching may be used as a defensive risk management tool. Patent watching is the periodical review of newly issued patents or newly published patent applications. Every patent application is automatically published by the patent office 18 months after the filing of the application. If a company has only a small number of relevant competitors in a certain technical field, it is highly recommended that it install patent watch systems for the most important fields and business areas. This is important, because an opposition after the grant of a patent may only be filed within a relatively short time period, eg within three months in Germany or within nine months in respect of European patents. For efficient patent watching, it is important to clearly define the relevant patent area and watch filter. An appropriate tool in this respect is the use of the international patent classification (IPC) and the use of several different filters, such as applicant name, inventor name, etc, which can be selected by experts such as patent attorneys.

Offensive IP patent risk management

On the other hand, there are several offensive patent risk management measures, such as the elaboration of infringement opinions, the use of patent rights in company marketing, and the identification of possible blocking positions in a specific technical area or licence negotiations.

On the basis of an infringement opinion elaborated by patent attorneys familiar with the specific technical field, a product or manufacturing method is evaluated with regard to a possible infringement of one or several patents. Patent infringement opinions usually contain a description of the examined product or method, a short discussion of the validity and an interpretation of the features of the claims. Finally, the infringement opinion discusses for each single claim feature the realization or non-realization of this feature in order to determine whether or not a technology is within the scope of protection (defined by the patent claims). In some cases it is advisable to ask several patent attorneys for separate infringement opinions in order to avoid the possibility of a product launch based on a wrong result of a single opinion, with serious negative financial and legal consequences.

Another possibility for managing patent rights offensively is the use of patents in company marketing. Patents may be used effectively to install an innovator

reputation in the market if a company is, for example, known for a large number of patented innovations. In such a way, the technological leadership may be supported, and patent-protected products are provided with an additional sales argument in the sense that very new techniques are used in the products. Regarding the use of patent rights in marketing measures, the company should respect legal boundaries for such marketing measures. For example, in Germany, under the rules of competition law, there are some restrictions regarding marketing with non-published patent applications. If marketing measures regarding patent portfolios are taken, a company should therefore take advice from patent specialists in the respective countries.

The identification of possible blocking positions is a further offensive patent management tool: blocking positions are gaps in a patent area (technical field) in which no patent rights have been filed so far. To identify such possible blocking positions either in a company's own patent portfolios or in the portfolio of competitors, the company may ask patent experts to conduct a search for valid patents in a specific field. If such a search reveals that there are gaps between important fundamental patents, the company may file new patent applications in order to improve its own IP situation or in order to limit the freedom to operate of competitors. One example of such a blocking position in patent matters is the filing of use claims and further developments regarding a basic patent. The proprietor of the basic patent will then either be prevented from using its own patent in these areas, or a cross-licensing agreement has to be sought between those companies.

This leads to a further offensive patent risk management tool, the so-called licence negotiations. Licence agreements are commonly signed between companies for patented technology; they may be limited either to a certain territory (covered by patents) or to a specific form of use of the patented technology. The licensor (or patent proprietor) receives a licence fee from the licensee either in the form of a lump sum and an annual minimum fee or in the form of a royalty per unit or a combination thereof. A patent proprietor will thereby increase its return on investment, and some companies today even concentrate on the filing and acquiring of patents only for the purpose of licensing out in exclusive or non-exclusive form. For the licensee (not having the patent), licence negotiations will possibly give access to a normally exclusive, interesting technology without the risk of filing and defending the validity of patent rights.

The measures listed in Table 3.4.1 are only some of those available to reduce and mitigate possible patent-related business risks. The advantages of consistently applying such measures in the operative and strategic management of innovative technology companies are:

- continuous securing of the company IP portfolio;
- reducing the probability of patent-related risk incidents;
- increasing valuable intangible assets;
- technical blocking of competitors (competition advance);
- maximizing return on investment and company margin with the company's own highly valuable patents.

Table 3.4.1 Defensive and offensive IP risk management measures

Measures	*Examples*
Defensive patent risk management:	
Clearance opinions before product launch	Expert opinions on the freedom to operate in view of competitor's patents
Prior art searches	Search for prior published inventive-step or novelty-destroying documents for a patent
Validity opinions	Expert opinions on novelty and inventive step
Patent audits	Review of patent rights to determine strength/weakness of company IP portfolio
Patent watching	Periodic review of newly issued patents/applications of competitors
Offensive patent risk management:	
Infringement opinions	Expert opinions regarding alleged or factual patent infringement by products
Patent marketing	Using patent matters in internal and external company marketing
Identifying blocking positions	Assessing possible gaps in a patent portfolio (own or competitors')
Licence negotiations	Licence negotiations between proprietor of patents (licensor) and potential licensee, exclusive or non-exclusive licence, cross-licensing, etc

Notes

1. In 2008, a total number of 522,949 patents were valid in Germany (German patents and European patents with German designation).
2. In Germany, the losing party has to bear the patent litigation costs of the succeeding party, court fees and its own attorney's fees.
3. The European Patent Office (EPO), after substantive examination, granted 59,819 patents in 2008.
4. Total cost risk, including statutory minimum fees in Germany for the company's own attorneys, the other party's attorneys and court fees (first and second instance).
5. Today's patent databases include more than 60 million published patent documents.
6. European opposition proceedings of the EPO resulted in 2008 in 39.8 per cent in a total revocation, 31.6 per cent in an amendment of the patent (limitation of scope of protection) and 28.6 per cent in a rejection of the opposition.
7. Only about 5 per cent of all patents are attacked by opposition in Germany.

3.5

What is freedom to operate and why do you need it?

Barry Franks and Kristian Fredrikson, Brann AB

Every new project, independently of whether it relates to a completely new product or improvements to an existing product, entails a number of risks and hurdles that must be overcome before the product will achieve commercial success. These range from 'Will people buy the product?' to 'Can we make it work?' Some of the risks are difficult to define and even more difficult to quantify. One risk that is relatively easy to define, and that it is possible to quantify to some extent, is whether you can pursue a commercial activity without infringing the intellectual property (IP) rights of a third party. This is your 'freedom to operate'. The IP rights include, but are not limited to, granted patents, trademarks, registered designs, copyrights and domain names.

Infringing IP rights can lead to you being sued and not only being prevented from commercializing the product – with the consequential loss of all the resources invested in the product – but also having to pay damages to the owner of the IP rights. In order to avoid this unfortunate situation a freedom-to-operate analysis must be performed so that the decisions on whether to risk investing resources in a project can be made on a sound basis.

Defining a freedom-to-operate analysis

The following examples, to avoid unnecessary repetition, will be limited to freedom to operate with respect to patents, but it must be understood that the same main principles apply to analysis in relation to all IP. However, differences in scope and geographical and temporal validity require different strategic approaches for different types of IP, regarding search, analysis and subsequent actions.

Patents are national (they are valid only in those countries in which they are maintained) and they have a limited life (usually a maximum of 20 years from the filing date of the patent application). This means that a search can be limited geographically to just the countries in which you intend to be commercially active and temporally to just cover patents that could still be in force at the time you will enter the market.

A freedom-to-operate analysis involves a search in IP databases for patents with claims that cover the product you wish to commercialize. There are free IP databases available via national patent office websites, and commercial IP databases that are accessible by subscription. Free databases suffer from the disadvantages of relatively unsophisticated search engines and, unlike subscription databases that allow full-text searching, they allow searches only in the abstract or claims of the IP, which reduces the chance of getting relevant hits. Most companies have neither the resources nor the skills to perform a freedom-to-operate search, and instead use one of the many specialist search firms to perform the search and some or all of the subsequent analysis.

An IP search is very similar to a search made on Google or other internet search engine – a string of words or characters (usually separated by logical functions such as 'and', 'or', 'not', etc) is put into one or more fields in the database user interface and a list of hits is generated. The next step is to analyse these documents to see how relevant they are, ie if an owner or licensee can use any of the patents to prevent you from marketing your product. The analysis has to determine first if a hit has been filed in the countries in which you wish to operate and, if so, secondly, whether it is alive. If it is alive, then the final step is to see if it covers your product.

Normally, the list can be divided into patent families, ie all the national patents and patent applications that originate from the earliest filed patent application in a series are grouped together. In this way it is easy to get details of all the related patent applications and granted patents. In the following illustrative example, let us assume that one of the hits is a UK patent application filed five years ago and that its family includes a European (EP) patent application and a granted US patent.

Whether or not a patent or patent application is alive can be determined from database information or, if not available, by contacting the relevant national patent office. The result may be that the patent application has been granted and become a patent, that the patent application is still pending, or that it has been refused or abandoned. So, for the example above, you might see a pending UK patent application, a pending EP patent application and a granted US patent.

The remedy for high blood pressure and sudden migraine

Patent/copyright infringement, brand theft, reputationparasitism, product copying. Not to mention pirate copying, improper marketing, breach of contract, licence and domain name snags. The symptoms are sudden migraine, anger, frustration and helplessness. Chronic disease leads to flagging margins, weaker brand, lost market shares and blunt competitive edge. Or, as in the USA, convictions, damages and the deal falling through.

The remedy is BRANN AB. A company that has specialised in intellectual property and commercial law in Sweden and abroad since 1949. No side effects other than a good night's sleep.

INTELLECTUAL PROPERTY LAW FIRM

BRANN AB BRANN@BRANN.SE WWW.BRANN.SE
STOCKHOLM +46- (0)8-429 10 00 GÄVLE +46- (0)26-18 63 20
LUND +46-(0)46-271 77 00 UPPSALA +46-(0)18-56 89 00

BRANN

As the US patent has been granted, if you intend to be commercially active in the US market you have to compare the subject matter of the claims (and, in some jurisdictions, equivalents of the subject matter of the claims) against your product. If your product has all the features mentioned in a claim, then you are probably infringing the claim. If your product lacks a technically significant feature that is mentioned in a claim then you probably do not infringe the claim directly. However, only an experienced local patent attorney will be able to give you an opinion on whether or not you risk infringing the IP, as there are considerable national variations in how the scope of a claim is interpreted.

If a patent application is still pending in a country that you wish to operate in (in our example the UK and the contracting states to the European Patent Convention) then your analysis is made more difficult, because the scope of protection that the application could have if it subsequently becomes a patent needs to be determined. The claims are still a work in progress and can change. However, the amount they can change is limited – they can be expanded but not so that they cover subject matter that was not originally present in the patent application at the time of filing. Analysis of patent applications in an attempt to estimate what their final scope of protection might be may require inspecting publicly available prosecution files to determine the relevance of cited prior art documents and what arguments the applicant has used to try to persuade the patent office to grant a patent – a so-called 'file history inspection' or 'file wrapper inspection'. Again, this is a task best left to an IP professional.

If a patent application has been abandoned or rejected it is necessary to check the national regulations regarding reinstatement or further processing of patent applications in order to be sure that the application is permanently dead and cannot be reactivated.

When a freedom-to-operate analysis should be made

The earlier in the life of a project that the freedom-to-operate analysis is made, then the lower the costs of dropping a project or taking remedial action, as discussed below. However, patent applications are not published until 18 months after their filing date, so a freedom-to-operate analysis made at the start of a project will inevitably miss recently filed patent applications. Consequently, a prudent model for performing freedom-to-operate analysis requires the analysis to be updated at regular intervals during the life of a project. Most development projects have milestones or project review meetings at regular intervals with the power to decide whether to proceed with or to kill the project. It is appropriate to update the freedom-to-operate analysis for such meetings.

Even if resources are tight, a final freedom-to-operate review before launching the product is indispensable to avoid the pain and suffering caused by a successful launch followed shortly by a warning letter claiming infringement of third-party IP.

Defining the subject of a freedom-to-operate analysis

There are two basic scenarios here: either you are producing an entirely new product or you are improving or upgrading an existing product. For the first scenario, let us assume that you are out on the golf course and are irritated by all the broken plastic golf tees littering the course. You decide to solve this problem by producing a new kind of tee that decomposes if left outdoors – a biodegradable golf tee. You decide that it can be made of compressed and glued sawdust or compressed peat. You have never worked in the field of golf tees before and have no idea of what the IP situation is in this field. Consequently, you will have to perform a full and detailed freedom-to-operate search and analysis covering biodegradable golf tees. Normally it is better to start off by making a wide search – in this case for any type of biodegradable golf tee – and then restrict it in an iterative process. This is because you are entering a new field, and starting off by limiting the search to biodegradable golf tees made of wood or peat would mean that there is a risk that you will miss broad patents that are not limited to the type of material used. Additionally, the quality of a database search is very much dependent on finding the right keywords to put into the search string, and starting with a broad search may reveal synonyms of keywords that you wouldn't have thought of yourself.

For the second scenario, let us assume that you have been producing biodegradable golf tees made of peat for 10 years and have noticed that you are losing market share to low-cost imports. You decide to revitalize your product and discuss possible improvements with your staff. They have a brainstorming session and suggest the following changes: add grass seeds to the mixture so that they help fill in divots in the course, and/or add fertilizer to help grass grow more rapidly, and/or add a water-absorbing powder to the tee mixture so that when exposed to the atmosphere they absorb moisture, crack and fall apart more quickly.

In this case, if you are fully conversant with the basic product, a biodegradable golf tee made of peat, and the IP situation covering it, it would be sufficient to limit each search to cover just the improvement you are planning to make. So if you want to investigate freedom to operate for all three improvements you would make three searches, ie a first search for 'golf AND tee AND (biodegradable OR synonyms) AND (seed OR synonyms)', a second search for 'golf AND tee AND (biodegradable OR synonyms) AND (fertilizer OR synonyms)' and a third search for 'golf AND tee AND (biodegradable OR synonyms) AND (moisture-absorbing OR synonyms)'.

Of course, if you are not fully aware of the IP situation then you should perform a complete freedom-to-operate analysis for the basic product as well. The fact that you have not been sued for patent infringement so far does not guarantee that you have freedom to operate even for your original product. It may be that currently you are too small to make it worthwhile suing you, but when you launch your new product it is possible that your increased sales will make it commercially attractive for an IP right holder to sue you or at least charge you a royalty.

Using the results from a freedom-to-operate analysis

A patent freedom-to-operate analysis should provide you with a list of relevant patents or a summary that concludes that there are no relevant patents. If the analysis reveals relevant prior art then if you do not want to risk being sued for patent infringement your choices are limited to:

- dropping the product;
- designing around the patent;
- getting access to the patent; or
- invalidating the patent.

Ideally, your company has a system for handling inventions and suggestions for new products that means that a patent review is made at an early stage and your lack of freedom to operate is detected before any investments have been made. If so, then you will have performed the analysis at an early stage of the development project and it will be relatively inexpensive and politically painless to drop the project.

If the final version of your product has not yet been determined then it may be possible to change it to avoid infringing the relevant patent. For example, if the patent specifically claims a tee made of compressed sawdust then you might be able to use compressed peat without infringing the claims. However, before going ahead you must consider that courts in some countries may think that peat is an equivalent of sawdust and decide that your peat-based product would still infringe the claims by equivalent means. Consequently, you should get an opinion from qualified local IP counsel if you attempt to design around the claims of a patent.

Getting access to the patent means buying it or getting a licence to use it. The earlier in your development process you start negotiations with the patent holder the stronger your bargaining position, as the costs of being refused access to the patent are relatively small and your options for designing around it, or dropping the project, are greater. Conversely, attempting to access a patent just before launching a product or, even worse, after launching it will be expensive, as the patent holder will realize that your options are limited.

However, even in this situation you may have an ace up your sleeve: namely the possibility of nullifying the infringement threat by invalidating the patent. A patent can be invalidated if you can show to a court that the invention claimed in the patent was either already publicly known (ie not novel) or obvious (ie lacked an inventive step) at the time the priority application was filed. (NB: there are also other situations that make a patent invalid or unenforceable, but these are beyond the scope of this chapter.) A common way of demonstrating a lack of patentability is to present documents published before the priority date of the patent application (prior art documents) to the court with reasoned arguments why the patent lacks novelty and/or an inventive step. Finding prior art documents usually requires an extensive database search and a lot of resources to

investigate the relevance of any document found. Any subsequent invalidity suit is usually expensive and time-consuming. Therefore, it might be better to search for reasonably relevant prior art documents, show some or all of them to the patent proprietor when negotiating access to the patent and use them as a lever to help you achieve better licensing conditions.

Finally, if the analysis reveals no relevant patents then cautious congratulations are in order – you have freedom to operate. You can go ahead with your product (indeed you might even consider filing a patent application for it), but with the caveat that no database search can guarantee 100 per cent coverage, as patent applications are secret for 18 months and therefore your database search can never be up to date. However, the risk that you will launch a new product and then be sued for IPR infringement has been significantly reduced. It would be prudent to update your search and analysis every six months or so for at least 18 months after your product is launched in order to detect possible problems, such as when an 18-month-old patent application is published and almost immediately is granted as a patent covering your product.

3.6

Recognizing IP-related problems arising from the development of the internet

Ari-Pekka Launne, Kolster Oy Ab

As we know, technical development in communications has been extremely fast in recent years. While it obviously makes many things easier and opens tempting opportunities for businesses looking for new markets, it has downsides too. In fact, it has created new needs for IP protection and seems to bring fresh problems almost daily. To protect brands in this new environment, some old tricks may still be useful, but new ones must also be developed.

The scene

For any company, whatever its line of business, the new virtual environment raises at least one question: to be or not to be in it. Those who can say that they

do not need the internet at all grow smaller in number all the time. Even if some pilot projects have not succeeded, different kinds of businesses have moved at least partly on to the web. And it is a fact that today some businesses exist only on the web. For traditionally thinking IP society, this creates a huge challenge. For the more open-minded the situation is an Eldorado with plenty of opportunities and possibilities.

The first and most fundamental change derives from the fact that traditionally the protection of IP is territorial, while the internet, in principle, does not recognize national borderlines. The internet is a technically constructed complex based on agreements governing the system and outlining the technicalities. From a very much simplified point of view, it is only a means of delivering data from one place to another. As such, it ignores, for example, the legislation and international agreements on IP. This may well be the actual source of all the problems arising from the data.

Second, it is necessary to understand that there are several different sectors in which IP plays a role and risks may exist for businesses. Since the web and practices there are evolving all the time, listing all of them may be impossible. Some may also disappear over time. But in any case, the following deserve to be identified:

- technical issues, including patents, licences to use equipment and programs needed;
- issues related directly to the internet as an environment, such as domain name registration, parking, tasting, phishing and slamming;
- use of trademarks on the internet;
- copyright issues when producing and distributing material on the internet;
- business-related issues, such as relations to the business partners and competitors, business practices and fair competition;
- criminal offences on the internet, such as the sale of counterfeit goods, copyright infringements or fraud.

In some cases, obviously, these issues may overlap each other, which only makes the situation even more complicated. In the following sections of this chapter, attention is given mainly to trademark and domain name-related issues, omitting copyright, patents and designs.

It is worth remembering that one may find oneself as a victim of infringement or conversely, much to one's surprise, infringing somebody else's rights. To avoid being the subject of blame, accepted practices need to be studied and used, and those that are not accepted need to be understood and avoided.

Domain name-related risks

A domain name is an identification label to define a realm of administrative autonomy, authority or control on the internet. It is based on the Domain Name System, and always relates to a certain internet protocol address. At the moment these are

not considered to be part of IP but the attitude is certainly moving towards inclusion. The needs of brand owners to both promote and protect their brands results in domain names becoming closer to trademarks, although the actual purpose of the two is completely different.

When registering domain names, companies once again face the need to reconsider their IP strategy and to budget the funds for creating and maintaining their domain names portfolio. Depending on actual needs for the use of the domain names as well as on the need to prevent others from registering and using certain domain names, the portfolio can in practice range from small (from one to several) to large (from several hundreds to thousands of domain names). In both cases there are advantages and disadvantages. But, no matter how large the portfolio may be, some of the problems arising from the simple fact that one cannot own them all will always remain. For example, there are so many different extensions on which to register, and there are different ways of misspelling the domain. Lots of money can be wasted if a clear policy for the choosing of domain names is not drafted.

Controlling the domain names portfolio and having them renewed in due time are also tasks that should be considered carefully. If the company has several hundred domain names registered in different extensions and is using different service providers for each of these, the mere payment of the invoices from these will be burdensome. There are risks relating to domain names that are not renewed in time or that are dropped. Such domain names may end up in the hands of a competitor or third party trying to benefit from the earlier use of the domain name.

It should also be mentioned that, in the case where a local presence for a certain extension is required, the company may need the aid of a partner to provide it – again, a situation in which risks may arise. For example, letting agents or licensees register the domain name in their own name is one of them. In the event of changes in the business relationship, transfer of the domain name may prove difficult. It is advisable to seek for a partner who can assist in these tasks covering as many extensions at once as possible.

One may ask what the risks are related to *not* registering the available domain names. In short, these can be divided into two: first, cyber-squatters registering the domain names and making money by using them; and secondly, some other business registering them for its own use. The difference between these two may seem insubstantial, but in reality there is usually a legitimate interest in the latter. In other words, the cyber-squatter makes or tries to make money on the domain name itself, while in the latter case the holder of the domain name runs a legitimate business and makes use of the domain name without infringing the IP of others. Depending on the nature of their business or of the location, target group and other details, this may or may not affect the profile or reputation of the company using similar domain names.

Why then would the cyber-squatter choose a domain name that already has some potential fame in the first place, as it is somebody's trademark? The answer is simple: just because of its fame. It relates to the way of valuing domain names

based on the traffic they are able to generate through their use. In the first instance the domain name is free and it can be obtained for a minor amount of money. Since the dominant word in it is a known mark or at least resembles one, it attracts users of the web and starts to generate traffic. This happens when the word is searched in a search engine, when the domain name is used in the address field of the browser or, finally, when it is set to point to a pay-per-click website. As the value of the domain name increases with time, the domain name can then be sold on to a further owner, who in turn may try to profit from it, usually in the same way. If the domain name owner gets lucky, the owner of the trademark may want to purchase the domain name instead of going through the dispute resolution process to recover the domain.

Some criminal offences make use of domain names, as people sometimes don't pay enough attention to the actual domain name used by a certain company. Phishing, in other words collecting personal information including user names and passwords of individuals, is a perfect example of this in practice. Misspelling the name of a bank in the e-mail address can go undetected and can lead to loss of money from the account. Surprisingly, a number of people fall into the trap of these criminals, even though the banks expend much effort in warning campaigns. One must emphasize that what is at stake here is the reputation and goodwill of the banking brands as well as the savings of their clients.

A clear and effective policy in domain name registrations also helps in cases of 'slamming'. Such a practice has become more common, and seems to target as victims mainly people unaware of the registration processes of domain names. In this activity a service provider informs a potential customer about an application for registration of (usually several) domain names that resemble the trademark or trade name of the company. A short period of time is allowed to answer the message, and registration can then be made in the company's name. A fee for the expedited process may be collected. The customer can never be sure if the attempt to have the domain name registered by a third party is real or if the alleged third party even exists. While this activity might not be regarded as completely illegal, it appears to fall into the category of improper business actions.

Hiding behind aliases and anonymity are features of the web that can make it almost impossible to identify the opposite side. In fact, internet society seems to value anonymity so much that it attracts criminals more than in any other field at the moment. In principle the balance of rights and responsibilities is still present, but real-life examples show that bringing the infringers to justice may be a task that is doomed to fail. Cases in which the infringer is caught and punished do exist, usually stimulating the next generation of infringers to develop their schemes further.

These are some of the current issues that are present in the internet, and they need to be considered by companies when entering the wonderland of the web. There are remedies to combat the problems, but the most important tool appears to be good planning of the strategies and tactics to be used. As always, well begun is half-done.

Use of trademarks on the internet

When discussing the use of trademarks on the internet the problems and risks seem to relate to the nature of the web as a medium and to the relations between the domain names and trademarks. As mentioned above, the internet recognizes no borders, while traditional registrations of trademarks are done on a regional basis. Competition is more global, and all the competitors may well have rights to their mark, confusingly similar to each other but protected in different countries or regions. This results in uncertainty in many respects.

The internet is full of information, which of course can be true or false. One faces this fact when trying to gain information on whether the trademark is actually in use or not, and if so for which goods or services. While legitimate businesses make use of the opportunities to promote their goods and services in the traditional way by advertising, offering and selling them, for example through newspapers or other media, some other players may misuse the good faith of the public and competitors for their own benefit. In some cases, it may simply be the intention of a company to benefit from the advertisement of others and to avoid costs relating to the need to be noticed.

A trademark can be used (and misused) on the internet in many ways. Risks relate not only to old-fashioned trademark infringement, but also to the new ways of infringing. In some cases, the new inventive way of exploiting the possibilities of the internet may actually result in the appearance of a completely new category of infringing actions.

One such relatively new phenomenon is the use of trademarks, or words that may be the trademark of others, as keywords in search engines. On the web, all companies want to be seen and found by their potential customers. They may also want to widen the range of their customers to new areas. Knowing that the people in their target group would usually type a certain word or mark in the search engine, companies bid for the right for their ads to be displayed when such search terms are entered. This is a fast-growing business and is likely to continue growing in the future. The problematic question to answer is: when does this practice infringe trademark rights, or does it infringe them at all? After all, many of the trademarks are simply words that are descriptive and in everyday use, although they have been registered as trademarks for certain goods or services, for which they have a distinctive character. This question needs to be answered case by case.

An important feature of the web is that the majority of users are not in the business at all, but rather customers or clients of the companies offering their products on the web. On the other hand, most of the IP is intended for use in business activity, and has no legal effect when its use is private. Little can be done if an individual makes use of a trademark in a distant country, when no business at all is conducted in connection with this usage. While it was stated above that one cannot own everything, it must now be said that one cannot supervise all possible websites and that one need not react to everything. Companies should clarify for themselves where the thin line exists.

Conclusions

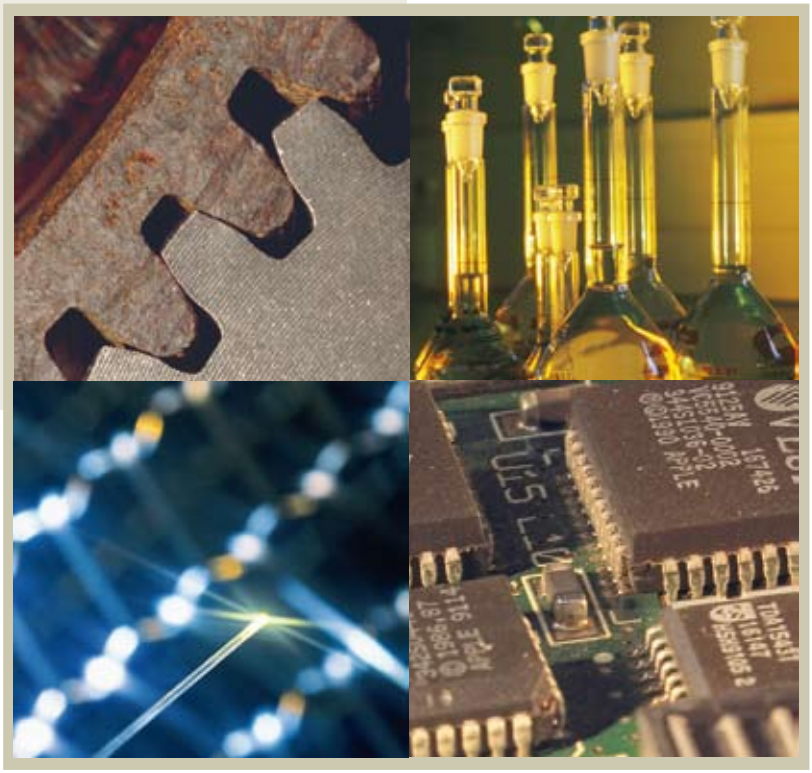
The internet has created a field of possibilities and an endless flow of attractive new propositions, but at the same time it is a source of new disputes and challenging new practices. To be successful in this new era of brands and globalization, much planning is needed and decisions need to be based on exact information. The key to success lies in a well-planned strategy, in the ability to keep to that strategy and, most importantly, in constantly trying to prevent problems from arising if possible. When this is not entirely possible, prompt actions are needed in order to limit the consequences to the minimum. In such cases and from time to time, former decisions may need to be reconsidered and amended. But one thing is certain: these matters are here to stay, and the new will continue to evolve as the world, the internet and global business life improve.

3.7

IP due diligence – evaluating a target company's IP assets before agreeing terms in a merger, acquisition or investment

Annelise Holme, Holme Patent A/S

An IP due diligence process is applicable in many contexts, ranging from mergers and acquisitions to licensing arrangements and venture capital financing. During the IP due diligence an investor, buyer and/or partner makes an investigation into the patents, trademarks, copyrights, trade secrets and other know-how of a target company, in order to identify weaknesses, potential liabilities and potential opportunities.



PATENTS | TRADEMARKS | DESIGNS | IP STRATEGY

HOLME PATENT A/S

Holme Patent is a dynamic firm that renders legal and technical assistance in all areas of IP law. Our European Patent Attorneys build on many years of experience from business, industry, and research.

We work with companies and researchers within mechanical and medical engineering, electronics, IT, chemistry, biotechnology, and genetics. For safeguarding our clients' interests outside of Europe, we have established an international network with some of the most prestigious IP firms in the US, in China, and elsewhere.

We are happy to arrange a non-committal meeting for discussing your situation and for identifying your IP opportunities. Feel free to contact us by phone, fax or e-mail, visit our website, or simply drop by our main office in the heart of Copenhagen, Denmark.

COPENHAGEN:
Vesterbrogade 20
1620 København V
☎ +45 3324 2121
+45 3324 9121

AARHUS:
Rosenkrantzgade 23
8000 Århus C
☎ +45 8687 2121
+45 8693 2121

holme@holmepatent.dk
www.holmepatent.dk

Verifying all the material facts relevant to the investment or purchase by conducting early IP due diligence is a prudent way to determine the value of business transactions involving IP and, therefore, to avoid or minimize costly mistakes and disappointing outcomes.

While the extent of the due diligence analysis may vary with the amount of money involved, the following discussion outlines some of the issues that may come under consideration and some practical advice for successfully concluding the due diligence process.

Identification

First of all, the target company's current IP portfolio must be identified and categorized. This process should include the dates of application, issuance, expiration, required maintenance payments, and whether foreign IP protection has been obtained.

The target company must also disclose all information about failed attempts to secure IP, including any filings that were rejected, withdrawn or permitted to expire. These filings can in some situations undermine the validity and enforceability of later IP filings.

Investors and buyers should not rely solely on the disclosures from the target company when the IP portfolio is identified. An independent search for undisclosed IP is often necessary. The goal of such a search is to locate pending IP, eg under the name of the inventors, founders, authors or subsidiary names, in addition to the name of the target company.

Thus, a company having IP assets should preferably keep a complete list of all IP filings and all relevant know-how, as this will later assist a potential investor conducting a complete due diligence process.

Relevant IP

It is then relevant to make an accurate description of the technology and/or products that are the focus of the transaction or investment. Such descriptions will inevitability be critical, but it is important to understand and establish how the relevant IP will be used. For instance, will the technology be sub-licensed, used to block competitors from entering specifics markets or simply used to attract other investors? The answers to such questions will enable the IP counsel to determine whether the dominant value lies in the patents, trademarks, copyrights, domain names or know-how, and prioritize accordingly. After all, there is no need to perform due diligence on IP that the target company no longer uses or in which the investor has no interest.

In contrast, IP that is essential for the target companies and/or investor must be afforded meticulous investigation.

Ownership

Ownership is one of the most important issues to explore in the IP due diligence investigation, as only the correct owner is entitled to sell or give licences to the relevant IP.

In this respect it must be kept in mind that many companies 'forget' to register assignments, name changes, licence agreements and/or transfers at the respective authorities and/or patent offices, either in order to keep cost at a minimum or because such registrations are not considered relevant. It is therefore not sufficient during an IP due diligence process simply to rely on the official registers, as the target company may have made other agreements after the IP applications were first filed. Thus, it is important to examine all the target company's licences, material transfer agreements and collaboration agreements, or any other transaction that involves a transfer of IP rights.

Another problem is that some companies draft their own assignments including only vague and/or indefinite statements, eg 'All relevant IP is assigned.' Not only is such assignment impossible to register at the respective patent authorities but, since it can be impossible later to identify which IP assets were actually assigned, the assignment will be subjected to disputes and, in a worst-case scenario, is useless.

An example of the importance of determining the correct owner before closing a deal is that of Volkswagen. In 1998, when it bought Rolls-Royce and Bentley from Vickers, it forgot to confirm the correct ownership of the relevant IP assets. Although VW paid about £430 million for the cars, designs and manufacturing facilities it couldn't use the famous Rolls-Royce trademark, as it had been sold to BMW by the correct owner – Rolls-Royce plc, the aircraft company. Furthermore, it is likely that the price Volkswagen would have been willing to pay for the purchase would have been much lower if the trademark ownership issues had been sorted out before closing the deal.

Thus a company that would like to have the IP assets in good order for a potential investor should make sure that transfers, assignments, name changes and licences are registered with the relevant patent authorities as soon as possible in order to avoid potential confusion of the correct owner.

Inventor

It is also important to ensure that all the correct inventors are mentioned on the patents applications and/or granted patents. Wilfully naming incorrect inventors can be a ground for invalidating patents in, for example, the United States. In this respect, make sure that inventorship decisions are based on facts and not on politics, so that only the correct inventors are listed on a patent application. Many companies have a tendency always to list the managing director or the head of a department as an inventor even though that person has made no contribution to the invention.

Furthermore, all employees involved in the development of new technology should sign contracts in which they automatically assign all rights, including rights to potential inventions, know-how and/or technology. To such agreements should

be added conventional assignments where the inventor assigns the right to the specific patent application(s), its patent family and any future filings based on that patent application.

A special note has to be made relating to inventors for US patents. In the United States, patents will be issued in the name of the inventor(s) unless an assignment has been recorded with the United States Patent and Trademark Office. If no agreement exists, eg an agreement where all inventors assign their rights to the company, each inventor owns an equal part of the rights to the US patent. Thus, if multiple inventors are involved and one inventor assigns his or her rights to a company, non-assigning inventors would continue to be joint owners with the company and could, without the consent of the other inventors or the company, grant rights to the patent that would devalue the rights that had been assigned to the company.

Getting inventorship wrong for a US patent can have detrimental consequences for a company, as was the case in Ethicon Inc *v* United States Surgical (Fed Cir 1998). Ethicon had obtained a licence to exploit a patent for a medical device and accordingly sued US Surgical for patent infringement. US Surgical rejected the allegation, stating that the proprietor had omitted the inventor Y J Choi on the issued patent. US Surgical had later obtained a licence from Y J Choi. The court ruled that the inventor was in fact incorrectly omitted and that US Surgical was allowed to practise the invention under the licence agreement.

Thus, if a due diligence investigation reveals that a patent is owned by one or more inventors rather than by the target company, it is necessary to have the inventor(s) assign their rights to the target company before the transaction is completed.

Strength of the portfolio

The IP profile of a company is more than just a portfolio of legal rights to be used as a defensive tool. Accordingly, a strategic review of intellectual property includes considering not only whether the target company is in possession of good IP such as patents and/or trademarks but, more importantly, whether the company has the right ones.

Patents

In respect of patents, three things will generally be considered. Even though the following points primarily are directed at patents, the same principles apply to all IP assets:

1. *Scope of protection.* The essential applications and patents should be evaluated to determine if they sufficiently cover the technology of interest. Unfortunately, it is not uncommon to find that a company's IP portfolio does not adequately protect its main technologies or assets. Such an evaluation includes the following essential assessments:

- An investigation of whether a company's IP portfolio is in agreement with or supports its business objectives and, more specifically, whether it supports the technological competitive advantages associated with current and future profit sources.
- A legal analysis of the relevant patents. The claims determine the scope of the patent, and all aspects of an invention that are not covered by the claims are not considered to be patented. It is important to bear in mind that it is not always easy to determine the scope of a patent, ie the written specification (as the claims are often interpreted in the light of the specification) and the prosecution history (ie the history of the application process). Thus the evaluation aims at forming an opinion interpreting the claims of the patents indicating what, and how well, the patents can reasonably be presumed to protect. The latter includes an analysis to determine whether the problem solved by the patented invention can be solved in any other way. In other words, how likely is it that a competitor could invent around the technical embodiments of the target company's patent?

2. *Geographical extension of the IP portfolio.* Companies generally make strategic decisions about the countries in which they will seek IP protection. In many cases, technologies may be protected in a company's main markets but may be in the public domain in other countries where commercialization is less likely. In the latter countries, a competitor will need no permission (or licence) from the owner to commercialize the product. Thus, it is important to evaluate in which countries applications have been filed and/or if it is still possible to file applications in countries that have a potential market for the technology or product of interest. In this respect, it should be remembered that patent protection is territorial, so the scope of protection for a patent may vary between countries according to national laws and international agreements.
3. *Validity.* It is important to evaluate whether the claims in the applications or patents are in fact valid. In this respect, it can be relevant to conduct prior art searches to confirm the novelty and inventiveness of the claims. Special attention must be paid here to prior publications such as scientific papers, oral presentations or symposiums from the inventors in order to determine if they have made any disclosures of the technology. Such earlier disclosures may deprive the invention of novelty or of an inventive step.

Trademarks

In addition to the general points listed above, the following further points are relevant for trademarks:

1. Determine if the trademarks have been used continuously on the relevant markets and for which goods and/or services the marks have been used. Non-use of specific goods and/or services may invalidate the trademark completely or in part.

2. Determine if the trademarks are used in the same form – and for the same goods and/or services – as they are registered.
3. Determine if the trademarks have been translated correctly for countries using a different alphabet from the original trademark, as a trademark translated improperly will sometimes cause negative effects or even lead to spoilage of the image of the product. As an example, a Chinese mark of the Chinese characters having the meaning of 'White Elephant' would be directly translated into 'Rubbish' using the Western alphabet. Thus, paying attention to the meaning of trademarks is essential.

Freedom to operate

An IP due diligence process also includes the evaluation of other patents that may influence the company's ability to use the patented technology. It is therefore important to point out that there is a clear limit on the extent to which a patent proprietor has the freedom to operate (FTO) or use the patented technology. A patent by itself does not provide the right to commercialize the protected technology but only the right to exclude all others from commercializing it. While the difference may seem subtle, it is a crucial distinction that needs to be made.

Therefore, the investor needs to determine whether it is possible to develop and commercialize the target company's products and technologies. A third party may, for example, have an even broader patent that encompasses the subject matter of the target company's patent.

In general, such an investigation is conducted through an FTO analysis that evaluates whether one company will be able to make, use or sell products without infringing on the IP rights of a third party. An FTO analysis identifies potential legal obstacles, such as valid patent claims of third parties, and therefore informs the investor of potential infringement lawsuits during the due diligence investigation.

How to ensure that an IP portfolio is attractive to a potential investor

Any potential investor or partner will critically evaluate a target company's IP portfolio before deciding whether or not to invest in or partner with the company. While a due diligence investigation may seem invasive for the target company, it should not uncover any surprises if the target company is well prepared.

Based on the above discussion, the following few points can easily (and should) be prepared in advance by any company interested in attracting potential investors and/or buyers – and will ensure that the company's IP portfolio is easier to access and therefore more attractive:

- Have a list of all IP assets, ie patents, trademarks, copyrights, trade secrets and other know-how, that the target company owns or licenses. If applicable, the list should include country of filing, the serial number, the geographical extension and the status of the IP.

- Have a list of all agreements relating to the IP assets, including any assignments, licences, research collaborations and material transfer agreements. Make sure that the agreements refer to the relevant IP assets preferably both by number and by name.
- Make sure that all the correct inventors are listed on the patent application(s) and/or patent(s).
- Make sure that all name changes, assignments, licences and other agreements and other relevant transfers are correct and in good standing and registered at the respective patent offices.
- If possible, carry out your own freedom-to-operate analysis and relevant prior art searches, giving the potential investor and/or partners a good starting point for their investigations.

Conclusion

A complete investigation into a company's IP portfolio can be expensive, yet the cost is typically almost nothing compared to the cost of litigating a patent infringement claim.

Today a company's single most valuable asset is its intellectual property; thus the importance of due diligence in any investment, merger or acquisition decision must not be underestimated. However, it is often seen that, unless the main motivation for the deal is acquisition of IP assets (such as a key patent portfolio or a valuable brand), buyers, investors and/or partners frequently do underestimate the importance of IP due diligence. Accordingly, IP due diligence is often relegated to the end of the checklist and, as a result, is addressed inadequately or in a last-minute manner. Not surprisingly, there are numerous cases in which an oversight in intellectual property matters has caused the buyer's or the seller's position to be seriously compromised. Thus, IP due diligence is necessary to avoid costly mistakes and properly determine the value of business transactions involving IP.

3.8

Innovation risk management – evaluating your freedom to operate

Karri Leskinen, Borenius & Co Oy Ab

Everlight signed a non-exclusive cross-licence agreement with Osram on 25 March 2009, providing the companies with access to certain areas of each other's patented LED technology.

On 9 July 2007, under the terms of a worldwide royalty-bearing agreement, Ericsson granted Samsung a non-exclusive licence under Ericsson's patent portfolio for the 2G and 3G mobile telephony standards to develop, manufacture and sell 2G and 3G subscriber and infrastructure equipment. In return, Samsung provided Ericsson with a royalty payment and a reciprocal licence under Samsung's valuable patent portfolio.

In non-exclusive cross-licence agreements parties to the agreement obtain substantial freedom to operate (FTO) under some of each other's intellectual property, to conduct research and develop the products and methods further. Such

agreements have become common practice in certain sectors, especially in the pharmaceutical sector and in electronics. In order to avoid litigation, companies seek to ensure that their products, processes and services do not infringe on the patent rights of others. Litigating patents is always risky, because the end result is uncertain and the amount of damages and legal costs that must be paid to the patent owner is typically higher than the licence fee would have been.

In our experience, there are certain methods available when planning for strategies culminating in freedom to operate. Small or medium-sized companies especially, without adequate patent portfolios to make cross-licence agreements, should carefully consider these methods when planning their product and marketing strategies. The importance of innovation risk management should be well understood by all firms, regardless of their size.

Innovation risk assessment – minimizing risks

Innovation risk assessment is the hot topic in innovation management at the moment. It is a new broader view on FTO analysis. Typically, a normal FTO analysis is a type of patent search, in which your opportunities to enter the market are evaluated in view of found patents. Innovation risk assessment is something that should be performed much earlier, before the product has even been developed. In innovation risk assessment, the focus is not only on finding patent rights that can potentially restrict your business, but on giving you an overview of the technological field you are working in. You may also get further information on your competitors, what alternative technologies might be entering the market and where your competitors are most active. Innovation risk assessment may even reveal potential new opportunities for you.

What makes the innovation risk assessment so vital today is the economic downturn, during which companies have to consider carefully where to invest. In technology-based companies, it is crucial to know which R&D projects have a high risk of failure. However, the evaluation of potential risks relating to new ideas is not an easy task. For example, when starting new R&D projects, CEOs and CTOs have to make decisions on investing in significant development and employee resources. It is important to make these decisions based on facts and information, not a gut feeling.

Planning the development, production and launch of a new product or entering a new geographical market area is as much a matter of forecasting future market developments as it is of minimizing risks. A major risk for any technology company is that the commercialization of a new product or technology may be blocked by a competitor holding a patent on a technology that is incorporated in the new product. This is why companies, prior to launching a new product and even prior to initiating a new line of research that may lead to the development of a new product, should seek to minimize the risk of infringement by securing their freedom to operate, ie ensuring that the commercial production, marketing and use of their new product, process or service does not infringe the intellectual property rights of others.

A worst-case scenario would be that a company first spends years on developing a new product, starts a massive marketing campaign, and only after launching the new product receives a warning letter indicating that the product is infringing someone's patent. In such a situation all the money and effort put to the development work could go down the drain. Therefore, the evaluation of freedom to operate should be a permanent part of the development process, and an FTO check should be done more than once. It should be done at least in the early stage of the development before a considerable amount of time and money has been spent on the process, as well as at a later stage when the final product or process is known and you can accurately compare your product or process to the patented products or processes. In such patent checkpoints, one should evaluate freedom to operate as well as the potential for patenting one's own ideas generated during the development process.

A good FTO analysis should give you sufficient ground for decision making on R&D projects as well as market entry.

Evaluating your freedom to operate

Owing to the huge volume of patents in almost all technical fields, evaluating your FTO has become maybe even more important than protecting your own innovations. Companies should therefore carefully review their innovation management systems to ensure that they have the required tools and processes for innovation risk assessment.

Carrying out an FTO analysis begins with a search of patent literature for issued patents and pending patent applications and obtaining a legal opinion on whether a product, process or service may be considered to infringe patent(s) owned by others. FTO analysis can be done, and it is recommended that it is done in steps. In the first step, an overall view of the patent situation should be obtained in order to provide a rough estimate of the patent landscape in the selected technical field. Then a more detailed patent search and analysis should be performed in order to identify potential risks, ie patents that might be harmful. Only after this point, when the number of patent documents is reasonable, should one start to evaluate the validity of the patents, their territorial coverage, and interpretation of the claims in view of the law in each country.

Many companies rely on IP firms that offer FTO analyses as part of their legal services to clients. It is highly recommended that companies use these specialized patent attorneys in IP firms, because the interpretation of the patent claims requires technical understanding as well as in-depth knowledge of national patent law and patents in general. In difficult and important FTO cases it is advisable to use local patent attorneys in each country for making the analysis.

An FTO is only an assessment on risk levels, and absolute certainty in regard to FTO will never be attainable. However, there are ways of minimizing risks, and these could save a company significant costs. A good patent search may provide a company with some indication that a new product is unlikely to infringe on third-

party patents, but, as there is a practical limit to the time and money that can be spent on a search, no patent search is perfect.

Managing innovation risks

If the FTO analysis reveals that there is a patent, or patents, that limits your freedom to operate, your company will have to decide how to neutralize these risks. The decision how to neutralize patent risks is always a strategic business decision, and therefore you should consider the overall situation and not just what risks the specific patent poses.

Although you might acquire the detrimental patents, acquire them together with some part of the company that owns the patent rights, or even buy the whole company, the more common neutralization strategies used are the following:

- *Neutralization by in-licensing or cross-licensing*. Licensing may be the most obvious and simplest way of clearing the ground for the commercialization of your new technology. The risks related to licensing can be minimized by careful consideration of the terms and conditions of the licence. However, in the end, the convenience of such agreements will depend largely on the licence fee. By cross-licensing you may save money, but cross-licensing requires that your own patent portfolio has value to the other party.
- *Neutralization by designing around*. A second alternative for neutralizing a detrimental patent is to design around the patented invention, which can often be done without significant costs if the company is aware of the detrimental patents in the early stage of the development process. If potential risks are found only after completion of development of a new product, it might be very costly to start over and design around detrimental patents.
- *Neutralization by cooperation.* In the European Community (EC) there is an intellectual property (IP) exhaustion doctrine under which the owner of an IP right cannot prohibit the further commercialization of goods protected by this right once the goods have been put on the market by the owner or with his or her consent. This means that once the patent owner has sold the patented product anyone can freely use it or sell it further inside the EC. If the detrimental patent is directed to a product that is only a part of your end product, you might consider buying these parts of the product from the patent owner instead of manufacturing them yourself. This way you would not infringe the patent if your products are sold only inside the EC.
- *Neutralization by invalidation.* Not all granted patents are valid. The examiners in the patent offices have a limited time to examine the patent applications, and sometimes patents are granted although there is prior art that may destroy the novelty or inventive step of the patented invention. This could lead to a situation where the patent is invalid in full or in part. It is important to understand that a partial invalidation of the detrimental patent may be sufficient to ensure your freedom to operate. For example, a patent could contain process and product claims. If your company is using a process that is different from the one

claimed in the patent, it would be enough to invalidate the product claims to ensure your freedom to operate.

The neutralization strategy should always be in line with your business strategy. For example, if in-house R&D work has a key role in your business strategy, licensing might not be the best choice for you, but you should consider designing around. On the other hand, if you are involved in open innovation, licensing should be your common practice, while, for those starting a new business, cooperation might be the easiest way to proceed.

Invalidation as a means of neutralization is dependent on the existence of prior art, as you obviously cannot create prior art for invalidating a patent. The strategic decision is what to do in case such prior art exists. You may actively start opposition or invalidation proceedings and try to invalidate the patent, or you could keep the information of the prior art documents secret and use them only if the patent owner attacks your company. Leaving the patent in force might be wise, because it might keep third parties from entering the market.

Potential opportunities

Conducting an FTO search and analysis is not only useful for risk assessment, but it may also reveal interesting opportunities. A patent search gives a lot of information about what your competitors are doing, as well as general trends in a particular technology field. It is especially important to bear in mind the general limitations of patents, because they may offer potential opportunities:

- *Patent protection is territorial.* There are no world patents. Companies have to make strategic decisions about the countries in which they will seek patent protection, and typically their technologies are protected only in their main markets. This leaves the technology in the public domain in other countries, providing an opportunity for others to commercialize the product in those countries.
- *Patents have a limited lifetime.* Patent protection is in force for a maximum period of 20 years, provided that the annual fees in each country are paid. After the expiry of the patent, it is considered to be in the public domain and may be freely used by others. Interesting opportunities may be revealed where a certain patent has been allowed to lapse before the maximum period of 20 years or in cases where the patent is maintained only in some countries.
- *Patents have limited scope of protection.* Patent claims determine the scope of the patent, and aspects that are not covered by the claims are not considered to be patented. The interpretation of the wording of the claims may vary from country to country, especially in regard to the equivalence interpretation that is carried out in some countries. It is important to bear in mind that the determination of the scope of a patent requires considerable skill and experience in interpreting the claims. For a good analysis one has to familiarize oneself with the written specification, the prosecution history, the case law and other relevant aspects.

Protecting your technology

When evaluating your freedom to operate, the most important thing to remember is that your own patents do not provide you with the right to commercialize the patented technology. A patent gives you only the right to exclude others from utilizing the protected invention, but does not ensure your freedom to operate. It is possible that your patented invention is infringing a patent owned by your competitor or someone else. For example, you may have developed a new process for manufacturing a known product and obtained a patent for the process. However, someone else might have a patent for the product and thus the ability to block you from commercializing your own product.

Despite the above, patents are powerful business tools and they can be used to improve your freedom to operate. Patenting may not explicitly clear the way for commercialization, but it should always be a strategic business decision that gives you a competitive advantage and may also prevent problems at a later stage. Patents give you an exclusive right to your invention and can thus create a legal monopoly in the market. You can also use your own patents for cross-licensing, and by patenting your own inventions you will also ensure that no one else will be able to obtain a patent for your invention. This could also be done by so-called defensive publication, which is one way of improving your chances of freedom to operate. Defensive publication means that you put your development results in the public domain without patenting them yourself. Typical ways of effecting defensive publication include publishing your inventions in a scientific article or in a seminar or simply disclosing them on your website. This prevents others from patenting the same invention at a later stage.

Conclusion

Innovation risk assessment is the hot topic in innovation management at the moment. In technology-based companies, it is crucial to know which R&D projects have a high risk of failure. Therefore, checking one's freedom to operate should play a significant role in the risk assessment of any technology company. Evaluation of freedom to operate should be conducted when entering new market areas or when launching a new product. Patent checks should be routine procedure in all development processes. A well-organized regular FTO check can reveal many risks, and once these risks are recognized you can make a decision on how to neutralize them.

An FTO analysis may also reveal potential opportunities for you. A thorough patent search gives you information on the latest technology trends as well as information about what your competitors are doing. The FTO analysis might reveal a weakness in the protection of some interesting products on the market, giving you an opportunity to enter the market with similar products.

3.9

IP risk estimation and management: the example of patents and patent portfolios

William E Bird, Bird Goën & Co

In times of recession, potential extra costs and loss of value need to be included within risk management. Risk management of patents is one important example of intellectual property rights (IP). A patent is a property right but the validity of a patent may be challenged at any time. For this reason a patent has been called a probability right – a property right with only a certain probability of being valid. Hence, there is a legal risk of invalidity at all times. This starts with the patent application, whose validity is in question until the patent is examined and then granted or 'issued'. The legal risk can be reduced by doing searches for relevant disclosures (ie sales, publications, verbal presentations, etc) or prior art and adapting the patent application and its claims accordingly. The legal risk can also be reduced by obtaining grant of the patent in different

jurisdictions, eg Europe, the United States and Japan, as the different examiners at the various patent offices will apply different prior art and hence a more balanced view is obtained.

However, even after grant, there is still a risk of invalidity. This can be reduced greatly if the patent is challenged unsuccessfully in a serious opposition procedure or before a court. If such a challenge does not happen, the remaining risk can be estimated, eg by applying actuarial ruin theory. If a patent is revoked (declared invalid) then it is 'ruined'. Attempts to invalidate the patent can be assumed to follow a model, eg stochastic processes that vary randomly in intensity. Only if the intensity exceeds a certain level will the patent be destroyed. Such a stochastic process leading to ruin can be modelled mathematically. An idea of the rate at which invalidation attempts reach this ruining intensity can be estimated from the opposition procedures at the European Patent Office (EPO). Opposition is raised against about 5 to 6 per cent of all granted European patents. In a third of the cases the patent is revoked. Hence the rate of effective oppositions is about 2 per cent of all granted patents. This risk factor can be applied to all patents in a portfolio and, if the financial value of the portfolio is known, the financial risk of invalidation can be estimated. If necessary an attempt can be made to insure against this residual invalidity risk.

The commercial risks

Besides the legal risk there are also commercial risks. These may be categorized into technical risks (that an invention cannot be implemented successfully or economically for technical reasons), market risks (that there is no market for the invention) and timing risks (that an invention is made available at the wrong time for the market). Technical risks are clearly in the domain of the applicant of the patent. Market and timing risks are more complex, as they relate to how an invention is received by third parties in the marketplace. A valid patent must satisfy the requirements of novelty, inventive step and industrial applicability. The legal requirement of novelty is that the claimed subject matter has never been disclosed in any form to the public without a confidentiality restriction in any language anywhere in the world. Hence all patents are about possible future technologies. Predicting the future is notoriously difficult and so is predicting the value of a patent.

An idea as to value of patented technologies can be obtained from the licensing efforts of universities, for which considerable information is available publicly. What is noticeable about the value of patents based on accumulated licence revenues is the skewed or asymmetrical nature of these revenues – and hence in the value of the patents. An example of a US patent portfolio from a well-known US university is given in Figure 3.9.1 taken over a period of 25 years showing the cumulative revenue for each patent. The range of revenues is over a span of four to five orders of magnitude!

Some results obtained from these statistics are interesting:

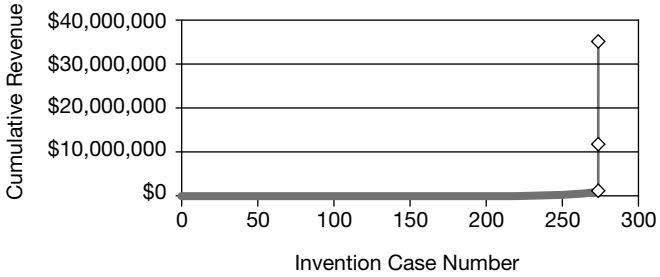


Figure 3.9.1 Cumulative revenue from a US university patent portfolio over 25 years
Source: Investigation of High-Value UCLA Patents AUTM 2005 Regional Meeting, 3–5 February, Arizona, Ken Polasko, UCLA Office of Intellectual Property.

- From the 270 cases (involving 400 issued patents) reported in Figure 3.9.1, 160 provided no revenue at all. These cases had only generated patenting costs. That is to say, about 60 per cent of the patenting effort resulted in negative return on investment.
- Only a few of the patents brought in significant figures, say above $500,000, ie about 2 per cent. That is to say, 2 per cent brought in over 90 per cent of the total cumulative revenue.
- Assuming about $50,000 for the costs of patenting alone, only about 10 per cent brought in more than they cost to patent – never mind the development costs. These figures have been confirmed in principle in other studies.
- A rather shocking fact from these statistics is that significant success occurs with a number of patents that is outside three times the standard deviation from the mean – that means success is an unusual result and statistically unlikely!
- There are a very few big hitters. The whole patenting exercise is dependent for its success on just a very few development projects – a hallmark of a risky business! One rule of thumb is that only one patent in a hundred has a value greater than $5 million.

In fact this kind of statistic is very difficult to manage. One way of portraying the difficulty is to compare patents with other well-known traded items that form a basis for investment like stocks, bonds and shares. The so-called Moody ratings are given in Table 3.9.1.

Figure 3.9.1 shows that 160 out of 400 granted patents (40 per cent) provided no revenue, ie at least this number defaulted. If one looks at the rate of default according to the Moody ratings over a relevant period of time (eg 20 years), the results displayed in Figure 3.9.2 indicate that a default rate of at least 40 per cent would be in class B or possibly in one of the C classes. All these are rated as 'below investment grade': 'very speculative', 'substantial risk', 'very poor quality'. Note that this does not mean that patents are not a valuable item; what it means is that they are not items that can be traded in a normal way. This is one reason why a market in buying and selling patents has grown only slowly.

Table 3.9.1 Comparative Moody ratings of well-known traded items

Moody's rating	*Definition*	*Notes*
Aaa	Highest rating available	Investment grade bonds
Aa	Very high quality	Investment grade bonds
A	High quality	Investment grade bonds
Baa	Minimum investment grade	
Ba	Low grade	Below investment grade. 'Junk bonds'
B	Very speculative	Below investment grade. 'Junk bonds'
Caa	Substantial risk	Below investment grade. 'Junk bonds'
Ca	Very poor quality	Below investment grade. 'Junk bonds'
C	Imminent default or in default	Below investment grade. 'Junk bonds'

Another statistic that can be generated from the reported material is that, although revenue is earned early for most of the patents that are successful, eg in less than 12 years from filing, some are still earning 19 years after filing, and some started earning first after 15 years. A technology must be the right one at the right time. That is, there is a 'window of opportunity'. If this is missed – by being either too late or too early – then the patent value is lower or non-existent. From experience, this window can occur at any time during the 20-year life of a patent. This makes it hard to decide when to abandon a project – maybe it will be successful next year! This uncertainty makes patents a very difficult type of business to manage. It is a risky gambling problem rather than a linear relationship between work input, investment and return. It is difficult to decide if a patented technology will be successful and when it is going to be successful. Such a skewed distribution would appear to require very special management techniques if a patenting policy is to be financially successful.

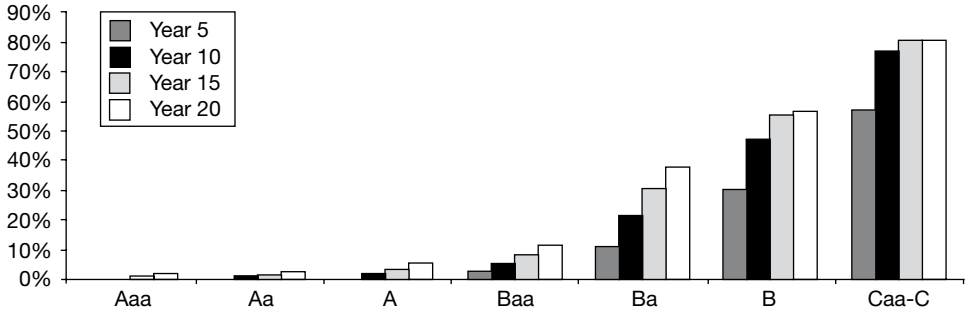


Figure 3.9.2 Cumulative default rates by rating categories, 1970–2001
Source: Understanding Moody's Corporate Bond Ratings and Rating Process, May 2002.

The patent portfolio

One approach to this type of risk is to rely on numbers – the patent portfolio concept. If one patent in a hundred is worth more than $5 million – then let's have a lot of them. Table 3.9.2 gives the top filers of patent applications at the EPO in 2006. Filing over 3,200 patent applications per year means over 15 per working day. This requires not only the necessary research and development personnel but also an organization able to capture these inventions and convert them into patent applications. This is patent portfolio management on a grand scale!

With a larger number of patents in a portfolio, the variation in average value is less. A well-publicized statistic from IP Bewertungs AG is shown in Figure 3.9.3. Here the value is given in thousands of euro. This suggests that a typical value will be about €55,000–65,000 per patent – very consistent with actual average value that can be derived from Figure 3.9.1.

For a novel and ingenious alternative to the use of the patent portfolio concept, see the UC Berkeley–Novartis agreement discussed in the box below.

> Novartis, through its subsidiary Novartis Agricultural Discovery Institute, entered into a five-year contract with UC Berkeley's Plant and Microbial Biology Department in 1998 for $25,000,000. The contract was with the entire faculty. The university owned the IP but Novartis had the first right to negotiate. Novartis also had the right to review all of the research whether funded by Novartis or by a government or public source. Novartis had an option to negotiate a licence for up to one-third of any of these discoveries annually. Novartis could cherry-pick the ones it wanted. The contract clearly makes use of the known statistics on patent value from academia (see Figure 3.9.1). Novartis obtained through the contract the right to review a large number of projects but was allowed to select only a few of these to negotiate a licence. This allowed Novartis at least the theoretical possibility to forgo the cost of building up a patent portfolio with only a few big hitters and instead to cherry-pick the best.

Table 3.9.2 The top filers at the European Patent Office, 2006

Rank	*Company*	*Applications filed*
1	Philips	3,222
2	Samsung	2,478
3	Siemens	1,850
4	BASF	1,474
5	Matsushita	1,395
6	Robert Bosch	1,166
7	LG Electronics	1,080
8	Sony	929
9	Nokia	873
10	Fujitsu	819

Source: European Patent Office.

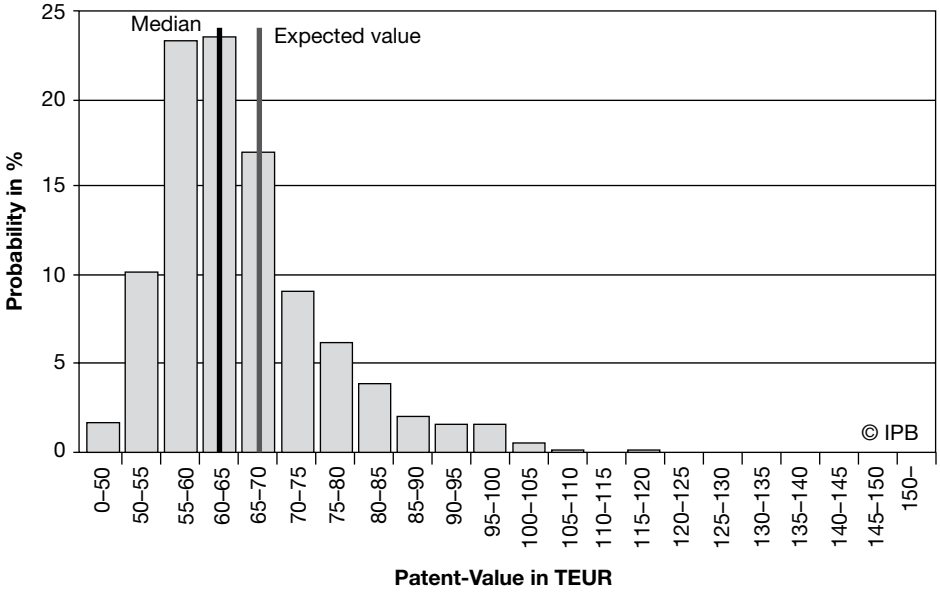


Figure 3.9.3 Patent value (in €'000)
Source: Monetary-Patent-Valuation: The certified IPB-Model, IP Bewertungs AG.

The small and medium-sized company

The accruing of a large-scale patent portfolio is obviously very difficult for small companies and for individuals. Here there is a David-and-Goliath situation; one has to hope that the few patents one has will prove effective to stop giants in their tracks. The risk of making a mistake can be reduced by detailed technical, legal and market analysis. Extensive legal and technical evaluations can be expensive.

The skewed nature of the value distribution (see Figure 3.9.1) makes the use of analytical tools such as the Black–Scholes formula (which relies on a normal distribution of both increases and decreases in value) inappropriate. An alternative is real options analysis. This technique is considered to be expensive (eg about €100,000 if done in detail) and only suitable for high-value patents such as those for pharmaceuticals.

In using real options analysis, greater security can be obtained if a patent portfolio or patent family is considered. The distribution of Figure 3.9.3 is then often approximated by a log normal distribution that fits well to real options analysis as there are no negative values.

Other valuation schemes have been proposed that rely on a less costly retrieval of information. An example of such a methodology is the use of value indicators, eg as proposed by IP Bewertungs AG and others. However, as this method relies on a certain statistical relationship between the value indicators and patent value, the method is recommended for larger numbers of patents, eg patent portfolios or patent families.

The individual patent remains a tough risk to assess – not only for the owner but for any third party as well.

The future – patent auctions

In the last few years it has become more common to auction off patent portfolios. Once this has become well established there will be more market data available on how patents behave as a traded commodity. This should, in the long term, result in better data for the assessment of patent value. The patent auction, if successful in the long term, should also allow a return on investment to be obtained with a reduced transaction cost in comparison to licensing the patents or implementing the technology oneself. This will in itself provide one escape route to reduce financial risk.

The spectre of third-party patent infringement

A risk for any company implementing a technology – whether patented or not – is the possible infringement of third-party patent rights. A patent is an exclusive, absolute and negative property right. A patent is not an acceptance to implement a technology. A patent provides the negative right of excluding others from technology defined by the claims. It is an absolute right; whether you knew of the patent or whether you copied or invented the technology yourself independently makes no difference.

The classic approach to guard against patent infringement is a freedom-to-operate (FTO) analysis. Once the exact commercially relevant design for a technology to be implemented is known, a search can be made in patent databases to identify dominating patents. As patents are national rights, patents of each country where a patented technology will be made, offered for sale, sold, used, stocked or imported must be considered. Such a search is often not easy to carry out, as keyword searching depends for its success on the choice of keywords. As different patent drafters may use different words for the same thing, choosing the right keywords is best left to a person with experience in searching and in the relevant technology.

Generally, broad search terms will be included to try to catch all relevant patents and patent applications. This will result in a certain amount of noise – hits that are not at all relevant. Do not be surprised if you get several thousand hits to analyse. The strategies for carrying out FTO analysis usually involve a series of cuts. With each cut the number of documents left to analyse is reduced, but the effort per document increases with each cut as the relevance of the documents increases.

If any documents are still left after the last cut, these will have to be considered in detail. Are the patents valid? Does the intended product or method fall under the claims? Can a licence be obtained or is it possible to design around?

FTO analysis can be expensive and time-consuming. As one is trying to prove a negative, there is always the possibility of missing something. A safety net for attack by competitors can be provided by a large patent portfolio. If a competitor

attacks for patent infringement, one may have a patent that the competitor infringes. Such a situation can lead to a cross-licensing defence. Such defences are used often by large corporations with big patent portfolios.

The cross-licensing defence usually does not work against individual inventors or against patent trolls. Both of these probably have no products that they sell; hence there is nothing that could infringe a patent of the defendant. The danger of this type of court case is magnified many times in the United States by the US court system. A patent troll or an individual inventor may obtain the services of an attorney who works on a contingency basis. This reduces the costs of the plaintiff – an option normally not available to the defendant, who is left to bear the heavy costs of legal defence. Either one defends against the patent infringement court case (eg by showing that there is no infringement or the patent is invalid) or one tries to come to the most economical settlement.

For small companies with too few patents for a cross-licensing strategy the outlook is grim. One may well be in 'bet-your-company' litigation!

Sometimes a major mistake is made with FTO – see the box on the Polaroid versus Kodak litigation. To deal with this risk, an option that has often been courted is that of patent infringement litigation insurance. Patent insurance pays a company for all or a part of the losses incurred if the company infringes, or is accused of infringing, someone else's patent. Presently, offers to provide such insurance are limited, and any that exist are likely to be expensive. No EU member state has any legislation on patent litigation insurance that might, for example, make it compulsory. A study of this topic has been made by the European Commission and a final report issued in January 2003: *A Study for the European Commission on Possible Insurance Schemes against Patent Litigation Risks*. The interested reader is referred to this extensive report for further details.

For 30 years, Polaroid built and dominated a worldwide market for instant photography. Kodak wanted to get into this market and produced its own design. It considered that it had FTO as this design did not infringe Polaroid's patents or otherwise these were invalid. Unfortunately for Kodak, the patent infringement court disagreed and in 1985 decided that Kodak had violated Polaroid's patents for instant photography. The decision ended a nine-year legal struggle between the two photography giants. The final damage award to Polaroid was $924.5 million. Ironically, digital photography dealt Polaroid a fatal blow; in 2001, it filed for bankruptcy.

THIS PAGE IS INTENTIONALLY LEFT BLANK

4

Operational Risk Management

LRQA BUSINESS ASSURANCE

HELPING YOU MANAGE YOUR RISKS

Today's risk management is about delivering the confidence needed to ensure that stakeholders' expectations are met; to know that key business risks are under control and provide the security of future performance in today's uncertain world.

This is why at LRQA our approach is different. LRQA's risk management support - Business Assurance - is designed to help you ensure that your systems are identifying and driving down critical risks to deliver real improvements in the eyes of your critical stakeholders.

Business Assurance is our approach to management systems assessment. It focuses on developing effective and efficient management systems giving your business the confidence it needs to thrive and grow.

By understanding your business and your goals, we are able to work with you to accurately pinpoint the key areas that need to improve, helping you turn risks into opportunities and weaknesses into strengths.

With Business Assurance, you can feel confident about your future.

To find out how LRQA can help you,
visit us at: www.lrqa.com,
contact us at: enquiries@lrqa.com
or call us at: +44 24 7688 2373

Lloyd's Register Quality Assurance is a member of the Lloyd's Register Group

LRQA
Measure the Difference

4.1

Embedding risk management and systems

David Lawson, Lloyd's Register Quality Assurance (LRQA) and Nathan Skinner, StrategicRISK Magazine

Risk management is the discipline by which organizations identify, assess and prioritize risks and subsequently intelligently apply resources to monitor, control and ultimately mitigate those threats. As evidenced by the banking crisis of 2008, risk management is not something that can be siloed into a single department. In order for organizations to successfully minimize the impact of unfortunate events they must take an enterprise-wide approach to risk management. This involves embedding a system and culture of risk management across the entire organization.

Management systems are the pre-eminent tool that the best organizations use to embed processes for ensuring that products and services are consistently and reliably delivered. Through the implementation of management systems in key risk areas such as quality, environment, and health and safety, organizations create an internal control environment where vital company functions are constantly

monitored and improved. Quality management systems can help deliver many business improvements, all of which help an organization to manage its risks successfully. In this chapter we will examine how quality management systems, both explicitly and implicitly, support and provide a framework for an organization's risk management process.

Boosting the risk management process

There are now many different standards defining the essential aspects of management systems, which provide the framework and tools to help organizations to design and manage business processes (ISO 9001), health and safety procedures (OHSAS 18001) and environmental concerns (ISO 14001). The elements laid out in each of these standards help to support a systematic approach to risk management. Furthermore, independent assessment and certification of a management system can help to improve the effectiveness and efficiency of the risk management process. In today's tough operating environment, organizations are increasingly seeking to have their management systems independently certified to help improve their ability to identify and manage risk, and consequently provide confidence to their stakeholders.

ISO 9001 provides the framework to enable a company to reliably deliver quality products and services. It also helps organizations to embed a process framework to effectively manage the risks that would prevent them from meeting their customers' needs and expectations. A certified company is required to systematically plan its activities to deliver those high-quality goods and services on time and, critically, to take preventative action to identify the potential risks that would prevent it from doing that. In order to do so, the organization must take a risk-based approach. During the process of certification, the organization is asked to identify what could go wrong, analyse those risks, evaluate them and, if necessary, treat them. In so doing, the organization has by definition gone through the traditional risk management process identified earlier.

One of the biggest risks facing most companies at present stems from economic uncertainty and increasingly difficult credit conditions. Data from previous economic downturns support the fact that certified quality management systems help organizations to meet their customer expectations reliably and on time, create market advantage and boost competitiveness. Critically, the process improvements achieved through certification can also significantly reduce costs and improve quality, thereby increasing the likelihood that a company exceeds its contractual obligations, gains repeat business and builds trust with customers. All this can help a company to survive and thrive, even in difficult market conditions.

Health and safety

In addition, recent updates to management system frameworks help organizations to address specific risk issues. OHSAS 18001 (Health and Safety) and ISO 14001 (Environmental) take an even more explicitly risk-orientated approach to ensuring

quality. For many manufacturing and industrial companies, health and safety is the most significant operational risk to which they are exposed. Ensuring a safe working environment is a prime concern for any responsible employer; not only does it benefit staff morale and therefore increase productivity, but it also helps to prevent accidents and limit liability claims. An injury at work, whether sudden or incurred over time, if found to be the fault of the employer, can lead to potentially crippling liability claims. Certification to OHSAS 18001 clearly states that measures should be taken to identify, assess and implement controls to limit or mitigate the health and safety risks that the organization faces. In other words, OHSAS 18001 is designed to identify, treat and control those health and safety risks that the organization considers worthy of attention.

Business reputation

Managing and maintaining one's reputation is another significant risk facing all organizations. When it comes to reputation, in today's eco-sensitive and media-saturated world, environmental performance is one of the most important business considerations. Sustainability is the flavour of the month, and no longer can organizations expect to escape public, shareholder and media scrutiny if they ignore their impact on the environment. ISO 14001 helps organizations to manage and continuously reduce their environmental impact. As above, it teaches organizations to systematically look internally, as well as up and down their supply chain to evaluate, assess and manage the risks associated with poor environmental performance.

Cost reduction

In a tough economic environment there is a significantly heightened emphasis on eliminating costs within the organization. Companies are sometimes concerned that the costs of implementing management systems outweigh the benefits. With businesses looking for ways to make cutbacks it could be hard to secure the funding for such a project. But the costs of getting certified should be balanced against the potential for losing business without effective management controls and the external credibility that it provides. The benefits of a certified management system should not be understated. ISO 9001 certified organizations report cost savings of between 5 per cent and 30 per cent resulting from improvements in company practices.

Shrinking markets

Another significant business risk emphasized by the recession is a shrinking market for a company's products and services. Identifying new opportunities and holding on to existing contracts become critical business imperatives during periods of economic contraction. Certification through an accredited provider offers organizations benefits above and beyond the basic compliance requirements. The additional credibility of working with a globally recognized certification body enables

suppliers to tender for contracts with large, global organizations that accept certificates only from a select number of accredited third parties.

Operational risk

Operational risk remains a huge threat to companies, and one that is significantly affected by the economic downturn. Many insurers report receiving an increase in the number of fraudulent claims during a recession. As people are forced to scrape by for money, some of them turn to unscrupulous means in order to get it. Launching a fraudulent personal injury claim against a company or exaggerating the extent of an injury are among the methods adopted. Certification to OHSAS 18001 helps ensure that your organization is addressing health and safety concerns transparently in an internationally recognized manner and helps to protect you against fraudulent insurance claims. Furthermore, ISO 9001 helps businesses to avoid the risks associated with defective products, another area of litigation adversely affected by the economic downturn. Staff motivation also emerges as an important benefit of using quality management systems. This is even more important during a recession, when morale is a serious risk issue, which is unlikely to be buoyed by a challenging financial environment.

Communication of risk information

Communication is another valuable benefit derived from such structured approaches to management systems. If implemented correctly, the system helps build interpersonal communication between managers and employees. This is also likely to benefit the risk management process. Risk communication is the idea that people are uncomfortable talking about risk. Company managers sometimes think that there is no risk in their department and to say there is would be to challenge their ability as managers. By building management and employees' communication skills and providing a clear system of risk documentation, management systems may help resolve these kinds of political conflicts. Better documentation and dissemination of risk information company-wide will also improve the quality of decision making.

A full and complete understanding of risks is fundamental in an organization's ability to manage them effectively, and this relies on sound, up-to-the-minute information. By providing the framework for information gathering and exchange, a management system invariably boosts the risk management process. Decisions based on risk information backed up with the data to prove it will not only allow companies to make the right risk-based decisions, but it will also avoid them wasting time on risks that have been misjudged or overemphasized.

Transparency of business processes

The improved transparency of business processes, achieved through rigorous auditing and review, which robust management systems enable, helps a company identify critical dependencies within its supply chain that, if compromised, could have

devastating consequences. It could be that there is a critical link in the supply chain that, were it to fail, would present a catastrophic loss for the organization. With a properly embedded management system, the organization is able to deploy the appropriate level of controls to prevent this from happening or, if it does, have in place a contingency plan or financing to plug the gap. In so doing the management system fundamentally supports and delivers the risk management process.

Certifying the risk-based approach

In the past, some certification bodies have been guilty of adopting a purely compliance approach when it comes to signing off on an organization's implementation of its quality management system. However, this approach does not support an organization's efforts to expand upon these compliance requirements to design a system uniquely suited to its own operating environment. Today, leading certification bodies take a different approach, which revolves around assessing the risk-based approach already mentioned and assuring the data and systems that an organization has in place.

This approach, taking into account elements unique to the organization, is concerned with ensuring that the design of a system supports the enterprise-wide risk management process. As we have seen, a properly embedded management system becomes the framework and mechanism through which risks are identified, analysed and treated. Certification takes into account the measures the organization has adopted to do this, as well as helping to identify risks and address them. The assessment also reinforces the need to continually improve the risk mitigation system and ensure that it is appropriate and sustainable.

Management system assessors, looking to certify an organization's business assurance approach, will examine whether or not these risk elements have been taken into consideration and handled appropriately. This process ensures that an organization has embedded the disciplines and routines to ensure it maintains control over its operations, has addressed the generic risks it faces and has put measures in place to manage them effectively. These are, for example, the standard requirements embedded in ISO 9001, such as levels of authority and approval of documents to ensure security, as well as performance monitoring to verify that systems are being implemented as defined. Business assurance seeks to identify whether an organization is managing the more specific organizational risks, and this comes from an understanding of how the organization is working in its particular environment. Taking this risk-based approach of identifying, analysing and treating will ensure that the organization is in a position to deliver consistently for its clients and customers.

Conclusion

Management system standards, such as ISO 9001, ISO 14001 and OHSAS 18001, provide a comprehensive tool that can help any company establish a robust and

sustainable risk management framework and embed it throughout the organization. With the right application, which is enabling and not prescriptive, the system will help establish the discipline, procedures and methods to ensure that risks are appropriately identified, analysed, evaluated and treated. Clear documentation and auditing also make sure that this process is learnt and improved.

Risk management demands that a company looks into the future to see what could prevent it from delivering on its goals. The typical processes and controls embedded within a management system can help a company design a framework that will help it to manage many of the risks it faces. Reassuringly, many of the process improvements, cost savings, and reputation and safety enhancements that an organization realizes through an independently certified management system will be particularly pertinent during the current period of economic contraction.

4.2

Human factors in operational risk: the final frontier

Paul Saville-King, Critical Engineering Services, Norland Managed Services

Introduction

If you want to significantly, cost-effectively and sustainably reduce operational risk for your business I am confident the following concepts could change the way you think about risk for ever.

Each of the following statements has been repeated to me in some guise or another: 'I have a Tier IV facility so it's nearly impossible to have an outage' and 'It doesn't matter who is operating my facility; we spent a fortune on designing it to be resilient.' Unfortunately, they are simply not true. Why is it that otherwise sensible corporations just don't get that a few hundred million 'design dollars' spent on systems and technology don't actually prevent a new hire, inappropriately inducted and poorly trained, being in a business-critical area and pushing the wrong button at the wrong time, thus shutting down a facility? People – or the human factors that

Winning Team; 'Operational Team of the Year' with Morgan Stanley.

Does a wise investment make a good investment?

YES.

It matters which mainenance company you invest in to safeguard your facility

M&E Maintenance | Critical FM | Projects | Structured Cabling | Fabric

Norland Managed Services Ltd is a leading provider of facilities maintenance and support services in the built environment, working in partnership with some of the UK's best known companies.

Norland operates all of their business critical operations through their dedicated Critical Engineering Services Division. This division contains all the resources you would expect to provide highly competent critical environment experts on an around the clock basis. There are dedicated chartered engineers on 24 hour call and these form the core of our incident response teams. Our incident response teams have access to preferred Critical Engineering and Risk Management (CERM™) supplier agreements, specialist labour and equipment and the highest levels of Norland management. Norland has developed a unique approach to Critical Engineering and Risk Management to reduce the softer people and process risks and the harder engineering aspects.

Norland Managed Services has signifi cant experience in the evaluation, maintenance and repair of highly resilient operations throughout the UK. This includes high specifi cation Tier IV data centres operated for global investment banking brands, state of the art data centres built for a global IT outsourcing organisation at a location outside the M25 and highly resilient operations supporting business critical corporate applications for Global FTSE 100 companies.

NORLAND

Your brand is safe in our hands

Norland Managed Services Ltd
City Bridge House, 57 Southwark Street,
London, SE1 1RU

www.norlandmanagedservices.co.uk

Contact: Anders Eklund T: 07786 197 792
E: Anders.eklund@norlandmanagedservices.co.uk

influence them – are that untamed, unpredictable, unknown quantity that, for some reason, most people in critical environments shy away from tackling.

Causes of failure

Our experience corroborates research pointing towards people and process failure as the major source of systemic infrastructure failure. This can be as much as 90 per cent of the root cause of an impact 'incident': serious numbers indeed. Addressing the underlying human factors can therefore significantly improve the odds of avoiding an outage.

Actually, if prevention is agreed to be better than cure then it can be seen from the above that there is clearly a significant opportunity to remove a majority of risk. Just how much probability is associated with particular human factors is now well researched, and proactive programmes to address these factors began with the airline industry following in the wake of a famous airline crash event. Shortly afterwards, other 'high-reliability organizations' realized that the 90 per cent drop in the incident rate in the airline industry was worth investigating. Now 'human factors training' is common language in airline maintenance and the nuclear and petrochemical industries and is growing in popularity even in fields such as specialist surgery. Its popularity has a direct correlation with the impressive incident reduction results obtained when human factors are addressed properly – in other words looking 'hard' at the 'soft' stuff.

Consider Table 4.2.1. You have roughly a 50/50 chance of doing something wrong if you are performing an unfamiliar task, at speed, when you are not 100 per cent confident of the desired outcome. If that sounds like a common business-critical situation or near-miss to you, then contrast that in Table 4.2.1 with a totally familiar task, performed often, by motivated staff, where the risk dramatically drops to just 0.04 per cent. This reflects trained, even scenario-drilled, engaged staff working in an environment that takes a long-term view of risk reduction.

Table 4.2.1 Situational probabilities

	Probability of failure
Unfamiliar task, at speed, no idea of outcome	55%
Complex task requiring a high level of comprehension or skill	16%
Restore system to new state following procedural checks	0.30%
Totally familiar task, performed often, well motivated, highly trained staff, time available to correct errors	0.04%
Respond correctly when there is an augmented supervisory system providing interpretation	0.002%

Based on a seminal piece of research by J C Williams in the 1980s: HEART – Human Error Assessment and Reduction Technique.

Table 4.2.2 Probability multipliers

Unfamiliar with infrequent and important situation	×17
Shortage of time for error detection	×11
Newly qualified operator	×3
Low morale	×1.2
Emotional stress	×1.3
Inconsistent displays and procedures	×1.2
Disruption of sleep cycles	×1.1

Multipliers must be factored and multiplied together for multiple conditions.

Just when you thought it couldn't get any worse, consider this. Condition multipliers can exponentially rack up the probability figures for lower-risk activities. Take 'unfamiliar with important and infrequent situation' as a factor; you can multiply an underlying 'task' risk by 17, thus putting it into the high-risk category (see Table 4.2.2).

Even in this 'ambiguous risk' there are harder and softer elements of concern. On the softer side and key to overall risk are influences of local culture and behaviours. This is the foundation that makes 'people and processes' work effectively and hence is a fundamental requirement for a low-risk, mission-critical operation.

The main elements illustrating culture were described by Johnson and Scholes as rituals and routines, symbols, organizational structure, control systems, power structures and stories (see Figure 4.2.1).

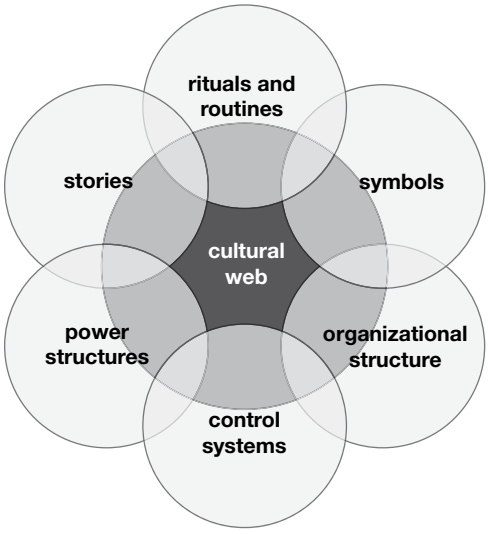


Figure 4.2.1 Cultural web

How can I judge my culture?

A simple way of describing culture is 'the way things get done around here'. Ask any new employee and they will sum it up for you. You may feel that culture is an abstract concept but in reality it is pretty simple to ascertain an accurate feel of culture by taking half an hour out of your day to walk around a facility, look around and talk to a few staff. You can soon see what is truly important. The rhetoric may be that risk mitigation is top of the agenda, but if key statistics, notice boards and other public displayed information are more focused on the next golf day, for example, than on mean time between failures (MTBF) or 'Top 5 mitigation objectives' it is easy to see where priorities lie in reality. Just as importantly, employees at all levels should at least be able to articulate some of the important initiatives in hand, explain core processes and share experiences on recent events. Bear in mind that culture is a complex thing and can be hard to change without concerted effort; sometimes you may also require additional expert support.

To help you make up your mind about your culture, consider the following key elements:

- *Stories:* the past events and people talked about inside and outside the company. Who and what the company chooses to immortalize say a great deal about what it values and perceives as great behaviour.
- *Rituals and routines:* the daily behaviour and actions of people that signal acceptable behaviour. This determines what is expected to happen in given situations and what is valued by management.
- *Symbols:* the visual representations of the company, including logos, how plush the offices are, and the formal or informal dress codes.
- *Organizational structure:* this includes both the structure defined by the organization chart and the unwritten lines of power and influence that indicate whose contributions are most valued.
- *Control systems:* the ways in which the organization is controlled. These include financial systems, quality systems and rewards (including the way that they are measured and distributed within the organization).
- *Power structures:* the pockets of real power in the company. This may involve one or two key senior executives, a whole group of executives or even a department. The key is that these people have the greatest amount of influence on decisions, operations and strategic direction.

Behaviourally, the most common issues that we see relate to problems such as a failure to tackle 'bad apple' individuals displaying the wrong behaviours, silo mentality between different shifts, departments, companies or service providers and finally a lack of risk awareness.

Culturally, the worst enemy of all is probably fear of openness. Recrimination and removal from site, often by overzealous management failing to think

through the impact, can lead to long-term cultural damage that will seed a future catastrophe.

Case study: How culture trapped a media company

A classic example of how culture affects risk was a middle manager afraid to approach his boss for capital investment of a couple of million dollars for an electrical infrastructure upgrade to rectify a known weakness. Despite his being fully informed about the risk and very aware of any potential consequences, budgets were tight and the perceived culture within the department was that performance was primarily judged on the ability to control annual budgets.

That conversation with his boss would have saved the company the multiple millions they lost through litigation, penalties and lost reputation. When his boss found out about his awareness of the problem beforehand he got fired, his boss had a hard time from the board, and the capital expenditure was fast-tracked through the system to prevent another outage.

This shows the importance of setting the right environment for decision making in critical environments and could have related to any industry sector.

What human factors look like

So what would training in human factors look like? We have now developed an industry-specific application of human factors training, and this can be relatively easily deployed in most situations. Human factors training focuses on the soft aspects of how individuals and teams work together. It covers culture, error concepts, working environments, procedural aspects, team working and communication. The full detail can be seen in Table 4.2.3.

Teams have reacted very well to this approach, and end users have seen and sensed an immediate change to the working environment and an improved level of confidence. To be most beneficial, the training should be delivered to the 'holistic' team, including service partners, management, administration, technical staff and other key stakeholders. Where this training has been delivered there is an improved level of risk awareness, risk visibility, and ownership with accountability and responsibility and, when an incident has loomed, the team have worked like a well-oiled machine. Of course, this depends on the underlying systems, processes, employee engagement and competencies being where they should be.

Table 4.2.3 Typical human factors components

Social psychology	Social, cultural and organizational environment
Human error	Slips, lapses, mistakes and violations
Error chain concept	Theories and models
Human performance and limitations	Fitness and health, stress, pressures and deadlines, workload, tiredness and fatigue, alcohol, medication and drugs
Physical environment	Noise, fumes, illumination, climate and temperature, motion and vibration, confined spaces, vertigo, distractions and interruptions
Procedures, practices and tasks	Following procedures, inspection and reporting, repetitive tasks
Information and technical documentation	Their use and importance
Communication	Effective communication, with and between teams, verbal and written, importance of handover, dissemination of information
Teamwork	Principles and benefits, the effective team, management, supervision and leadership
Professionalism and integrity	Individual responsibility, standards

Giving change a helping hand

Another key element of making sustainable change is being able to show progress and define your end game and, most importantly of all, being clear about cause and effect. I'm not talking here about failure mode and effects analysis (FMEA) or other such instruments, which are fantastically useful but well covered by many other more able commentators. I am talking about ensuring that basic principle of 'what you measure is what you get'.

All too often key performance indicators (KPIs) are aligned to measuring outputs such as mean time between failures, uptime, incidents and availability. These are great tools that show the operational performance in critical environments, but they do not reflect the need to focus on the priority risk prevention (or input) measures that will ensure the output measures stay healthy. Some of these leading measures actually give some significant warning about future potential for incidents as inputs are overlooked or poorly delivered. Examples of this include scenario training hours, drills, staff turnover, average length of service and training hours. Neglect these measurements at your peril, as they will give you a good indication of how robust the underlying operation is.

Conclusion

What does this all translate to in terms of the risk to your operation? Take a step back and have a think about this. Hand on heart, which one of the following describes you? 1) You have robust site processes but 'sense' a lack of buy-in and

'feel' the wrong culture. Are people hesitant to make decisions under pressure, or do they repeatedly make the wrong ones? 2) Your team is highly motivated, creative, proactive, open and willing but lacks clear guidelines and processes?

If you have a strong 'positive' culture and great processes, consider yourself one of the select few – the top 20 per cent. The frequently overlooked aspect of human factors – culture and behaviours – is often present through default rather than design. If you have a strong positive culture, protect and nurture it; if not, work on it – your facility could be up to 90 per cent less at risk as a result. Surely that is a result worth having.

4.3

Making risk management deliver business value

Ruth Murray-Webster and Peter Simon, Lucidus Consulting Limited

In this chapter we start from the position of accepting that risk management for business is a good thing, required by regulation and supported by standards (eg the IRM/AIRMIC/ALARM risk management standard or BS 6079-3:2000), methods (eg the UK Office of Government Commerce's Management of Risk – M_o_R®), tools (eg @RISK or Crystal Ball) and training supplied by a wide range of providers. Yet many organizations find it difficult to make a process that seems complete common sense work for them. They struggle to build the culture and working practices necessary to transform the rhetoric into reality. Why might this be? We have some experiences and insights to share that may help to make effective risk management a reality for you.

What does risk management really mean for business?

Our experience is that to really make sense of risk management for business it is necessary to go back to examining risk management from a life perspective.

Although standard dictionary definitions of the term 'risk' and our everyday use of the term suggest potential threat (something that is uncertain that, should it occur, would mean something bad for one of our objectives), common business parlance also embraces the notion of risk as an opportunity (uncertainties that would have a beneficial impact on something that matters). If you stop to think about how we as human beings look at the uncertainties around us, then it is easy to see that the process that is going on is a weighing up of chances (probabilities or likelihoods) and consequences (impacts or effects) and a resulting process that results in a decision being made on how to proceed.

So what risk management really means for business, we suggest, is summed up by these two questions: 1) How does your organization identify and manage those uncertainties (threats or opportunities) that have the biggest impact on business value (matter the most to you)? 2) How do you use this information to make optimal decisions in uncertain situations?

How published standards and methods help, and how they hinder

Published standards and methods can help in many ways. By using a common language and a step-by-step process an organization is able to provide a consistent, repeatable approach to risk management. This has the advantage that an organization has one way of working to teach or make people aware of, and no one has to 'reinvent the wheel' every time a risk assessment is undertaken.

The UK Office of Government Commerce's Management of Risk (M_o_R) is a good example of a publicly available method. Like most other risk management methods it is based around a series of steps or stages: identify context and risks (both threats and opportunities), assess or evaluate risks, plan responses and implement responses. M_o_R also recognizes that the risk management process needs to be embedded and reviewed, and that communication is essential.

With a common language and understanding of a structured method in place, businesses can move forward from random risk management, based largely on personal intuition, to a more formal process where there is a way for all interested parties to contribute to risk identification, assessment, response planning and management. Figure 4.3.1 identifies a typical risk management process.

We work with many organizations that have invested heavily in the adoption of a structured and standard process for risk management, yet many of these organizations perceive that this rigour gives them little more than administrative benefits. Yes, they 'tick the boxes' at audit and can be seen to be doing something – but is the risk management process working to create, or at least prevent the destruction of, tangible bottom-line business value?

Standards and methods are an essential aspect of risk management, the alternative being to make it up as we go along. However, most do not recognize two things. First, any process needs to be scalable, ie fit for use in any business context

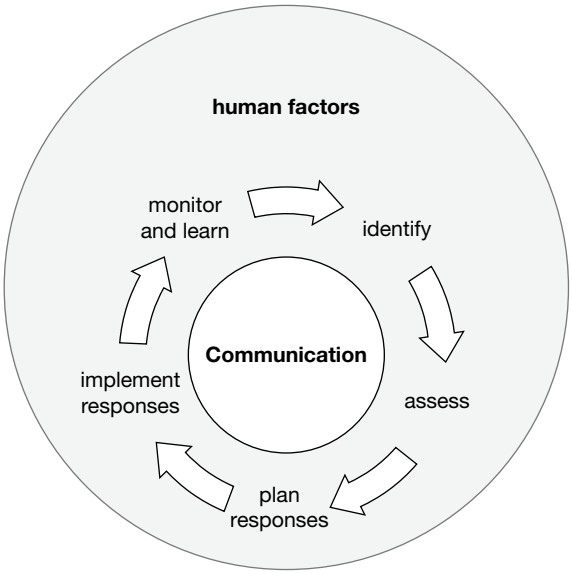


Figure 4.3.1 A typical risk management process

and therefore avoiding the 'sledgehammer to crack a nut' syndrome. Second, and most importantly, any process must overtly take account of the inherent human factors in the assessment of what is risky and what isn't, and the degree to which those things matter.

The complication of human factors

In the final analysis, individual people and groups of people make business decisions in uncertain situations. When making decisions those human beings weigh up the things that they perceive could happen, the chances and consequences and make a judgement. Although most people in business would attempt to be rational and systematic about this, it could be argued that, despite such attempts, 'risk is in the eye of the beholder'. Certainly, there are some situations where there is sufficient historical evidence and data for future situations to be predicted with some confidence; but different people will still put their own personal 'spin' on the data and the decision that is made as a result of it. Moreover, there is never enough information to predict future situations with certainty. Unless we are talking about situations of pure variability (like throwing an unloaded die or playing the lottery) where a mathematical probability can be calculated, there will always be residual uncertainty that could matter a lot to the business. These may be 'unknown unknowns' or 'Black Swans', as coined in the book written by Nassim Nicholas Taleb, or just uncertainties that are knowable but that we have failed to notice in the day-to-day thrust of our busy lives.

There is a wide body of academic literature underpinning the complications of human factors in risk management, and we have suggested some interesting follow-on reading at the end of the chapter. However, this can be summarized by the concept of the 'triple strand' (Hillson and Murray-Webster, 2007; Murray-Webster and Hillson, 2008).

The triple strand, illustrated in Figure 4.3.2, shows how three categories of influence work together to bias the judgement of people when faced with uncertainties that matter to them. We are influenced firstly by our conscious, 'rational' assessments of things like our relevant experience, the manageability of the situations and the closeness in time of the effect should it occur. Secondly, humans are influenced subconsciously by a whole range of systematic cognitive biases and mental short cuts. Many of these are summed up by sayings embedded in our language, such as 'A bird in the hand is worth two in the bush' (loss aversion), 'First impressions last' (the representativeness heuristic) or 'Safety in numbers' (groupthink). Lastly, and often disconcertingly for many in business, we are influenced by our feelings and emotions about the situation, programmed automatically to seek pleasure and avoid pain in situations.

Working together these three strands of influence cement our risk attitude in a particular situation and also our resulting opinions and judgements about the best way forward in that risky situation. This happens to all individuals and to all groups, all of the time.

So, in our businesses, we want to identify and manage those things that might happen that, if they did, might destroy or significantly enhance business value. We want to make good individual and collective decisions in uncertain situations. We can help ourselves significantly by adopting scalable methods that bring a common language and structure, whilst allowing enough flexibility to deal with situations with an appropriate level of rigour. But we also need to be aware of those hidden factors that may be biasing our judgement and bring those to the surface for discussion and wider consideration.

Figure 4.3.2 The triple strand of influences on perception and risk attitude
Source: Murray-Webster and Hillson (2008)

Understanding all the uncertainty, but managing the unusual risks

All businesses need to forecast and to make estimates and predictions in the face of uncertainty; that we have to make these estimates and forecasts with significant unmanaged risk 'on the table' is a fact. But we shouldn't confuse our need to have as good an appreciation as possible of the underlying uncertainty and potential variability in a situation with the need to identify and manage specific risk events. It would be wasteful to spend our scarce time and funds on trying to make our projects and business ventures certain; some risks it is right to acknowledge and leave to chance, particularly those risks that could be classed as 'normal' for your business. Risk management delivers most business value when your processes for identifying uncertainties that matter can pick up the unusual things that could 'blind-side' you, and not just the typical sources of variation in your business cycle.

Driven to precision

However, given that we need to make estimates and forecasts, a further complicating factor is our apparent need as human beings for certainty and, therefore, our need to talk about estimates and forecasts precisely rather than acknowledging the inherent risks and therefore to talk in ranges.

As technology becomes more accessible on the desktop or laptop, more and more organizations are using probabilistic modelling to help their decision making in uncertain situations. This was once the domain of the specialist risk manager, but the general manager can now easily model the effect of risks on criteria such as delivery times or net present value of an investment.

Whilst it has become commonplace, and often a requirement in business, to forecast (and bid for work) in precise terms, our desire or habit of being 'driven to precision' blinds us from seeing the more uncertain reality. We must learn as a society that it is delusional to be precise when making business-related promises. What we should learn to do is use either words or ranges to express uncertainty, eg 'We expect profits to increase in the order of 5 per cent' or 'Turnover is predicted to increase by between 4 per cent and 6 per cent.' Once we start to accept that our estimates and forecasts are our best guesses, made in a context of significant uncertainty, then perhaps risk management will start to take the position of supporting those decision-making processes, rather than just one of trying to stop the horse bolting from the stable.

Our experience working with business is that talking in less precise terms or using ranges can have a dramatic impact on the way in which you lead your business and work with your staff, clients and suppliers. Expectations can be managed in all directions. Where uncertainty exists in any objective, this can be understood and plans established that reflect this. If there is only a 10 per cent chance that the office will be completed by the end of the year, then perhaps it might be a good

idea not to recruit 100 new staff to start on 1 January. Alternatively, if there is a 90 per cent chance that sales will increase by 40 per cent next year then projects to increase production capacity should be put in place now.

Risk management needs to be exciting, not boring

Even if we recognize that methods and standards alone are inadequate and that human factors are undoubtedly important, there still appears to be one more problem. Unfortunately for many people, risk management is just boring and, as such, when it is done it is often under duress, because we 'have to', or with a 'tick box' mentality. Both of these attitudes to risk management reduce its effectiveness and in many cases make it useless. So how can we make risk management exciting, not boring?

Clearly a consistent, repeatable approach needs to be applied, but at the same time this needs to be varied. Different methods should be applied to identify risks other than individuals just thinking of them themselves or attending a workshop or brainstorming session. Creative techniques such as Six Thinking Hats, developed by Edward de Bono, or the Delphi Technique, developed by the US military, can be used to trigger different thoughts. The objectives of any risk assessment need to be understood and in many cases focused; being specific about objectives – the things that matter most – can certainly help keep people's attention.

In addition, what motivates people in your business to be good, anticipatory, proactive risk managers rather than reactive 'firefighters'? There is lots of evidence, particularly in Anglo-Saxon cultures, that we enjoy and reward crisis management more than risk management. If this is your preference, or the behaviour that your business rewards, then risk management will struggle to break free from an administrative, tick-box process.

Walk the talk

So, as with all aspects of your business, there is a significant leadership element to effective risk management. Leaders must show by example 'the way they want risks to be managed around here' and what culture for making decisions in risky situations they want to support.

Our suggestions for how you make that happen are listed below:

- Use a consistent risk management method that is fit for purpose across the whole business, and make sure everyone is aware of it and can apply it.
- Talk to stakeholders – peers, colleagues, advisers and consultants – about their perception of the risks that could affect the business, the things they are assuming will happen, the things that may have a negative effect on objectives and the things that could make the business run even better. Keep that dialogue open,

two-way and constructive. Be prepared to examine your own motivations and risk attitudes and to challenge those of others.

- Document all the risks raised in a risk register or database. If everyone does this there will be fewer completely unexpected occurrences. You don't need to manage them all actively, but the act of identification opens up the mind to possibilities.
- Expect there to be many threats, so support the identification of them; that isn't negative – it's sensible.
- Encourage the identification of opportunities as a way of pushing continuous improvement in the business.
- Talk in ranges, acknowledging that you can predict few business situations with anything like certainty. If presented with a single figure, always ask the question 'What is the chance of achieving it?' and further ask what is the minimum and maximum it might be. Acknowledging inherent uncertainty in your language and behaviour is actually empowering for others, not demotivating.
- Make risk management a daily exercise. Use the language of risk management in your everyday communications.
- Hold your team accountable for being able to talk to you about the top five threats and top five opportunities for their business unit or project. What circumstances might help the business run more effectively? What circumstances are the show-stoppers in terms of threats to stated business objectives?
- Ensure that resources for planned responses to priority risks are secured and built into work plans, or the planned actions won't happen. Promote close attention to risks that you have chosen not to manage actively; their status may change and you need to be ready with a 'plan B'.
- Find ways of rewarding anticipatory behaviour by highlighting when good risk management has taken place: where threats have been identified and responded to in such a way that the business's risk exposure has been reduced or where opportunities have been exploited and as a result have increased the chances of successful outcomes. Do not reward the firefighters who only put out the fires they could have prevented in the first instance.

Act of faith, or proven concept?

In the final analysis, unless you have good evidence to the contrary, risk management can seem more like an act of faith than a proven concept for business. The logic of the self-evident theory is compelling, yet there are habits embedded in our individual and collective behaviour that seem to work against that compelling logic.

There is a strong parallel between risk management and quality management. Both cost money to implement and both can decline into expensive administration, with the business taking its eye off the goal, but both, done well, can make a significant contribution to creating customer satisfaction and competitive advantage.

Risk management is perhaps caught in a trap in our collective mindsets. There is no doubt that risk management matters significantly for all types of business, but if

the effectiveness of risk management is not measured as part of the normal performance of management arrangements of the organization then it will be perceived as either a 'black art' – an inherently risky, albeit necessary, process in itself – or as peripheral. Process measures are easy to find (eg whether there is a risk manager, whether governance addresses risk management, etc), but adding on process can destroy ultimate value. Performance measures are much more important (eg prevention of opportunity loss through proactive rather than reactive management).

Recent developments in the area of enterprise risk management (ERM), discussed in others parts of this book, are undoubtedly a step in the right direction. We argue, though, that this is not enough and that paying attention to the human leadership and cultural aspects of risk management and to performance management may be the route to ensuring your investment in process, tools and training pays off.

References and further reading

Ariely, D (2008) *Predictably Irrational: The hidden forces that shape our decisions*, HarperCollins, New York

Hillson, D A and Murray-Webster, R (2007) *Understanding and Managing Risk Attitude*, 2nd edn, Gower Publications, Aldershot

Murray-Webster, R and Hillson, D A (2008) *Managing Group Risk Attitude*, Gower Publications, Aldershot

Office of Government Commerce (2007) *Management of Risk: Guidance for practitioners*, Stationery Office, London

Taleb, N N (2007) *The Black Swan: The impact of the highly improbable*, Penguin, London

4.4

The role of document management in managing risk

Julian Buck, Version One Limited

Introduction

Managing risk has become a necessity and not an option. However, all too often organizations invest time and resources into managing the most obvious areas of risk, such as those associated with insurance, whilst ignoring some of the most basic risks, including document security and handling.

When it comes to safeguarding critical documents, some organizations' document management and security processes are alarmingly lax and, in the event of a fire, flood or security breach, key documents could easily be lost, destroyed or tampered with. This is why electronic document management (EDM), which enables the electronic storage and management of documents, is such an invaluable technology in the fight against document loss, damage and fraud, and it is vital that implementing this technology becomes standard risk management practice.

Probably the Easiest Investment Decision...

You Will Ever Make!

Cut Costs

Improve Efficiency

Reduce Late Payments

ROI in Six Months

Improve Cash Flow

Free Up Storage Space

Version One's document management and imaging enables the electronic storage, retrieval, management, delivery and authorisation of business documents such as invoices, purchase orders and statements.

Seamlessly integrated into all major business systems, this 'paperless office' technology is enabling hundreds of organisations to cut costs and improve productivity.

To find out how your organisation can benefit from using Version One's document management solutions, contact:

marketing@versionone.co.uk or call

+44 (0) 1625 856505

www.versionone.co.uk

Document Management & Imaging

VersionOne

Inadequate business continuity plans

Version One recently carried out research with senior staff from 75 UK organizations (primarily managing directors, financial directors and IT directors) to find out how comprehensive their business continuity plans are. Of those questioned 80 per cent claimed to have a full or reasonable business continuity plan in place. However, when they were questioned further, it emerged that ensuring documents are securely stored is an area that only a small number of organizations had considered; only 17 per cent of companies with a plan had worked this into their business continuity strategy.

So what are the risks of not securely managing and storing business documents? As a society, we still rely heavily on paper documents, which is unusual considering how prolific e-mailing, texting and social networking now are. Contracts, invoices, purchase orders, credit agreements and personnel records are just some of the documents that are frequently circulated and stored in paper form. As well as being inefficient and costly, paper-based processes are also vulnerable to disaster, error and fraud.

Imagine if an organization that stores all its contracts, financial documents and personnel records in on-site filing cabinets has a destructive fire and all of these documents are destroyed. What would the implications be? For a start, without copies of staff, supplier, customer and partner contracts, the organization would be unable to dispute terms and conditions. Without purchase invoices, until the supplier sends further correspondence, the organization could lose track of monies payable and may be charged late-payment penalties. Lost copy sales invoices and other credit control information could result in the company losing sight of monies receivable, making it very difficult to chase debt. Importantly, the destruction of financial documents would also result in the destruction of an audit trail for tax purposes. In addition, with the loss of personnel documents such as staff absence records and disciplinary documents, the organization might not be able to provide proof of underperforming and/or disruptive members of staff during dismissal hearings and/or defend itself against staff grievances.

The role of EDM in continuity planning

Some organizations believe that their documents are securely stored because they are archived in a third-party storage facility; however, what if there is a fire or an explosion at the third-party provider's premises? The only real solution to the safe storage of documents is EDM.

EDM, which can be tightly integrated into organizations' accounting and enterprise resource planning (ERP) systems, enables the electronic storage of all business documents. Paper documents arriving into the organization, such as purchase invoices and statements, are scanned in and bar-coded and the original paper documents can then be shredded. The imaged documents are then automatically stored in the archive and linked to the appropriate records in the accounting system.

Outbound electronic documents, such as sales invoices, purchase orders and credit agreements, can also be automatically stored in the archive.

Once in the electronic archive, all documents are securely stored and can be retrieved by authorized personnel only by drilling down through the accounting/ERP system or via a secure web browser. In the event of a fire or flood, the electronic documents remain safe and undamaged in the electronic archive and, as long as the organization follows standard IT backup procedures, all electronic documents will be able to be quickly and easily retrieved as soon as the IT system is back up and running.

Despite a common misconception that document management is all about electronic filing, there is a lot more to EDM than just this. Modern EDM systems also assist with the electronic creation, presentation and delivery of documents. As documents can arrive electronically, such as customer orders as PDF files, delivery schedules in Excel and bank statements downloaded from a website, EDM is not just about scanning paper but also encompasses the storage of incoming electronic files. EDM systems also enable the electronic delivery of documents and support the use of electronic 'workflow' so that documents can be circulated, processed and authorized electronically, providing a comprehensive audit trail in the process.

Document management as a fraud prevention tool

As well as ensuring the safe retrieval of documents in the event of a fire, bomb or flood, document management also helps to achieve a high level of regulatory compliance, helping to prevent fraudulent activity. Whether it is the news about Sir Allen Stanford orchestrating a fraudulent, multibillion-dollar investment scheme or Bernard Madoff, the former chairman of the Nasdaq stock market, being arrested for running a hedge fund that allegedly racked up a phenomenal $50 billion (£33.5 billion) of fraudulent losses, stories of fraud are never too far from the headlines, reminding us of the catastrophic impact it can have on business.

Without doubt, EDM would have played a significant role in preventing the fraudulent activities surrounding the most prolific false accounting scandals in history – Enron and WorldCom. Few can forget the false accounting scandal at Enron in which Arthur Andersen LLP was found guilty in the United States of obstructing justice. The prosecution alleged it had destroyed relevant documents after it had become aware of an investigation by the Securities and Exchange Commission (SEC) into the affairs of its client Enron. Similarly, executives at telecommunications giant WorldCom perpetrated an accounting fraud that led to the largest bankruptcy in history. Evidence shows that the accounting fraud was discovered as early as June 2001, when several former employees gave statements alleging instances of hiding bad debt, understating costs and backdating contracts. The Enron and WorldCom scandals, which proved devastating to both companies' reputations, were directly responsible for their downfalls.

The lessons learnt from these scandals include the importance of managing risk by having effective document retention policies and document management systems in place. Had Arthur Andersen and WorldCom had document management systems in place, the members of staff embroiled in the fraud would have been unable to destroy and alter incriminating documents.

So, this raises the question of whether members of your finance team could easily shred invoices, credit agreements and correspondence in an attempt to cover their poor handling of a situation. Would they be able to cover their tracks and get away with it? And could members of staff fraudulently doctor documents to suit their own agenda, creating a false audit trail?

It is always going to be a challenge to prevent unscrupulous employees from committing a fraudulent act if they have their mind set on it. However, organizations can implement measures and systems to help protect themselves from acts of fraud, and EDM is one such system that is vital to the prevention of accounting fraud.

EDM systems, tightly integrated into organizations' accounting and ERP systems, minimize the risk of fraud, as documents such as invoices, purchase orders and remittances are imaged and then securely stored in an electronic archive. These documents are a permanent record, which cannot be destroyed, shredded, 'lost' or altered in any way by the users, reducing the risk of employees eliminating or manipulating evidence to cover their tracks.

Document management systems also allow strict levels of document access and make it possible to maintain audit trails so that it is clear who approved what and when, further counteracting attempts to hide suspicious activity. In fact, every document in the archive has its own distinct 'electronic fingerprint', with any activity relating to that document being logged. It is impossible to delete any of the activity logs, and so the attempts of even the most ardent hackers to cover their trail would be detected.

Corporate fraud is on the increase

The findings of a survey by Version One in 2008 highlighted that, despite the controls that exist in the UK, three-quarters of senior finance professionals believe that a case of fraudulent activity on the scale of Enron could happen in the UK. Version One carried out the research with 190 senior finance professionals (finance directors and managers) across a range of public and private sector organizations.

The survey revealed that 73 per cent of senior finance professionals believe an Enron-scale scandal could occur in the UK owing to 'poor controls, collaboration between unscrupulous employees and the ease in which paper documents can be modified'. The same 73 per cent stated that someone in their organization would be able to tamper with or 'lose' a document to suit his or her ends, whilst 38 per cent of the 190 respondents admitted that they had come across activity that could be considered fraudulent involving business documents. Worryingly, a quarter of these stated that they had witnessed document fraud 'a number of times'.

And cases of corporate fraud are on the increase! KPMG Forensic's annual Fraud Barometer revealed that UK courts heard more than £1.1 billion worth of fraud cases in 2008, the survey's highest recorded level since 1995. According to KPMG, company managers, employees and customers were tried for fraud relating to £300 million in 2008 – three times the value seen in 2007. Worryingly, these figures are still on the increase, with UK corporations losing an incredible £960 million to publicly reported fraud in the half-year to 30 June 2009, the highest six-month total since at least 2003, when BDO Stoy Hayward began tracking corporate fraud. As the credit crunch continues to tighten, more and more employees are likely to undertake desperate measures to solve their own financial problems, and so companies need to ensure they have effective systems such as EDM in place to protect themselves.

Document management as an enabler to corporate governance

As well as protecting against fraud, EDM systems are also invaluable tools for ensuring HM Revenue & Customs (HMRC) compliance. HMRC requires the retention of numerous documents, with six years' worth of documents plus the current year being required for VAT purposes. Retaining these documents electronically ensures they can be quickly and easily retrieved, and electronic retention is perfectly acceptable as long as the business advises the VAT office of its intention to store scanned images of paper records. HMRC also accepts electronic documents as laid down in the British Standard BSI DISC PD0008 (relating to 'Legal admissibility and evidential weight of information stored electronically').

Failure to produce accurate tax records to back up a tax return or claim could result in a significant penalty and, as of April 2009, with the introduction of HMRC's new legislation, these penalties got even tougher, making EDM systems all the more important. With the new legislation, failure to produce accurate records is deemed a 'failure to take reasonable care', with the maximum penalties being 30 per cent of the potential lost tax if the inaccuracy was careless, 70 per cent if it was deliberate and 100 per cent if it was deliberate and the taxpayer attempted to conceal it. In addition, the new HMRC legislation has extended taxpayers' record-keeping obligations, meaning that there is a need for organizations to retain more documents than ever before. These documents include those relating to income tax, capital gains tax, VAT, PAYE and NI contributions, the construction industry scheme, corporation tax and the administration of student loans.

Conclusion

Documents are the backbone of any business, from contracts and invoices through to staff sickness records and quality assurance documents. If all or some of these documents were to be destroyed, lost or tampered with, the implications could be

catastrophic. With this in mind, it is extraordinary that so many businesses continue to produce, handle and store paper documents.

EDM is key to preventing destroyed documents, safeguarding against fraud and avoiding HMRC penalties, and so why are so many organizations still failing to view this technology as a risk management tool? It is vital that EDM becomes part of every organization's risk management toolset before any more paper-reliant companies are faced with the charred remains of their business-critical documents or the damaging aftermath of staff fraud.

nortech

Working with you to take advantage of all the benefits that access control can offer . . .

Managing the movement of your staff and your visitors (both invited and uninvited) will enable you to:

- Improve efficiency
- Protect your assets
- Protect your information
- Reduce the risk of accidents

Delivering solutions that suit your business

sales@nortechcontrol.com

www.nortechcontrol.com

4.5

The role of access control in risk management

Keith Hardy, Nortech Control Systems

Introduction

The term 'access control' is generally used to refer to a system that checks the identity of personnel in order to ensure that they have the correct authority to access either a restricted area or computer-based information. The benefits of using such a system to help reduce the risk of personal injury and the loss and/or damage to capital assets may seem quite obvious. In particular, the need to control access to computer-based information is self-evident. However, there are many ways that access control techniques can be applied to the physical movement of people and/or vehicles around a building or site to help to reduce risk.

In this chapter, we will discuss the various technologies used by access control systems and suggest ways in which they can be deployed as part of risk management.

Access control overview

As stated above, an access control system checks the identity of each person and determines whether or not that person has the authority to access a restricted area.

It must also have a means of preventing people who don't have the appropriate authority from entering the restricted area.

Credentials

The identity of a person is usually determined by a 'credential', which may be a physical object such as an access badge, a piece of knowledge such as a PIN code, or a facet of a person's physical being such as a fingerprint. In some cases, combinations of two or more of these credentials may be used to identify the person.

The most common type of credential is an access card. There are many card technologies, including magnetic stripe, bar code and radio frequency identification (RFID) cards such as 125-kHz proximity cards and contactless smart cards. RFID credentials are also available as key fobs, which are more compact than cards. Biometric technologies now available include fingerprint, facial recognition, iris recognition, retinal scan and hand geometry.

The details of the credentials for an access control system are usually held within a database. This will typically contain the credentials and access rights for all staff members of a given company or organization. The assignment of credentials must be strictly controlled and must comply with company regulations relating to each person's responsibilities and qualifications, ie a person should have access only to those areas and/or equipment for which he or she has the appropriate authority and, where applicable, the correct skills.

Access control points

For controlling access to a restricted area, one or more access control points are required. This can be a door, turnstile, parking gate, lift, or any physical barrier where granting access can be electrically controlled. Typically, the access point will be a door with an electric locking device and a reader. The reader may be a keypad, a card reader or a biometric reader. The reader sends the credential details to an access control panel, which verifies the information against a database. If the credential is valid, access is granted by unlocking the door for a short period. A magnetic door sensor may be used to monitor the door position so that it can raise an alarm if the door is opened illegally. When the access control panel has unlocked the door and the door is opened, the sensor detects this and the door alarm is temporarily ignored. If, however, the door is not closed within a given period, the door alarm will sound.

A door is the simplest form of access control point, but it has no means of ensuring that only one person passes through when it is open. Strict rules must therefore be in place forbidding authorized personnel from compromising the system by allowing unauthorized people to pass through the door. Where this is not practical, then a one-pass system such as a full-height turnstile should be fitted. There are several alternatives to physical turnstiles available, such as 'optical' turnstiles. These devices can count the number of people passing through

an access control point using optical sensors, thermal imaging or video analysis techniques, and can raise an alarm if the incorrect number of people passes through the access control point.

Networked access control

In larger access control systems, the access control panels are networked to a master PC that is used to manage the credential database for all access points in the building. Furthermore, the system can track personnel attendance and movements within a facility. This is very helpful in deterring would-be thieves or saboteurs, especially if it is linked to CCTV.

The wider options

There are many ways in which access control techniques can be applied to help reduce risk in a company or organization. The following are some applications and implementation methods:

- *Preventing unauthorized personnel from accessing restricted areas.* This is the most common access control application, but its use isn't limited to keeping out potentially hostile personnel. It can also be used to prevent personnel from inadvertently entering controlled areas such as 'clean' or hazardous areas without taking the appropriate precautions or receiving suitable training. The issuing of credentials must be linked to staff status and training. One measure for accessing hazardous areas could be the fitting of access control tags to protective clothing or headgear.
- *Keeping account of the movements of authorized personnel.* Knowing where members of staff are at any given time can help ensure that, in the event of an incident, those involved can be quickly identified. This can also deter would-be thieves. Some access control systems can provide individual cardholder-tracking data to track down key staff members, such as first aid staff, whenever they are needed urgently.
- *Evacuation mustering systems.* An access control system that keeps account of staff locations within a building can be used as an evacuation mustering system. At the point of an emergency evacuation, all members of staff and visitors present within the building are on record, a print-off of which can be used for roll call at assembly points. Also, readers can be installed at the assembly point(s) so that evacuated personnel can register their presence, thereby highlighting missing staff members.
- *Ensuring that sufficient special duty or safety staff are present in a controlled area.* Some access control systems can monitor the numbers of specific categories of staff present within a controlled area. This provides the ability to ensure that the required number of key staff members, such as safety officers, are maintained within the area by raising an alarm whenever this number falls below the required minimum level.

- *Ensuring that maximum numbers of personnel or vehicles within a controlled area are not exceeded.* The same type of monitoring can be applied to preventing the number of personnel within a controlled area from exceeding a prescribed safety limit. Here, the system can refuse entry to further personnel whenever the limit has been reached. This type of control can also apply to vehicles crossing bridges, entering tunnels or simply operating in high-risk environments. The concept may also be applied to the prevention of pedestrians from entering an area when certain types of vehicles or machinery are present.
- *Restricting machine operation to trained operators.* Where there are different types of machines within a workshop, simply controlling access to the workshop may not be sufficient to reduce the risk of accidents. Access control may also be applied to the machines themselves. An access control device can be fitted as a power isolation switch to the machine. Trained operators are issued with pass cards that allow them to power up the machine by placing the access card in a special holder or reader. The machine is powered down when the card is removed. This system is more effective if pass cards are also used for access to other parts of the building such as canteens and rest areas. This will help to ensure that machine operators remove their cards when they leave their machines unattended.
- *Controlling airlock access.* Wherever a controlled environment requires an airlock access point (ie a two-door sealed vestibule that prevents free airflow between the controlled area and the external environment), an access control system with magnetic locking devices can be used as a cost-effective method of ensuring that only one door is opened at any time. Each door is unlocked using a pass card, but neither of the doors can be unlocked whenever the other door is open. This type of system can also be used for other airlock-type applications, such as anti-terrorist control, by including a metal-detecting device within the airlock.
- *Tracking the movement of vehicles.* Vehicle access control provides an excellent means of managing an inventory of vehicles and trailers. With all tractors and trailers fitted with long-range radio frequency ID tags, their movements can be monitored at key points as they move on and off site as well as within it. Systems can monitor which tractor unit is pulling which trailer. Driver identities can also be monitored by issuing personnel ID tags to each driver. It may be a purely passive monitoring system or it may be used to restrict movement through access points to valid combinations of driver, tractor and trailer.

Case studies

Nortech Control Systems has many examples where its Access Control systems have made a major contribution to risk management. Here are two of them.

Petrochemical Research Facility

Due to the nature of its work, a major petrochemical research facility required a secure Access Control system to keep an accurate record of the personnel and visitors on site and provide a mustering system. The facility also has its own fire crew

to provide a first response to any potential incident. The Access Control system was required to provide an instantaneous indication of whether or not sufficient fire fighters are on site to carry out a first response so that, if an incident does occur, a decision can be quickly arrived at to follow the most appropriate emergency procedure.

It is essential that at least two trained first aiders be available on site at all times. To help meet this requirement, the system needs to continually monitor the number of first aiders on site so that, wherever necessary, off-duty first aiders can be called in to relieve those about to leave the site.

Nortech Control Systems supplied a solution using an Access Control system especially adapted to provide all of these features.

Caravan Storage Facility

Despite having a comprehensive security system, a caravan storage facility with a capacity for over 2,000 caravans suffered several incidents where caravans had been removed from the facility without permission. The proprietors needed a system that would minimize the risk of the theft of caravans without causing delays or inconvenience to its customers.

All caravan owners were issued with long-range RFID tags to fit to both their caravans and their towing vehicles, and Nortech Control Systems developed a system that reads the tags on all vehicles entering and leaving the facility and verifies the access rights of each vehicle. Using a combination of sensors, the system is able to determine whether or not the vehicle is towing a caravan and, if so, it checks that the vehicle has the authority to tow that particular caravan. The system can automatically allow any valid combination of vehicle and caravan on and off the facility by operating entry and exit barriers, and raise an alarm whenever an unauthorized vehicle and caravan combination attempts to leave the facility.

The system also logs caravans on and off the site and maintains an inventory of all caravans on the site.

Conclusion

Modern technology combined with ingenuity enables access control techniques to support many aspects of risk management. Many companies in the UK have benefited from access control concepts that have helped to reduce delays, loss of productivity, accidents and crime. Furthermore, some access control systems can provide management with a wealth of knowledge to help them to identify the causes of inventory loss, accidents and even inefficiencies.

4.6

Managing supply chain risk

Emma Brooks, Chartered Institute of Purchasing & Supply (CIPS)

Being aware of risk means you can plan for the mitigation of its effects, and also take advantage of any opportunities it offers for the future.

The current environment

Modern organizations operate in a very commercially pressured and global environment. Because competition is so strong, to remain efficient and competitive firms must be prepared to take risks. Although risk can be perceived as having a negative impact on organizations, it often comes with opportunities and the chance for innovation, and should not always be seen as a threat.

Modern supply chains are complex networks that link organizations, industries and economies. The current economic climate has provided us with a hard-hitting example of how risk can affect your business, your customers and the suppliers in your network if you're unprepared.

The last few years have shown us, with startling results, that change is rapid and unpredictable and spreads on a global scale. The recent credit crisis has seen record

levels of bankruptcies and individual voluntary arrangements, and manufacturers turning to reduced working weeks or, in the case of Honda, ceasing production for several months altogether. This leaves an already vulnerable business environment teetering on the edge of survival. Change has become so rapid and unprecedented; it is those flexible and creative firms with strong liquidity and robust risk management strategies that remain on top.

Cash is king, we hear. Never has that been more important as credit dries up, consumers buy less and suppliers reduce their credit terms – the ones that are still in business, that is. A recent report from Citigroup's investment bank shows that, since the credit crisis began, the returns of firms with ample liquidity have outperformed those of their cash-strapped industry peers by almost 7 per cent. Before the crunch, cash-rich firms were generally underperforming. Building a sustainable business model for your organization and its supply chain should help you to remain in business and create opportunities to come out on top.

The effect of modern working practices

Organizations have become very lean and mostly operate on a just-in-time basis. Therefore the slightest disruption to any element of their supply chain can have devastating results. Supply chain initiatives such as outsourcing, low-cost-country sourcing and lean supply have exposed us to new risks but have also given us the experience to mitigate and avoid their impacts. Trends such as reducing the supply base and using sole sourcing have forged closer working relationships in order to collectively monitor and manage risks in the supply chain.

British Airways (BA) more than anyone discovered the consequences of risk when it experienced a relationship breakdown with Gate Gourmet. The result? Its planes were grounded for several days in 2005. BA probably didn't view its catering supplier as particularly high-risk at the time. So, wherever possible, any purchasing organization should understand who its key suppliers are and adopt a partnering approach to those important or vulnerable supplier relationships to avoid disasters like this.

Industries have also become more consolidated, so, if one major player is affected, the knock-on effects can be catastrophic. It makes switching to alternative suppliers that have similar capacity almost impossible, especially when non-standard products are used. Generally, there is no slack in these manufacturers' capacity either, so finding a supplier to switch to may be impossible. One example of this is the packaging industry, where there are only a few large consolidated businesses. Organizations must become agile and risk aware, so that they have the ability to switch to contingency plans at short notice.

Customer of choice

Finding the right supplier during tough times is key to an organization's success and survival. This is a time for buyers to ensure that they have the right people with

the right relationships on board. Both buyers and suppliers need to show that they understand their own and each other's needs and demonstrate that they are a customer and supplier of choice.

To identify, manage and mitigate risk, buyers and suppliers need first to reassess their relationships and where their priority focus should be:

- *A time for synchronicity.* Understanding each other's needs on how to survive now and grow in the future is critical for joint success. Ever-closer synchronization is the key – tightening and understanding the links between suppliers, your organization's operations and your customers.
- *Build information bridges.* Information is power. Establishing a valuable flow of information amongst your stakeholders, suppliers and customers will build a common bond of trust.
- *Seek sustainable relationships.* Build enduring relationships with your closest suppliers, because you are all in this together. Re-examining existing relationships and deciding whether they are the most effective and efficient for you under these new testing conditions is a difficult process. You will not be able to establish a partnership with every supplier, but it is important to determine which ones will be sustainable. Focus on those suppliers that you can't afford to lose and find a way to ensure that they survive alongside you.
- *Make strategic changes.* Carve out some time from the daily grind to focus closely on the supply chain and think about the future. Can you deal effectively with the recession's volatilities? Are you prepared for when the upturn comes? You don't have to go it alone, though. All these considerations are an exercise for the whole organization and its partners, so encourage that joint collaboration too.
- *Advance everyone's understanding of the value chain.* The more people think about their roles and the part they can play in dealing with the economic downturn and its effects on the organization, the better they will do their jobs and benefit the organization they work for. Rethink the way you appraise employees and evaluate their contribution to the 'value chain'. Promote greater coordination at all levels between purchasing people and other parts of the organization; this should help to stimulate innovation through a greater understanding of the issues facing all.

Struggling suppliers

Risk needs to be managed throughout the whole supply chain, and suppliers can be both the cause and the solution to most problems. Their performance is critical to your success.

Businesses rarely fail without some initial outward signs that they are in difficulty. Most will naturally attempt to reduce any outward signs of difficulty in order to maintain an air of normality. They don't want to set off alarm bells with customers, suppliers and staff, who may decide to abandon ship if they believe the busi-

ness is in trouble. This obviously makes the task of saving the business even more tricky if there's a cloak of secrecy to maintain.

Exactly how can we pick up on signals that a supplier is in difficulty? Information for analysis, such as reports and accounts, are publicly available to view, but these, by their very nature, lack recent data. Having said that, this type of information may still give a longer-term warning that a supplier needs a closer watch, and there is also much that the purchasing professional can pick up from day-to-day dealings with a supplier. One of the most effective ways of assessing a supplier's position is through regular visits to its premises. These visits should increase in frequency if there is some suspicion that the supplier may be experiencing hard times.

Warning signs that suppliers are in difficulty

- A reduction in the number of staff may indicate a downturn in the activity of the business. There may be a valid business reason, but ask those pertinent questions and root out the reasons for the reduction.
- A change to working patterns. For example, if a manufacturing company that has operated a three-shift system changes to a two-shift system, it may indicate that there are problems, especially if the change cannot be accounted for by normal seasonal working patterns.
- If the supplier is working for only a small number of customers.
- A sale of assets such as premises or equipment may point to a contraction in the business.
- A lack of investment in the business. The supplier may be increasingly reliant upon old technology and working practices in comparison to its competitors.

The right tools for the job

Supply chain professionals have a wealth of tools and skills that can be used equally for risk management, from close working relationships between buying and supplying organizations, to monitoring and performance measurement techniques. As one example, purchasing and supply chain professionals are experienced in calculating and making savings, so this is one way of demonstrating the value they can add to an enterprise-wide risk management programme. Pricing a risk or disaster in terms of the cost of the loss is a useful tool; it's then possible to calculate a 'saving' to avoid that loss. This is indeed a powerful tool to get the deserved attention of the board and shareholders. Successfully managed risk taking is also likely to attract attention. Showcasing examples of increased profit, innovation or sales

through the successful mitigation of risks will also raise the profile of the supply chain team.

Through carefully monitoring supplier contracts, relationships and performance, comprehensive risk assessments can be profiled and problems foreseen and avoided, or opportunities successfully managed to fruition. Partnering and outsourcing can also lead to improved relationships and more prudent performance measurement tools.

What can we do?

The increased use of IT, the globalization of supply chains and the integration of networks of companies into 'extended enterprises' have helped reduce companies' exposure to a catastrophic 'single point of failure' disaster. An extended geographic footprint and an increase in information flows within and between businesses mean that companies can diversify and manage risk more effectively than ever.

A static business continuity plan will not protect a company from disruption. An integrated and ongoing enterprise-wide plan, with assumptions that are regularly tested and that keeps pace with the risks prevalent in the business environment, is crucial. We can learn the lessons of the past to inform, improve and update our plans in years to come.

Practical steps to reducing supply chain vulnerability

Expecting the unexpected

The Met Office recorded rainfall in the UK during May to July 2006 at 387.6 millimetres – the wettest since records began in 1766. Many homes and businesses had to be evacuated by boat as they were flooded and became inaccessible. The knock-on effects on homes and businesses were phenomenal. Some businesses closed or became bankrupt, while others rode the crest of that summer's wave and its opportunities.

The most obvious directly affected businesses were farming and those businesses with flooded premises. Cadbury Schweppes had to close its Sheffield factory because of the flooding, issuing a statement explaining that 'employees on site are currently leading an extensive clean-up operation. We have now evaluated the extent of the damage to the building and manufacturing equipment, and believe that it will be a number of weeks before the factory is fully operational.' Access to the factory was limited for a number of days, the clean-up operation was slow, and the damage prevented the movement of goods in and out of the area.

A major shopping centre also reported up to five feet of flooding to the ground level of over 50 stores, including a large food court, which was closed for several months. That's the effect on big business. Similarly, in the farming industry crops were ruined, and others had to be harvested before their due time. Drying-out processes were put in place for those crops that could be salvaged. For the smaller independent retailer the pressures were greater, and such a disaster became a 'make or break' opportunity.

On a more positive note Hunter, a wellington boot manufacturer, operated at full capacity. Glastonbury rock festival that year was a complete washout as the festival turned into a swamp. The mud did not deter the 150,000-plus partygoers, and stallholders sold out of wellies, raincoats and dry clothes; sun hats and sunglasses on the whole remained unsold. Domino's Pizza also benefited from the spell of wet weather. The biggest competitor for this industry was the summer barbecue, and without sunshine people preferred to eat indoors instead.

Events such as the flooding in the UK, the South-East Asian tsunami, foot and mouth disease, bird and swine flu, and the credit crisis are all risks to be mitigated and opportunities to be discovered. By understanding how far reaching the direct and indirect consequences of these events are, businesses can bring and apply those ideas to new and existing risk management schemes.

- Learn from previous experiences of supply chain vulnerability ('How well is our process working?'). Use all non-conformance events as a way of checking if the supply chain network is working as expected and build in resilience.
- The best source of information and to pick up practical steps is to check previous experiences inside the organization. The buyer should be constantly checking on how well the current processes for supply chain management are working. Whenever there is a non-conformance event, analyse and learn from any mistakes.
- Develop a detailed knowledge and understanding of markets and your suppliers. Relationships will be easier with more proactive management and increased awareness of emerging supply chain vulnerability issues.
- Learn from the experience of others, using benchmarking, research and case studies.
- Prioritize effort using risk evaluation techniques.
- Assess the possible impact of supply chain vulnerability against the probability of it happening. This will help to determine the impact on the customer and set priorities for your own time and attention. It is not necessarily the biggest-value supplier that is the biggest risk, but the high-priority supplier.
- Cause and effect. Our actions have reactions and consequences. New plans and initiatives need to go through a thorough risk assessment process.

Stay ahead of the game

Survival during these tough times means that organizations have to stay agile and innovative. Staying ahead of the game means digging deep into your organization's processes (both internal and external), and sharing information with both customers and suppliers. Identifying suppliers at risk and taking action are essential, but be mindful that your customers will be doing the same to you. Openness, transparency and sharing information will build trust and forge stronger relationships. Make sure your customers know your level of commitment in tackling risk management, and your suppliers should also know how important their part is in the risk management strategy.

Risk management in the supply chain is more about resilience than about avoiding risk. Risk is on the increase and is part and parcel of our business lives. Managing and minimizing its effects are the only way forward. A lack of time and resources is the common excuse why assessing risk is not so important until it arrives on the doorstep. Purchasing and supply chain professionals need to raise awareness and the understanding of supply chain risk management tools so that senior managers give it the time and attention it demands.

4.7

Competence and confidence – accreditation and risk management in post-recession Britain

Jon Murthy, UKAS

We are constantly told that we live in the information age. Usually, this is taken to mean that we are lucky enough to have access to formerly unparalleled amounts of data at speeds that were a pipe dream two generations ago. However, the problem facing risk managers is not access to information, but the accuracy of that information. And this has never been more important than as UK plc tries to pull itself out of the worst recession for the last half-century.

'Risk' is a word that means very different things to different audiences. To the general public it is something to be avoided; one need only open a newspaper to

see an article bemoaning the fact that society is so 'risk averse' that parents are imprisoning their kids in front of the television. To a financier, 'risk' means something quite different and well defined, quantifiable in purely financial terms. But, to risk managers, it is the bread and butter of the job. Identifying, planning, analysing and mapping risk are becoming more sophisticated all the time.

Confidence is clearly vital, and confidence comes from having the right, accurate information: knowing that quality control is taken care of, that third-party suppliers and providers are competent and fit for purpose, that the business has the insurance cover that it needs, and that there is a strategy in place just in case it all goes wrong. One of the tools that businesses are increasingly turning to in order to ensure that confidence is accreditation.

UKAS – accreditation and UK plc

The United Kingdom Accreditation Service (UKAS) is the sole UK accreditation body recognized by government to assess organizations that provide certification, testing, inspection and calibration services. UKAS assesses organizations against internationally recognized standards, which means that UKAS accreditation is recognized across the world. It is recognition that an organization is competent and complies with best practice.

There are a number of reasons that an organization might choose to try to gain UKAS accreditation. It can open up new markets – both at home and abroad – and having a robust assessment of systems and processes can help to reduce duplication and downtime. But where does this feed into risk management?

Quality management – know thyself

Quality management is one of those areas that has suffered in the past from an image problem. Much like health and safety, an equally essential part of business that can suffer from slightly negative connotations, there used to be an air of 'box ticking' attached to quality assurance and quality management. It is easy to see why the general public might think that this is a world away from risk (a far more exciting word!). However, good risk management doesn't just depend on knowing where you want to go or how you want to get there; it is vital that you also know where you are.

For most businesses, de-risking the supply chain is a priority. When unknowns are present at the procurement stage, this makes any manager's job much harder, which is why confidence in suppliers is vital. When this is viewed at a micro-level, consumers are always more likely to source from names that they trust, which is precisely why brands spend so much money convincing the general public that they are trustworthy and dependable. If risk management intrudes into the process of buying a car or even a loaf of bread, how much more important is it likely to be in a business setting where thousands or millions of pounds are at stake? This is one of the reasons that specifiers for large projects are increasingly relying on

accreditation as a mechanism for ensuring that risk is minimized, by suppliers covered by accreditation. Being able to have confidence in the supply chain means that a risk manager's life starts to get a lot easier and that businesses can concentrate on their own quality management without having to worry about someone else's as well.

Quality management within a business is no less vital for proper risk management. The key to management is to know what it is that you are expected to manage, which is why assessment has become so important. However, in-house assessment is not the most effective mechanism to follow; the people who are closest to a project are rarely the ones who are in the best position to act as impartial observers. Even if they are able to do so, it is extremely unlikely that other people further down the line will accept first-party assessment as the most transparent method. This is why third-party assessment conducted by impartial observers has long been a cornerstone of effective quality assurance. Ultimately, having confidence in your assessment process will mean that a business knows where it is starting from; what can be measured can be managed.

Confidence in inspection

In terms of risk management, the other area where it is vital that an organization can have confidence in its suppliers is inspection. In some arenas, such as construction or engineering, testing and inspection can literally be the difference between life and death, so it is imperative that the inspectors and testers are trusted to be competent and impartial. For some areas, like asbestos, it is already mandatory under the law for organizations involved at crucial stages of the testing process to be accredited.

Where risk management relies on measurements taken by third parties, success will always be dependent on having confidence in those providers. In an unregulated market economy, the 'invisible hand' has been trusted in the past to act as a form of quality control – if you are unsatisfied with what you receive then you will seek out a different provider next time – but this is clearly inappropriate in a case where one mistake can cost lives. It is also undesirable when such a mistake can cost money. The links between inspection and risk management can be traced back to the industrial revolution, when mill owners realized that machines breaking down didn't just cost lives but also cost money in terms of downtime and business interruption. Attitudes to corporate social responsibility and commerce have developed a long way since then, and the inspection industry has become far more sophisticated, but the basic process is the same; by having experts assess equipment or processes, safety can be maintained, risk reduced and productivity increased.

Choosing an accredited inspection body is one of the best ways to ensure that it is both competent and impartial, having been itself assessed against robust and stringent criteria. And this, in turn, means that managers can have the confidence to plan ahead in the knowledge that they are receiving accurate data and that problems will be identified and addressed as swiftly as possible.

The certainty of uncertainty

It has been said that only death and taxes are certain. In business, however, this isn't the whole story. Another element that is certain is uncertainty. Even the most rigorous measurement in the world will involve an element of uncertainty, something that anyone who works in the world of calibration will encounter on a daily basis. Implicitly this is recognized throughout all levels of business, which is why the insurance industry is so large! However, managers – understandably – like to plan on what is, rather than what might be.

But this does not always take into account the possibility that there is something in the pipeline that could come as a complete surprise. In 2003, Donald Rumsfeld, then US Defense Secretary, explained this perfectly. At the time it earned him only ridicule, but examined closely it is a clear explanation of one of the problems facing risk managers. What he said was: 'There are known knowns; these are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know.'

The 'known unknowns' can be planned for to an extent, but what of the 'unknown unknowns', the things that you aren't even aware that you need to know? This is where the focus needs to shift from outcome to process. Businesses are goal driven as a rule, and this is only natural; there is nothing so concrete as results, and success is measured in results. But this might not be the best approach when planning for unfamiliar or unforeseen circumstances is concerned. 'Planning for unforeseen circumstances' might seem paradoxical, but by having robust processes in place before the unknown happens it is more likely that an organization will be well placed to react quickly and appropriately. This is why many businesses are opting to be certified to quality management standards such as ISO 9001. Having confidence in management systems means that an organization can reasonably expect to be as well placed as it can be to react both quickly and appropriately to a situation when the unknown occurs.

Insurance – a bit of culture

Insurers are increasingly looking at risk management and risk profiles as a way to determine what cover and premiums are most appropriate for a business. Where insurance was once a tool of risk management, the increasing sophistication of the industry – combined with new demands as the world of commerce constantly evolves – has meant that there is now a mirror image of that relationship as well. Insurers are now interested in a business's risk culture, and this is being used as a tool to help determine what a client needs in terms of insurance support. It is not surprising that the more sophisticated a business is in its approach to risk, the more confidence an insurer will feel and, in turn, the more appropriate the levels of cover on offer will be.

So what will an insurer be looking for when it assesses a 'risk culture'? It is most likely that it will be hoping to see systems and processes in place that demonstrate

a mature understanding of risk management and – crucially – that there is some guarantee that these systems and processes will be executed faithfully throughout the business at all times. There are a number of key areas that an insurer would be examining, including health and safety, environmental and management practices and a robust approach to quality. However, insurers are not experts in conformity assessment, nor in evaluating competence. Recently, UKAS has seen a growth in insurers recognizing accreditation as a sign of a sophisticated risk culture, reflected in lower premiums and more comprehensive cover. It would seem that accreditation and certification are fast becoming an effective way for a business to demonstrate an integrated approach to risk management.

When the worst occurs

The least pleasant aspect of risk management, though one of the most important, is planning for the worst. But it would be far more unpleasant for a business to find itself in that situation without a strategy. The Roman general Vegetius is said to have told his commanders 'Si vis pacem, para bellum', meaning 'If you would seek peace, prepare for war', an early example of sophisticated risk management! What constitutes 'the worst' will change tremendously between organizations, but one common denominator is to find a business embroiled in costly legal action, with another party seeking damages. However, the fact is, and the law recognizes, that sometimes things go wrong. What is crucial is how an organization reacts to things going wrong and whether it was at fault at any point. Organizations will therefore want to prove both compliance and due diligence and that both the company and the individuals were not negligent.

It is important to note that the law in this area has also seen some changes. Until 2007, gross negligence need only be proved in the actions of an individual. But since the Corporate Manslaughter Act it can now be found to have happened in the collective actions or culture of a company. What this means is that it is now even more important to be able to demonstrate that there is a culture of responsibility right across an organization.

It is clear that being able to demonstrate due diligence should be a vital part of any risk management strategy and that part of this should be to have a mechanism to demonstrate that it is built in at every level. This is another reason why third-party assessment is becoming popular as a method of determining and demonstrating competence. Regular and robust impartial assessment is one of the most effective ways that an organization can demonstrate, if called upon, that compliance and due diligence are not only taken seriously but built into management systems and processes from the start.

Conclusion

Having confidence – confidence in planning, process, system and, most importantly, information – is the starting point for ensuring that risk can be managed to

the optimal level for any organization. Wherever there is a need for accurate information or for a business to be able to demonstrate competence and confidence, there is a clear place for accreditation. The public sector has long recognized that accreditation is a mechanism to deliver confidence without the need for burdensome regulation or legislation, so it is no surprise that areas of the private sector, such as the insurance industry, are also coming to offer real financial benefits to accredited bodies. At a time when quality assurance and risk management will be the watchwords of any business looking to put the last few months behind it, accreditation is likely to become more pertinent than ever.

4.8

A question of perspective: uncertainty, resilience and efficiency

Allan Robinson, Appleyards

Introduction

We live in an age when increasingly turbulent events are putting an added focus on the many different aspects of risk and risk management. The (near) collapse of the global financial system has raised questions about the fundamental resilience of many of our organizations and institutions. At the same time there is an increasing focus on efficiency, both in the basic operations of many organizations (eg because of restricted funding) and in the mechanisms used to manage risk. But what do the terms 'resilience' and 'efficiency' actually mean and how do they relate to risk?

The *Chambers English Dictionary* has the following definitions:

- *resilience – recoil, elasticity, rebound*; in the context of risk, this could mean immunity to the effects of risk or, in the case of an assumption, how robust that assumption is (regarding the base position) and how likely it is to be correct;

- *efficiency – ratio of a machine's output of energy to input; capability of doing what may be required*; in the context of assumptions about an uncertain future, this means the relative efficiency of the base position implied by the assumption.

Many of the definitions of risk found in risk management guidelines and standards are of the type 'risks may represent threats as well as opportunities'. This stylized representation of uncertainty limits the way risk managers record, analyse and assess risks, and constrains the relationship between the risk management process and what it is being applied to. Overall, the aim of the risk management process is to improve organizational resilience and overall efficiency, by ensuring that the 'right' amount of resource is allocated by the organization to the management of response to risk.

Uncertainty can be defined only in relation to a base position (cost estimate, project schedule, operational process, etc). However, how do we tell if that base position was optimistic or pessimistic, realistic or fantastic? The answer is: we cannot, except by inference from the level of assessed risk exposure. From a strategic perspective, this means that it is hard to understand what the results of a risk management process are telling us. Is a given project really extremely risky, or is it merely that the base cost estimate was extremely optimistic?

This issue, which relates to the context in which any risk management process is implemented, is typically dealt with through phrases like 'following good industry practice', 'benchmarking', etc, to give credibility and confidence in the base position. However, since each project is unique, and given that the same set of risks can be and are looked at from different perspectives (eg a client organization issuing a tender as against bidders competing for the work), how can we compare the risks identified by each party without understanding how optimistic or pessimistic each base position is from a strategic perspective?

What are uncertainty, resilience and efficiency?

Uncertainty surrounds everything, past, present and future. It represents both the limits of our knowledge of the present and our ability to predict and forecast future events. When seeking to understand uncertainty, the first and most important point is to understand from what perspective we are looking.

For example, consider my journey to the train station every morning. In my experience, it takes approximately 15 minutes to drive from my house to the train station, with the fastest time being 8 minutes and the longest being 35 minutes. If I plan my journey on a particular day on the basis that it will take only 10 minutes to drive to the station, then experience suggests that I am being highly optimistic and am likely to be disappointed. On the other hand, if I allow 30 minutes for the car journey then experience suggests I am being highly pessimistic and am likely to spend several minutes waiting for the train to arrive. This demonstrates that it is only possible to assess the level of uncertainty in the context of the planned activity.

However, the optimistic and pessimistic options reveal a great deal about the relationship between uncertainty, resilience and efficiency. If I am pessimistic, then my assumptions are far more resilient and I am unlikely to have to worry about missing the train. On the other hand, if I am optimistic and succeed in getting to the train station in 10 minutes, then my base position is more efficient than if I allow 30 minutes, while should I fail to get to the train station in 10 minutes then my base position may turn out to be less efficient. This implies that resilience and efficiency are opposed in the context of risk management, in the sense that an attempt to increase resilience can reduce efficiency, and vice versa.

As the planned activity lies in the future, the plan also represents a whole suite of assumptions about what the future will be. Therefore another way of looking at the process of managing uncertainty is in the context of our assumptions and the uncertainty around them.

Assumptions and uncertainty

Any uncertainty management process is simply one of understanding the robustness of the assumptions we are making about the future. Each assumption we make, whether explicit or implicit, also represents a risk – the risk that the assumption will prove to be incorrect. If our assumption proves to be incorrect then understanding the impact of this failure in our assumption(s) is essential. Since we do not know which of our assumptions will fail, an uncertainty management process must consider the consequences associated with each assumption failing. This highlights that the true purpose of any uncertainty management process is to help decision makers understand the robustness and consequences of their decisions.

Figure 4.8.1 shows a graphical representation of how uncertainty relates to assumptions, and what those assumptions mean.

We can separate all assumptions into three categories:

- *Contextual.* These are the assumptions that form the context for the plan. For example, in the context of driving to the train station a contextual assumption is that I am going to drive to the train station, as opposed to walking from home, ordering a taxi or getting a lift from someone. The important point about these assumptions is that they are believed to be (by the decision maker): 1) robust, where the assumption is unlikely to change; and 2) valid, where the assumption is based around the best available information. In the context of a project, a contextual assumption represents the base plan, cost estimate or scope.
- *Normal.* If contextual assumptions represent the 'cast in stone' beliefs or the 'if this changes then we're not talking about the same project' type of assumptions, then normal assumptions represent the 'usual' sort of variability that does not require senior management involvement. In the example of driving to the train station, it represents the usual process for travelling to the train station, without the need to take exceptional or unusual action. In the context of a project, 'normal' assumptions represent those behind a particular value and will often be evidence based. For example, the statement 'It takes me on average

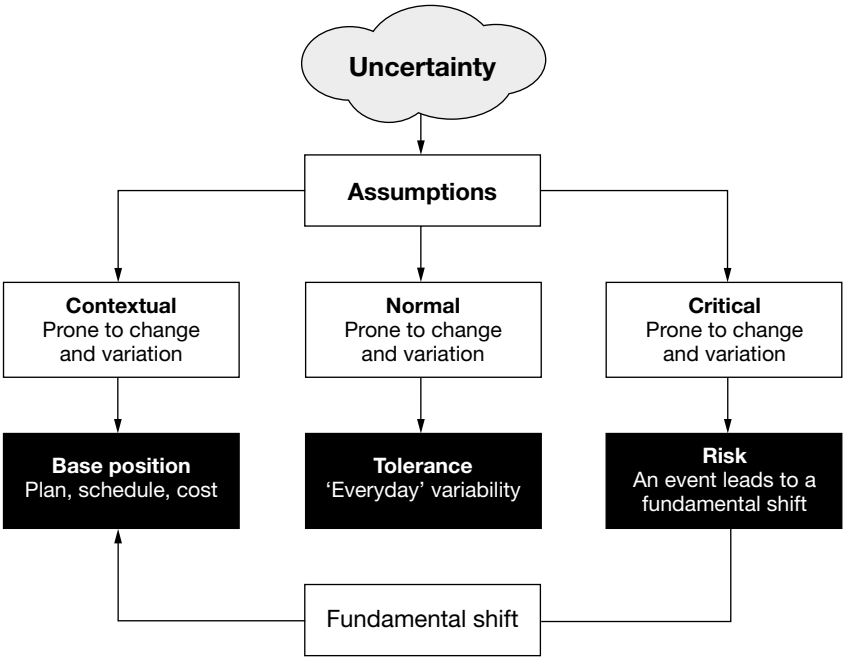


Figure 4.8.1 Relationship between uncertainty, assumptions and risk

15 minutes to drive to the train station' is subjective, but may be viewed as reliable given that I am the decision maker and I am trying to manage the uncertainty around my journey. These assumptions therefore represent the 'normal' range of variability around a project or process. In terms of a heat diagram, they represent the high-frequency, low-impact types of variability that are often not worth actively managing.

- *Critical.* Critical assumptions are the opposite of contextual assumptions. These assumptions are prone to change and variation and/or have a significant impact upon the objectives of the activity or project. Critical assumptions represent the low-frequency, high-impact risks in the heat diagram, the unusual events that are outside the norm. In the example of driving to the train station, a critical assumption would be 'I assume that my car won't break down.' This sounds like a reasonable statement, but is it? On what basis can it be assumed to be 'reasonable', what information is required to provide confidence in that statement, and what level of confidence does the decision maker require?

This classification is shown in Figure 4.8.2.

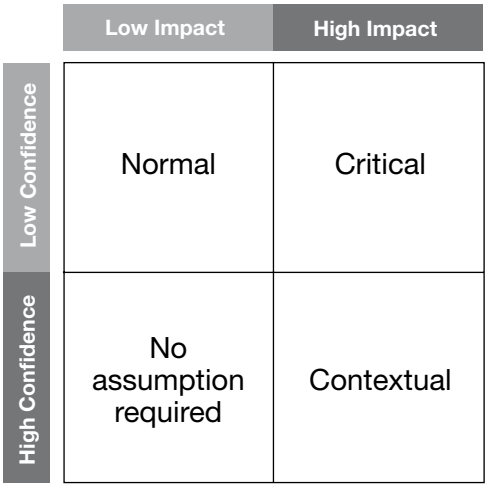


Figure 4.8.2 Assumptions classification

Assumptions, resilience and efficiency

Case study: Risks, assumptions and subjectivity

If all assumptions may lead to risks, then it follows that any uncertainty management process that hopes to be complete will have to take account of those assumptions within the process.

On a complex infrastructure programme, this led us to introduce assumptions dictionaries as a means of keeping track of all the various assumptions being made by different parts of the organization. Each of these assumptions presented a potential uncertainty, and there was also the possibility of different parts of the organization making conflicting or contradictory assumptions.

As we implemented these assumptions dictionaries, we were faced with questions as to what information needed to be included and, fundamentally, what an assumption is. The *Chambers English Dictionary* definition is: *that which is taken for granted or supposed*. For our purposes, we defined assumptions as the subjective beliefs, both explicit and implicit, of an individual or team about the future within a particular context. This highlights our belief that all information within the uncertainty management process is fundamentally subjective – even if a large amount of objective data is available around an area of uncertainty, the use of the data to inform (either

statistically or otherwise) our view of the future is based on the often implicit assumption that the future will be the same as the past.

Recent events both in the environment (climate change) and in the financial services industry (credit crunch) demonstrate that the reason uncertainty management is important is because the future is not the same as the past.

Given our earlier definition and in the context of risk management, resilience may be considered to be the confidence that an assumption will not be proved incorrect or, more precisely, that events will not turn out worse than a given assumption implies. The assumption that it will take no more than 30 minutes to drive to the train station is resilient – experience suggests it is unlikely to be proved incorrect. Efficiency, on the other hand, relates to what the assumption implies about our base position and is therefore relative: the assumption that it will take no more than 10 minutes to drive to the train station gives a more efficient base position than the assumption that it will take 30 minutes.

In the context of risk, efficiency also relates to the magnitude of risk exposure. The maximum risk exposure under both assumptions is the same in absolute terms; however, proportionately the scale of the risk is much greater for the more efficient assumption. This leads us to a different classification of assumptions (see Figure 4.8.3).

Thus we see that the assumptions that are critical are those that both are fragile (ie not confident that they will be correct) and lead to an efficient base position.

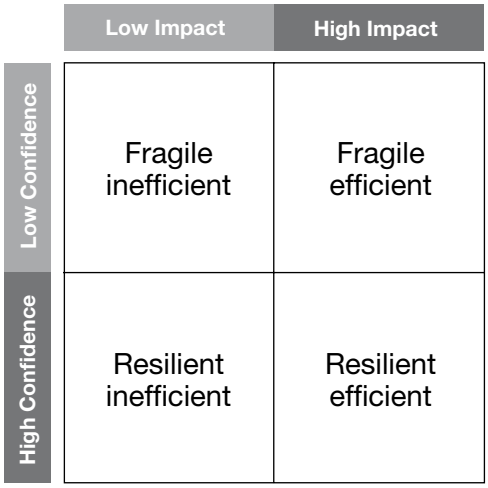


Figure 4.8.3 Resilient/efficient assumption classification

Opportunity and optimism

Optimism by definition implies that more output is produced for a given input, so that there is a correlation between optimistic assumptions and those that are efficient. Similarly, pessimistic assumptions are by definition those that will be more resilient, as it is less likely that reality will prove worse than a resilient assumption.

However, another way of looking at resilient versus efficient assumptions is to consider opportunities. A resilient assumption allows for the potential to exploit opportunities should they arise. Having allowed 30 minutes to drive to the train station, I may arrive in sufficient time to catch an earlier train, have a coffee, buy a paper, etc. It is less likely that I would be able to take advantage of such opportunities if I have made the efficient assumption that I will get to the train station in 10 minutes.

One of the common pitfalls encountered in risk and opportunity management processes is that project teams assume that the opportunities will occur while the risks may occur. Essentially, opportunities get built into the base position without proper accounting for the potential failure of the assumption that the opportunity will occur.

By considering the resilience and efficiency of each assumption, we get another perspective on whether a particular assumption (and what it implies about the base position) is optimistic or pessimistic.

Uncertainty analysis

Once we have a clear understanding of the assumptions that we are making, we can then begin to assess the uncertainty surrounding those assumptions. Similarly to what happens in the quantification of risk this becomes the likelihood that the assumption is correct (which approximates to resilience) and the impact on the objectives of the project, process or activity should the assumption prove incorrect (which approximates to efficiency).

Case study: The limits of knowledge (or risk and quantum physics)

For a major metropolitan transport organization, one of the key issues faced is: what is the condition of our physical infrastructure assets? Where detailed information on the condition of an asset is not available, assumptions have to be made to allow the normal business processes to proceed. Asset A is of unknown condition. Asset B is known to be at condition X, and is of similar age and type to Asset A. Therefore, we can assume that Asset A is also of condition X, and will require work Y to be done at time Z. However, when Asset A is actually investigated, it may turn out to be in a very different condition to that assumed.

All of this is very similar to the principles of quantum physics. Schrödinger's cat faces the risk of being poisoned, with a certain probability (unknown) and impact (death of the cat). Even though the condition of the cat is decided in advance of the box being opened, our uncertainty regarding the risk cannot be resolved until the box is opened.

This reveals that the key point in time for any uncertainty and its associated assumptions is the point at which the uncertainty materializes, when we open the lid of the box to see if the cat is alive or dead.

For example:

Assumption 1: The drive to the station takes 15 minutes. It is unlikely that 1) the journey will take exactly 15 minutes and 2) the average journey to the station is exactly 15 minutes, given that this quantification (of 15 minutes) is based on my subjective judgement of what a reasonable time for that journey should be, so we might say that it is 100 per cent likely that the time taken to drive to the station will be somewhere between 12 and 20 minutes, though it is most likely that it will take 15 minutes.

Assumption 2: My car will not break down. The car I currently own has never broken down. However, in my experience of car ownership (let's call it 20 years) I have had two breakdowns and two accidents. So let's say there's a four in 4,000 (20 years × 200 driving days), or 0.1 per cent, chance of a breakdown on a given day, with the result that my journey to the station takes between two and four hours.

The first example represents a 'normal' assumption. There is some inherent variability in it (probably owing to some further unidentified assumptions – such as which route I take), which is hard to manage successfully. The second example represents a 'critical' assumption. If my car breaks down it will have a significant impact on my journey. It is much easier to manage (eg have the car serviced regularly), but cannot be completely avoided even when mitigated.

From a risk management perspective, we are assessing the risk that the assumptions we are making are not in fact true.

Reduced uncertainty

Having assessed all the assumptions that generate our base position we are now able to assess whether, in our view, our base position is optimistic or pessimistic, and if appropriate to adjust it to make it more realistic. It is quite possible that in certain circumstances an organization will choose to take an optimistic or pessimistic view, as that aligns better with the organizational objectives and risk appetite, by making assumptions that are more resilient or more efficient.

Making this choice consciously, however, allows for more robust decision making and reduced uncertainty.

Summary

The future is uncertain, and by default we make assumptions about how the future will turn out. By examining, testing and reviewing these assumptions we:

- make the assumptions explicit – thus enabling us to ascertain whether we think they are realistic;
- are enabled to understand whether our base position is optimistic or pessimistic, and whether this is appropriate;
- are provided with a way to integrate risk management and risk analysis explicitly with the assumptions that lie behind the base position.

4.9

Sometimes the softer issues cause the hardest problems

Graham Massie, Centre for Effective Dispute Resolution (CEDR)

This chapter is different from most others in this book. Whereas they cover specific risk topics, I want to discuss the uniform people-related aspects of risk that apply to nearly every situation in which an organization or group of individuals need to identify and agree upon their response to risk issues.

My background is that I'm a commercial mediator. As a neutral intermediary, I help organizations negotiate settlements to often complex and high-value business disputes. And in nearly every single case I handle, the question of risk comes up. Whether it's debating the chances of winning or losing at trial, or quantifying the operational consequences of continuing with damaged relationships and distracted executives, risk comes up as a key consideration in virtually every discussion.

As evidenced by the other chapters in this book, risk management is a very sophisticated field. And yet it still bothers me that – in what I suspect is largely an attempt to bolster their own confidence – people will claim they've got a '75 per cent chance of winning at trial'.

The trained statistician in me yearns to understand how they have come to such a conclusion – and what they mean by it. Presumably, they're saying that if the same dispute was separately heard by 100 different judges then they would prevail 75 times. But that's never going to happen in practice. And in any event how does such analysis square with the other side's perspective? In a perfect market of equal knowledge and equal expertise, then, does this imply that the other side are running their case with only a 25 per cent expectation of success?

Of course, the law reports bear weighty evidence that for every winner there is also a loser – a long-run success rate for litigants as a whole of only 50 per cent. Yet mediators are well used to discovering that both sides are telling themselves they have a 75 per cent chance of success. Part of my job is to address such anomalous joint perspectives by facilitating information exchange and encouraging fuller analysis and evaluation – in effect, helping parties move towards a position of shared information and mutual understanding.

And yet, even if I do achieve the nirvana of reducing parties' aggregated evaluations of their likelihood of success to only 100 per cent, we still have to consider the matters of how individuals respond to risk in conflict.

To confuse the situation even more, some of us will be quite prepared to take on a 60 per cent chance of winning, but would be scared off by a 40 per cent chance of failure. This isn't just a question of the diminishing marginal utility of money (the richer we get the less value we place on the next £1,000) or of what Thaler[1] called the endowment effect (whereby we place a higher value on things we already own) but also, more worryingly, of simply how the question is asked – as a general rule, we are so risk averse that we would rather, say, choose a medicine that saves 40 per cent of patients rather than one that we are told will still see 60 per cent die.

Helping parties conduct an appropriate risk analysis is an essential part of the toolkit of the commercial mediator, and we are generally very good at what we call 'reality testing' – helping them identify and think about the relative strengths and weaknesses of their and their opponent's situation.

What we pay less formal attention to, however, is the question of how parties respond to risk in these conflict situations. So in this chapter I would like to explore other aspects of our psyche that seem to apply even where the full extent of risks is brought to our attention. Key questions include: How do we evaluate risks? What factors influence our appetite to take on such risks? And are we always the rational actors that we like to think we are?

Personalization of risk

As a starting point, we should recognize that helping people to identify risk is not sufficient. For all too often, even when we accept intellectually the theoretical possibility that something will go wrong, we comfort ourselves with the assurance that 'Surely it won't happen to me', that somehow we're immune from the fortunes that affect ordinary folk. Reflecting what social scientists now term the Lake Wobegon effect,[2] numerous studies have shown that, across a wide range of char-

acteristics and traits, a statistically improbable number of people tend to regard themselves, or their luck or skill, as being above average.

Of course, you and I are too sophisticated to fall for such conceit. But ask yourself this: 'Am I a good driver? Above average?' Ask your colleagues for their rating of their driving ability too, and see if your experience bears out the results of repeated studies that reveal that around 80 per cent of us claim to be above-average drivers – a figure that remains remarkably constant even when the survey is taken amongst participants in driver re-education programmes or traffic school. Thus, even people who have convictions, of the criminal variety, for poor driving nevertheless retain faith in their ability to be above average!

The same thing happens in risk situations. We can see ourselves as immune from risk, dazzled as we are by our own self-confidence, and failing to see any daylight from other perspectives, often with the result that we get a nasty surprise later on.

As a mediator, I often have to spend a lot of time with parties revisiting their risk analysis, encouraging them to reflect fully on the strengths of their opponent's position, on the weaknesses of their own, and on the vagaries of what former US Defense Secretary Donald Rumsfeld once termed 'the known unknowns' and 'the unknown unknowns'.[3]

Perception of risk

Of course, it is only if we can get all of the risks of any situation laid out on the table that we can have any chance of undertaking a proper evaluation. However, unfortunately, we are not very good at assessing the level of risks even when they are brought to our attention. I'm a very relaxed traveller, but as I write this chapter at some 36,000 feet above the Middle East en route to London even I can feel a heightened sense of nervousness as I see my companion reading the latest news of the recent air disaster in the South Atlantic. Obviously, I'm not at any greater risk than the last time I flew, but the possibility is now at the forefront of my mind and makes me worry just a little more. And I also worry more than I should about dying in a fire, or of cancer, or from a snakebite. Why? Because, like most people, I am not very good at calibrating different levels of risk. Research has shown that we all tend to overestimate the risks of suffering from one of the higher-profile or more spectacular causes of death, and we underestimate our exposure to the more mundane, or at least less luridly publicized, causes (such as diabetes, stroke or asthma).[4]

The old joke about doctors reveals how this plays out in risk situations – we all celebrate our successes and bury our failures. And thus it is our successes that are at the forefront of our mind – not only do we rejoice in past victories, but we pay more attention to formulating the winning arguments to support our own position than we do to listening and responding to the merits of someone else's analysis.

Quantification of risk

And our difficulties in the perception of risk are only heightened once mathematical figures or patterns become involved. There may be a stereotype that only accountants are obsessed with numbers, but the failure of business managers to compute probabilities and to assess risks or patterns of behaviour is a worryingly widespread failing.

Try yourself on the following questions:

1. If I toss a coin seven times, which of the following sequences of heads (H) and tails (T) is most likely to be observed?
   (a) HHHHHHH
   (b) HHHTTTT
   (c) THHTHTT
2. A claimant knows that, in order to succeed at trial, it will have to persuade the judge on 10 separate issues. Counsel advises that it has an 85 per cent chance of succeeding on each individual point. Should the claimant pursue the case to trial?
3. How many people must there be in a room before it becomes more likely than not that two of them share the same birthday?
   (a) 23
   (b) 103
   (c) 183

Each of these questions challenges our ability to compute probabilities associated with multiple events. We all know that on a single toss of a coin there is a 50:50 chance that it will come down heads. But, when looking at multiple events, our inclination is to look for patterns. Some of us fall prey to the gambler's fallacy: 'I've flipped heads with this coin five times consecutively, so the chance of tails coming out on the sixth flip is much greater than heads.' Others fall for the clustering illusion (also known as the patternicity effect) – a tendency to find meaningful patterns in meaningless noise. When he said that 'Once is happenstance; twice is coincidence; three times is enemy action',[5] Auric Goldfinger, James Bond's wealthy nemesis, may have had particular concerns about people interfering with his plans, but he would have been wrong to read anything into the apparent patterns in answers (a) and (b) to my first question. In fact, assuming a fair coin toss, each of the three sequences is equally likely.

My other two questions highlight the difficulties many of us have with composite probability assessments – of computing risks that are dependent on a series of events. Intuitively, most of us would consider that the claimant in question 2 has a fairly good chance of success, but, when the 85 per cent probabilities are multiplied together, the combined result drops very quickly, down to below 20 per cent in fact.[6]

The birthday question is an application of the same principle, with the maths leading to the even more counter-intuitive result that only 23 randomly chosen

individuals need be in a room before it becomes more likely than not that two will share the same birthday.[7]

So what does all of this say about our risk assessments? Simply that we're not very good at gauging the odds. We see patterns that don't exist, leading to unfounded predictions, and we underestimate the implications of compound probabilities, leading to overconfidence about our chances of success in complex situations.

Over-reliance on limited data

We also often base decisions on very limited data. Consider an informal experiment reported by Stuart Sutherland in which he compared his own perceptions of Australians following a visit to Earls Court in London with his findings from a subsequent visit to Sydney.[8] Based on his Earls Court experience, he described Australian men as being 'loud and hearty' and 'slightly uncouth', but his later visit to Sydney found its residents to be 'extremely courteous and gentle'.

Motivated scepticism

This tendency to place excessive reliance upon limited data is exacerbated when the data have been gathered through our personal experience, or where they confirm our existing prejudices or beliefs, possibly leading to the conclusion that the way individuals respond in risk situations depends, at least to some extent, on their degree of familiarity with other similar situations.

Taber and Lodge have proposed a model of 'motivated scepticism' whereby, when we are presented with a balanced set of pro and con arguments, we tend to place greater reliance upon those that support our prior views, and we place less reliance on – and even seek to disprove – opposing arguments and evidence.[9] Even more worryingly, this biasing also affects our future researches – when looking for fresh material to consider, we tend to seek out confirmatory evidence. And the consequence of these biases is that, as time goes on and more and more evidence is considered, our attitudes become even more polarized.

This behaviour presents a challenge in risk management, explaining as it does why so many organizations become more and more embedded in collective denial rather than properly address the realities of their situation.

Groupthink

The role of the group also has an impact upon parties' evaluation of risk situations. In a phenomenon known as 'risky shift', people in groups make decisions about risk differently from when they are alone, with the group generally likely to take riskier decisions.

A number of reasons have been advanced to explain this behaviour; possibly the shared responsibility of a group decision eases the burden on the individual (ie a diffusion of responsibility); perhaps higher-risk takers have higher social status

and/or are more persuasive in influencing the group decision; or perhaps it is simply that, as people pay more attention to a possible action through group discussion, they become more familiar and comfortable with it and hence perceive less risk.

Whatever the reason, the implications for risk management are clear. With group decision making involved in most corporate matters, there is a clear need for the questioning, or at least sceptical, voice. But not every team is sufficiently robust to be able to cope with the dissident, and it is not uncommon for a further level of internal conflict to break out if one individual is regarded as not being a team player, particularly in stressful situations where the team is seeking to bond together against a common concern.

Clearly this is one area in which a mediator or neutral chairman of discussions, as a trusted outsider, can play a key role; but I would suggest that a more effective solution would be to have sufficient conflict literacy and self-awareness within a team such that it can tolerate someone – a designated cynic if you will – who can take a long, hard and dispassionate look at the realities of a situation, to ensure not only that the assessments of risks are accurate but also that the organization achieves cost-effective and workable responses.

This means training, not just in risk management but in the communication and teamwork skills necessary to manage the conflict of differing opinions effectively. Comprehensive identification and management of risk require thorough analysis and debate that can tolerate differences on the issues whilst maintaining team cohesion and avoiding dissent degrading into relationship conflicts. These are the sorts of skills with which conflict management professionals are familiar, and they need to be part of the risk managers' skill set if they are to have any chance of overcoming the obstacles that our human foibles and often irrational responses to risk situations put in the way.

Notes

1. R Thaler (1980) 'Toward a positive theory of consumer choice', *Journal of Economic Behavior and Organization*, **1**, pp 39–60.
2. 'Lake Wobegon… where all the women are strong, all the men are good-looking, and all the children are above average.' Garrison Keillor, *A Prairie Home Companion*.
3. 'There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know.' US Defense Secretary Donald Rumsfeld, February 2002.
4. B Fischhoff, P Slovic and S Lichtenstein (1979) 'Weighing the risks: which risks are acceptable?', *Environment*, **2**, pp 17–20, 32–8, reprinted in P Slovic (2000) *The Perception of Risk*, pp 121–36, Earthscan, London.
5. Ian Fleming (1959) *Goldfinger*.
6. The formula to compute overall chance of success is: $(0.85)^{10}$ or (85% × 85% ×… × 85% × 85%) = 19.7%.

7. The formula for the chances of no duplicated birthdays is: $^{365}/_{365} \times {}^{364}/_{365} \times {}^{363}/_{365} \times {}^{362}/_{365} \times {}^{361}/_{365} \times {}^{360}/_{365}$ etc. This produces a result below 50% with the 23rd multiplication (ie … $\times {}^{343}/_{365}$).
8. Stuart Sutherland (1992) *Irrationality*, Constable, London.
9. Charles S Taber and Milton Lodge (2006) 'Motivated skepticism in the evaluation of political beliefs', *American Journal of Political Science*, **50** (3), pp 755–69.

5

Patent Filing, Defence and Litigation

MAIKOWSKI & NINNEMANN

Patentanwälte • European Patent and Trademark Attorneys



Mission

Taking personally care of our clients' interests has been in the center of our strategic thinking and work for the last 30 years. Whether your company is large or small, you will find a permanent and personal counsel – that is the basis for an individual, trusting relationship that is fundamental to our success together.

The firm

Maikowski & Ninnemann is a leading Patent Attorney Law Firm with offices in Berlin and Munich.

Our work covers all core areas of intellectual property such as prosecution, ligitation and defence of patents, utility models, trademarks and design rights as well as counselling on inventions, trademarks, designs, know-how and licenses.

Fields of competence

- Automotive engineering, naval technologies and mechanical engineering
- Telecommunications
- Semiconductor technology
- Electrical engineering and electronics
- Medical technology
- Optics, light engineering and precision mechanics
- Software
- Polymer chemistry
- Biotechnology

MAIKOWSKI & NINNEMANN

Patentanwälte • European Patent and Trademark Attorneys

Kurfürstendamm 54-55
D-10707 Berlin
Tel. +49-30-8818181
Fax +49-30-8825823
E-Mail office@maikowski-ninnemann.com
Internet www.maikowski-ninnemann.com

5.1

Reducing business risk through patent strategy

Gunnar Baumgärtel, Maikowski & Ninnemann

Creating value through intellectual property (IP) is an important aspect in business. However, intellectual property is also a source of significant business risk. If an organization fails to protect its intellectual property it runs the risk that the intellectual property is exploited by competitors, which will cause a loss in revenues and will harm the public image of the organization.

Furthermore, third parties' intellectual property rights, such as patents, pose a considerable risk for any organization because an infringement of those intellectual property rights may result in detrimental legal consequences such as an obligation to cease and desist from making, offering and selling infringing products as well as an obligation to pay compensation for damages.

In this chapter we shall discuss how the risks outlined above may be minimized by an effective IP strategy. More specifically, the discussion will focus on intellectual property in the form of patents, ie on intellectual property rights serving to protect technical inventions.

Patents

In general, *patents are granted for inventions in all fields of technology* that are new and involve an inventive step with respect to the prior art. Technical inventions

that can be protected by patents include devices, products and processes in any field of technology, such as chemistry, physics, electrical engineering, mechanical engineering, biotechnology and so forth. In Europe, patents may be granted either through national law or through the European Patent Convention (EPC). National patents confer protection in a specific country. European patents confer protection in up to 36 member states of the EPC depending on the number of states designated in a European patent.

Owing to the harmonization of patent law in Europe, national patents on the one hand and European patents on the other hand have the same effect. *A patent confers on its proprietor the right to prevent all third parties* not having the proprietor's consent *from making, offering, putting on the market or using a product that is the subject matter of the patent*, or importing or stocking the product for these purposes. This means that an organization that succeeds in protecting its intellectual property and more specifically its technology by patents is in a position to prevent all competitors from using the protected intellectual property/technology.

To obtain a patent, a so-called patent application has to be filed with the competent national Patent Office or the European Patent Office. The Patent Office will examine whether the claimed invention, ie the subject matter of the patent application, is new and involves an inventive step with respect to the prior art. If so, a patent will be granted so that all third parties are excluded from using the subject matter claimed in the patent.

It is very important to note that a *patent does not confer on its proprietor a positive right to use the subject matter of the patent*. It is not uncommon that a patent is granted for a specific aspect of a device, product or process while at the same time an earlier patent exists for a more general concept covering the same device, product or process, ie an organization may obtain a patent for a specific improvement of a device, product or process that is also protected in a general manner by an earlier patent. As an example, let us consider a patent relating to an improvement of an optical sensor for monitoring and controlling a specific chemical process. A sensor manufactured according to the patented invention may be more reliable and cheaper than the sensors that had been used to monitor and control the respective chemical process so far. By means of the patent, the patent owner may prevent third parties from using the improved sensor in order to control the chemical process to which the patent applies. However, if there exists an earlier patent relating to the general concept of using an optical sensor to control the chemical process in question, then the owner of the earlier patent may prevent the owner of the second (younger) patent (relating to an improvement of the sensor), from using an optical sensor to control the chemical process at all. Thus, even if an organization obtains patent protection for a device, product or process (such as an improved optical sensor for controlling a specific chemical process), this by no means excludes the risk that the organization may at the same time infringe an earlier patent relating to a more general concept (such as the concept of using an optical sensor for controlling a specific chemical process).

To summarize, by *protecting its intellectual property/technology through patents an organization may prevent third parties from using its intellectual property/*

technology so that the organization has an exclusive right (monopoly) to make, offer and sell the product. However, *this does not eliminate the risk that the patented invention (technology) may infringe an earlier patent* owned by a competitor. In this case, the owner of the earlier patent may obtain an injunction, in some cases even a so-called preliminary injunction issued within weeks or even days, preventing the organization from using its (patented) technology. Furthermore, the organization will have to pay damages, which may amount to all profits made by selling the infringing products; and the owner of the earlier patent may obtain permission to have the infringing products removed from the market and/or destroyed, including products that had already been sold to customers. Thus, by filing patent applications and obtaining patents for its intellectual property an organization may prevent third parties from exploiting the protected intellectual property. However, there is still a substantial risk that even a product that is protected by a patent may at the same time infringe earlier patents so that it is impossible to put the product on the market, leading to a situation that may threaten the existence of an organization. Consequently, in order to minimize business risks through patent strategy an organization has to deal simultaneously with two aspects, namely: 1) the protection of intellectual property/technology through patents; and 2) careful study and consideration of third parties' patents on the same footing.

Protecting intellectual property through patents

In order to obtain optimum patent protection for an invention, it might appear to be necessary to file patent applications in all countries where competitors could manufacture, offer or sell a claimed device or product or could apply a claimed process. However, this might cause tremendous patent costs.

Therefore, a more elaborate patent strategy can be useful in obtaining a sensible patent protection at reasonable expense:

- After an invention has been made that is to be protected, it is sufficient to *file a patent application in a single country in a first step*. By filing a so-called 'first application' in one country the applicant is entitled to a 'priority right'. This means that the applicant may file additional applications in other countries within one year from the filing date of the first application by claiming the priority of the first application. All additional applications (relating to the same invention) that are filed within one year from the first application are treated as if they had been filed on the same date as the first application. Thus, after filing a single patent application for an invention in one country the applicant has one year to investigate the technological and economic relevance of the invention and to decide whether the relevance of the application justifies seeking patent protection not only in a single country (eg in the country where the applicant has its main place of business) but also in a number of additional countries.

- Furthermore, in many cases it is not necessary to seek patent protection in all countries where an invention might be put on the market by a competitor. The reason for this is that there might be only a limited number of countries where competitors are active that are capable of manufacturing a claimed device or product. In such cases it would be sufficient to seek patent protection in those countries where the most relevant competitors have or may have (future) facilities where a claimed device or product can be produced.
- And in those cases where a device or product that is to be protected can be produced in almost any country, it is frequently sufficient to obtain patent protection in a limited number of countries. For example, if a product is put on the European market it will normally be available in all or at least most European countries. *Thus, if patent protection is obtained in a number of core countries it will be possible to prevent third parties (competitors) from successfully marketing the product* in all of Europe or even worldwide. Preferably, patent protection is to be sought in countries providing an effective judicial system for the enforcement of patents.

Freedom to operate

As discussed above, intellectual property rights such as patents confer on their proprietor the (negative) right to prevent third parties from using the patented invention. However, they do not confer a positive right to use the invention if there are conflicting earlier patents. (This is in contrast to other areas of property law where ownership means both a positive right to use the property as well as a negative right to exclude third parties from using the property.)

Therefore, it is essential that a so-called *freedom-to-operate analysis* is performed before a new product is put on the market in order to determine whether the product may infringe third parties' patents. The same is true in cases of business transactions such as mergers, acquisitions, joint ventures or financing of young companies.

Failing to perform a freedom-to-operate analysis means running a high risk of infringing third parties' patents, ie the risk of being forced to stop the production of infringing products, to destroy infringing products that have already been put on the market and to pay damages.

When performing a freedom-to-operate analysis the first step is to determine those third parties' patents and patent applications that are potentially relevant in a specific case (patent search).

As a second step, a detailed analysis has to be made to identify those patents that may be infringed by the product to be put on the market.

If there is potential infringement, then there are various possibilities to react:

- One may try to design around the patent, ie to modify the product in question in such a manner that there is no infringement.
- A prior art search may be performed in order to determine prior art on the basis of which a conflicting patent may be attacked and invalidated.

- In other cases it may be possible to obtain a licence under the patent or to purchase the patent.
- In cases of business transactions such as mergers, acquisitions, joint ventures, financing and so forth one may reconsider the value of the transaction in case serious problems with third parties' patents are found.

Summarizing, it is *essential to perform a freedom-to-operate analysis whenever a new product is to be put on the market or a business transaction is planned*. The ownership of patents per se does not reduce the risk of infringing earlier third parties' patents.

Conclusions

In order to reduce business risk through patent strategy, two aspects are of equal importance, namely: 1) protecting intellectual property/new technology through patents; and 2) determining and analysing possibly conflicting third parties' patents in order to avoid infringement. These aspects of patent strategy are *closely intertwined*.

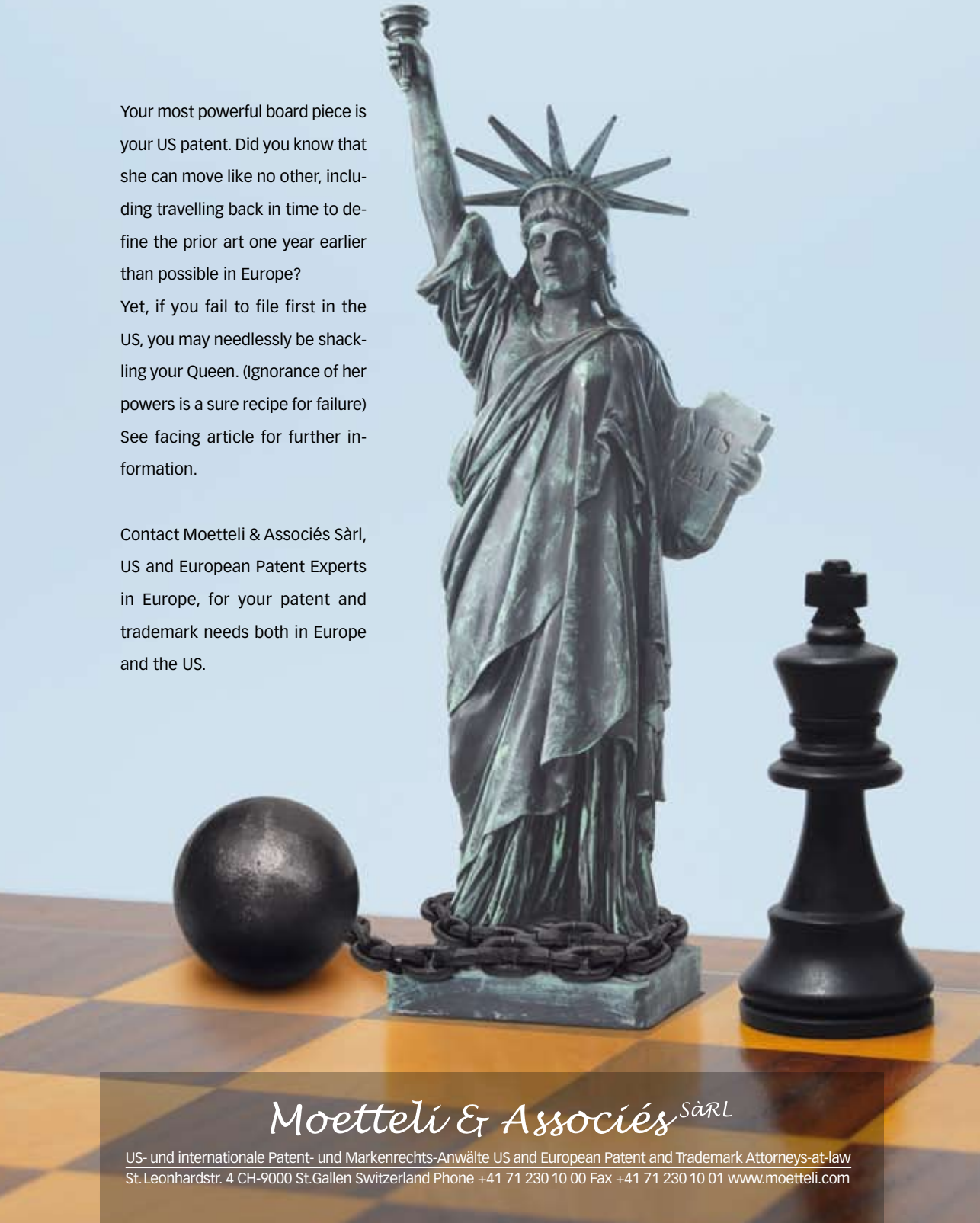
For example, after filing a patent application in order to protect a new technology the applicant will receive a search report and/or office action from the competent Patent Office citing prior art that is relevant with respect to the subject matter of the application. By analysing the prior art the applicant will learn which competitors are active in the respective technical field, providing a first indication of where to look for possibly conflicting earlier patents.

On the other hand, by performing a systematic prior art search in order to prepare a freedom-to-operate analysis an organization will learn a lot about the state of art concerning the relevant technology, which may be extremely helpful for its own efforts in research and development and which may in particular provide new starting points for additional inventions.

In conclusion, business risk involved with IP can be systematically reduced by filing patent applications for new inventions and at the same time performing regular freedom-to-operate analyses in order to avoid infringement of third parties' patents. These two aspects of patent strategy mutually support each other, enabling an organization to minimize IP-related business risk effectively.

■ 256

DON'T SHACKLE YOUR QUEEN!



Your most powerful board piece is your US patent. Did you know that she can move like no other, including travelling back in time to define the prior art one year earlier than possible in Europe?
Yet, if you fail to file first in the US, you may needlessly be shackling your Queen. (Ignorance of her powers is a sure recipe for failure) See facing article for further information.

Contact Moetteli & Associés Sàrl, US and European Patent Experts in Europe, for your patent and trademark needs both in Europe and the US.

Moetteli & Associés SàRL

US- und internationale Patent- und Markenrechts-Anwälte US and European Patent and Trademark Attorneys-at-law
St. Leonhardstr. 4 CH-9000 St.Gallen Switzerland Phone +41 71 230 10 00 Fax +41 71 230 10 01 www.moetteli.com

5.2

Patent filing strategy to minimize litigation risk

John Moetteli, Moetteli & Associés SàRL

Introduction

Few risk managers are aware that one simple choice made as part of a company's overall patent strategy can be fine-tuned to significantly reduce litigation risk, namely the choice of where a company starts the patent application process. Where permitted under national law and where there is a potential market for the product in the US, patent applications should be filed in the United States first. This chapter is intended to enlighten risk managers so that they can help their Europe-based clients loosen the deep-seated practice of home-country priority filings that, in most cases, needlessly handicaps the client vis-à-vis their US-based competitors.

Clients are best advised to start their patent filings in the country of the most commercial importance to them as determined by the market in that country, or by the presence of competitors or potential licensees.[1] Systematically taking the correct first step can significantly increase the value of the company's patent portfolio, which in turn reduces litigation risk. The practice of merely filing locally without justification other than tradition only haphazardly serves the client's best interests. Why? Because, where the US market is important, failing to file first in the United States needlessly handicaps the client's US patent rights, which may ultimately subject the client to a patent infringement suit and so cause commercial damage to the client.

Yes, for companies whose markets are local and whose inventions have little licensing value in the United States, advising the client to file a patent application locally is certainly legitimate. On the other hand, for globally minded clients and for clients whose inventions may have a significant market in the United States, clients should file in the United States first or at least concurrently with or immediately after a home-country filing. Why? If clients do not file early in the United States, they can lose significant rights because, with each passing day that the US filing is delayed, more prior art can be cited against the client's US application. If clients fail to obtain patent rights for their products in the United States, then they have no in-kind currency that can be used to entice a partner or competitor to sign a cross-licence agreement. Consequently, clients may needlessly subject themselves to a patent infringement suit, or the need to pay license fees that, had they filed the patent application in the US first, they might have been able to avoid. Besides this, filing first in the United States makes good business sense. The United States has a developed patent system (more than 200 years old) that, in many ways, has helped shape the laws of many other industrialized nations. This developed patent system helps reduce uncertainties, which increase the risks of litigation. Still further, the United States remains a dominant force in international commerce and, if clients are forced (because of budget constraints, for example) to choose one single national patent to have in their portfolio, most clients choose a US patent.[2]

For these and other reasons listed below, the client's US patent rights are probably the most flexible and powerful tools for monetizing an invention, particularly where a potential licensee or infringer resides in the United States. To fail to communicate the advantages of early filing in the United States is the strategic equivalent to a chess instructor failing to tell a student that the queen is allowed to move in all directions as far as the way is clear. In other words, failing to communicate these advantages typically results in diminished US patent rights caused by an up-to-one-year loss in priority for the US application. Winning at the game of intellectual property is difficult enough without being handicapped by ignorance of the rules of the game. The game is global now, and clients expect to be informed of the basic rules affecting their international patent strategy, particularly if ignorance of a simple rule subjects them to increased litigation risk.

The author has identified more than 20 reasons supporting a patent strategy that begins with an early US filing. Besides the case where a co-inventor is a resident of the United States (in which case filing in the United States first is obligatory), here is an ordered listing of the 10 most compelling such reasons.

The 10 most compelling reasons for filing first in the United States

1. First and most important is to better ensure that the client obtains the broadest possible US patent, which if obtained can be used to barter away litigation risks. Filing in the United States first allows the applicant to jump back in time one year in defining the prior art against which the client's US patent application will be judged. In other words, filing early in the United States is necessary

in order to take advantage of the one-year grace period in which prior art is defined one year prior to the filing of the client's first US application, thereby excluding from the prior art the client's own as well as third-party disclosures that take place during the one-year period immediately preceding the US filing. Here's why: Title 35 USC, section 102(b), states the following:

> 35 USC §102 Conditions for patentability; novelty and loss of right to patent
> A person shall be entitled to a patent unless
> … (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States…

Consequently, although the priority filing date is the date that determines prior art for a European patent (and in fact most national or regional patents), for a US patent, prior art is defined one year before the earliest filing in the United States.[3] Yes, although the practice of 'swearing behind' using the clients' non-US priority filing as evidence helps to a limited extent because clients can claim inventorship at least back to their priority filing date (only available for WTO member countries), this allows clients to go back in time only to their priority filing date, *not one year earlier* than their priority filing date, as they would have been able to do if they had filed first in the United States. Consequently, if clients choose to file anywhere but the United States first, they are choosing to put themselves at a disadvantage vis-à-vis other patent filers who have 102(b) filing dates in the United States that are earlier than the clients' priority filing dates. In almost all cases, this would be a strategic mistake that rational clients, if fully informed, would never expect to make were it not for their ignorance of the rules. Although it's the duty of patent attorneys to inform their clients of current law and rules in order to help ensure that clients do not make such mistakes, unfortunately, self-interest sometimes clouds the advice that client's receive from their patent attorneys. Consequently, a client's risk manager can act as an important check to patent attorney self-interest by sharing the responsibility of informing their clients of the significant advantages of filing patent applications in the US first.

One may fairly ask, why does early filing in the United States offer this very significant advantage? It is because the United States is a first-to-invent country (not a first-to-file country), and US authorities consider the filing of a US application to be the best proof of date of invention. Further, by the provision of a grace period of one year, a client receives the benefit of the *de facto* assumption that it took a year to develop the invention from its date of conception, prior to filing in the United States. Consequently, if the client files first in the United States, the US patent examiner can assert less prior art against them and, therefore, the client's US patent claims are likely to be broader than elsewhere in the world. In addition, if third-party competitors wish to defeat your client's US patents, the competitors must find prior art that is one year older than they would otherwise have to find had the client's first filings been a non-US filing. Alternatively (the downside), your client must find prior art that is one year older than a competitor's US filing date in order to defeat that competitor's US patent.

2. Fortunately, the European Patent Office and the patent offices of essentially all industrialized countries of the world consider a US patent filing a valid priority filing for their own purposes, thereby enabling the US priority filing to serve as a reservation of rights in these countries as of the US priority filing date. This means that, where filing in the United States is not barred on national security grounds (a very rare situation for all countries but France), a US filing provides all the priority benefits that a local filing can provide. Of course, the Paris Convention requirement that the regular filing be made within one year of the first filing still applies. In other words, a Swiss resident filing a US patent application first and later (within one year) a European patent application can claim priority to the US patent application and thereby fully preserve his or her rights in Europe, just as if the client had filed in Europe or the home-country first. As already noted, where the applicant is a French resident, France might not consider a first US filing by such an applicant as a valid filing because of French national law requiring that residents of France file first in France for national security purposes.[4] In addition, UK and German law forbids filing patent applications abroad for military technology developed by residents.[5] The United States has a similar requirement.[6] Fortunately, essentially all other industrialized nations allow their residents to choose where to file first.
3. US patent applications can be filed in any language. Only six months or perhaps a year or more after filing in the United States (within at most six months of receiving an official notice to do so) the application must be translated into English. This means that the client or applicant can gain the advantage of an early US filing, without having to translate the patent application into English. Consequently, a non-English US provisional patent application can be filed concurrently with a home-country filing, for a cost of an additional perhaps 500 euros over the costs of filing in the home country alone. Further, for those practitioners or clients who wish to file a PCT application in a language other than English, filing a priority US filing (in any language) is essentially the only way for the client to avoid the detriment of filing a non-English PCT application with respect to the client's US patent rights.[7] Where the client chooses to file a non-English-language PCT application, the English translation of the PCT need not be filed in the United States until at least several months after the filing date of a non-English US continuation application of the PCT, perhaps 36 months after the priority date. In this way, the patent attorney may be able to justify continuing to work in a non-English language in a manner that does not potentially damage the client's interests in the United States (subject of course to meeting the other requirements mentioned in, for example, point 6 below).
4. The filing fee for a US provisional application is $220, significantly lower than the filing fee in most other industrialized countries. For individuals or companies having less than 500 employees, the official filing costs and most future official fees are reduced by 50 per cent (so $110 for a US provisional filing).
5. Monetizing a patent is generally much easier in the United States than in other countries because the US legal system allows clients with valuable patent rights to negotiate a contingent fee agreement with even the largest law firms, thereby enabling them to enforce their rights without themselves taking on any

further litigation risk (ie the law firm takes on this risk). Depending on the perceived value of the patent, these firms will not charge for their time or expenses unless and until they win the case and a damage award is granted. In Europe, most countries (with the possible exception of the United Kingdom) do not allow lawyers to accept contingent fees, and so clients must pay their lawyers by the hour in Europe no matter how strong their case is. Large companies know this and so sometimes ignore the European patent rights of others until a suit is actually filed. Because of the advantages that a US patent offers in this regard, many large European research institutions and universities often file for patent protection only in the United States for certain technologies.

6. The United States has the most stringent filing requirements in terms of 'best mode', 'enabling disclosure' and completeness of the drawings, as well as the US duty to disclose.[8] Filing first in the United States using a patent firm that is thoroughly familiar with these filing requirements ensures that the patent application filed internationally will have fewer troubles during global prosecution (ie during substantive review by examiners in national or regional patent offices). Failure to respect these requirements may result in the US part of any PCT filing being held invalid in court, thereby depriving the company of patent rights it might otherwise have been able to use to barter away an infringement suit.[9]
7. Because the United States represents the largest domestic market for a broad range of products and services and because the likelihood is high that, if any patent in the client's portfolio is litigated, it will be litigated in the United States, the US market is arguably the most important single market for the client. Because of a homogenous consumer demographic, a single department store chain includes hundreds of outlets. Consequently, there are fewer but more significant targets in the event of litigation in the US than in Europe. This means that nationwide enforcement in the United States is typically less costly than transnational enforcement in Europe. In fact, based on anecdotal observations of the author, including discussions with Jeremy Lack, an international attorney experienced in IP mediation with Altenburger Attorneys in Zürich, the US patent can represent half, or perhaps 70 per cent, of the value of the client's entire patent family. Further, the size of the US market and the fact that a single patent covers this market mean that, on a per capita consumer basis, the United States is by far the least expensive jurisdiction in which to obtain patent protection.[10] A US patent typically costs less than half that of a European patent, for example. Further, renewal fees are due only every 3.5 years, not yearly as in Europe. This means that, if the US market is the most important one to the client and the client later decides not to file anywhere but in the United States, starting with the United States is the least costly option, one that avoids aborted non-US filings while preserving all options for the client.
8. English is the language of computer science, information technology, business and law, and the native language of many industrialized nations around the world, such as the United States, the United Kingdom, India, Ireland, Australia, Canada, New Zealand and Singapore. Further, Japan and Switzerland (to name just two) permit filing in English, subject to the submission of a translation at a later date. In addition, patent rights in Germany, Switzerland, France, the UK, the Netherlands, Denmark, Sweden, Luxembourg, Monaco, Slovenia,

Iceland, Latvia, Liechtenstein and Croatia can be protected via a later English-language European patent application, without further translation costs, thanks to the London Agreement.[11] Therefore a patent application drafted in English first can be prosecuted through grant in many important jurisdictions without translation and so, in addition to minimizing translation costs, is less likely to suffer from losses in meaning due to translation in these important regions.

9. An early US filing date means that the client's application won't be rejected by the US Patent Office under section 102(b) or (e) of the US Patent Law, when another party's US patent application has been published during the prosecution of the client's application, even though the non-US priority filing date of the other party is earlier than the client's US filing date. Conversely, if the client's priority filing is a US filing, then the publication of the client's application creates section 102(e) prior art against competitors.[12]
10. Provided clients do not file any foreign applications and request non-publication of the US application at the time of the US non-provisional filing, their US application is kept secret and is not published by the US Patent Office until it is granted. Therefore, clients who practise a secret process need not relinquish trade secret protection until they are convinced that the patent protection obtained in the United States will protect them more effectively than merely maintaining the secrecy of the technology. Preserving trade secret rights in this manner is simply not possible once a European, Japanese, Chinese or Korean patent application is filed.

Exceptions

Despite the above-enumerated advantages of filing in the United States first, as already mentioned, for companies whose markets are local and whose inventions have no real licensing value in the United States, advising the clients to file a patent application in their home country remains legitimate. Further, owing to national security laws, French residents must file in French in France first, using a French patent attorney. UK and German residents must file applications comprising military secrets in their respective countries first. In most other countries (including Switzerland, for example), clients are free to file first wherever they choose.

In addition, when publication or disclosure is imminent, and the inventor is not an English speaker, preparing an application in his or her mother tongue (say German) and filing in the most convenient location using an available home-country patent attorney in order to obtain the earliest filing date may mean that filing in the United States first or on the same day as the home-country filing is not possible. Fortunately, if the US application is filed soon after the priority filing, most of the advantage of early filing in the United States can be preserved.

Finally, if the client would like to receive a US patent quickly, the filing of a US provisional patent application (which is not reviewed substantively until a regular application is filed) can delay the ultimate issuance of the US patent. Therefore, this may be a factor in the client's decision not to file a US provisional application. In this case, the client should file a US non-provisional application (which will result in a search conducted by the US Patent Office) as soon as possible or file a

US provisional application along with a regular home-country application, paying the search fees and any fees for accelerated review in the home country, in order to get an early search report through the home-country patent office while at the same time securing an early US filing date.

Note that one reason sometimes given for not filing in the US first is that in the US the named applicant is the individual inventor and not the client company, and so if the inventor later becomes uncooperative, this could place a cloud on the title to any resulting patent. In fact, this is a problem with all patent filings, not just US filings, and so, this reasoning is not at all legitimate.[13]

Conclusions

If the risk manager wishes to minimize their client's litigation risk and maximize the potential scope of protection their client can obtain for their inventions as well as maximize their licensing value, and their client's invention and provided the client is not a resident of France (or, if residents of Germany or the UK, the inventions does not comprise sensitive military technology), then the risk manager should advise their client to file a patent application in the United States first or at least concurrently with or soon after a priority home-country filing. If the patent application covers a commercially valuable and patentable technology with applications in the United States, then ignoring these advantages may lead to increased litigation risk. Because most large European companies rely on their risk managers for such strategic information, the author hopes that European risk managers will do their part in educating their clients of these important particularities of US law. If this is done, the typical client will be in a better position to avoid needless litigation and will be able to augment the value of their patent portfolio while keeping related costs to a minimum. What's more, the typical European client will no longer operate at a disadvantage vis-à-vis their US-based competitors.

Notes

1. Where such a choice is permitted under national law, as discussed below.
2. Companies and institutions that, from the public record, do this include: IBM Rüschlikon, Logitech, the University of Geneva, HUG, the EPFL, and many large Swiss chemical and pharma companies, for example, to mention just a few.
3. When it comes to issues in US patent law dealing with proof of inventorship, which is a unique characteristic of US patent law vis-à-vis other countries, the equal treatment provisions of the Paris Convention do not apply.
4. See Article L. 612-9 of the Code de la Propriété Intellectuelle français. However, this requirement is considered by many to be invalid under GATT TRIPS, an international trade agreement.

5. German law forbids filing German state secrets abroad. German state secrets are defined as facts and knowledge accessible to a limited number of people whose revelation would damage the external security of the German nation, section 93 Nr. 1 Strafgesetzbuch (StGB) (Ger), translated in Joseph J. Darby (1977) *The Penal Code of the Federal Republic of Germany*, p 118, F B Rothman, South Hackensack, NJ. Therefore, this covers almost all military-related inventions the details of which are known by only a few. As for the UK, filing applications abroad on military technology, or technologies that could harm national security or public safety, is prohibited under section 23 of the UK Patents Act.
6. Where a co-inventor is a US resident, a foreign filing licence must be obtained from the US Patent and Trademark Office (USPTO) before filing abroad.
7. See 35 USC section 102(e).
8. See Title 35 USC section 112, first and second paragraphs for requirements for support ('best mode') and enabling disclosure, and 37 CFR section 1.83(a) for drawing requirements ('drawing in a nonprovisional application must show every feature of the invention specified in the claims'). The 'best mode' requirement is a safeguard against the desire on the part of some people to obtain patent protection without making a full disclosure as required by the statute. The requirement does not permit inventors to disclose only what they know to be their second-best embodiment, while retaining the best for themselves. *In re Nelson*, 280 F.2d 172, 126 USPQ 242 (CCPA 1960). The duty to disclose ('duty of candor') is a statutory obligation that seeks to ensure that stiff penalties may be assessed against those who wilfully withhold known prior art in hopes that the patent examiner will not find it and thus accord the client a broader (albeit invalid) patent.
9. PCT requirements deal primarily with formal matters. Therefore the PCT examiner is not charged with reviewing an application to determine whether it meets US standards. Consequently, the applicant is solely responsible for ensuring that such requirements are met.
10. The licensing value of a US patent is therefore probably much greater than any other national patent.
11. See http://www.epo.org/topics/issues/london-agreement.html for further information.
12. See above.
13. Fortunately, the risk of a struggle with an uncooperative inventor can be minimized by ensuring that the inventor has signed a contract agreeing to assign the rights in the invention to the client company, and the inventor is denied access to the serial number of the priority filing until after any patent application has been officially published by a patent office (usually 18 months after the first filing). For employees, risks can be eliminated by ensuring that each employee signed an employment agreement that clearly gives the employer exclusive rights in the employee's inventions. Finally, country law may give ownership in inventions of an employee to the employer by statute, thereby obviating the need for employment contracts in order to secure ownership in an employee's inventions under certain circumstances (such is the case in Switzerland).

5.3

Mitigating risk when managing intellectual property in the United States

Helene Vik, Ipendo Inc

Introduction

The United States is undeniably one of the most desirable markets to access, but protecting intellectual property (IP) rights in the United States involves risk and considerable financial commitment. Counterfeiting, and patent and trademark infringement are costly, and the constantly changing regulatory environment only makes matters worse. With new intellectual property rulings, increasing administrative burdens by the US Patent and Trademark Office, and cumbersome reporting standards, companies need to stay informed and be prepared to handle the changes and risks. However, along with risks come great rewards, as the United States offers one of the world's largest marketplaces. Now more than ever it is vital for business managers to take an active part in IP management and plan a strategy that

- Are you in control of your Intellectual Property Data? Documents? Costs?
- Is your company working with several law firms?
- Are you relying on outside counsels' databases?
- Do you have a good overview of your IP portfolio?
- Are the IP processes efficiently controlled by your company?
- Does your company have a safe and secure IP Management System (IPMS) in place?

What Companies Must Do to Reduce Cost and Risks in Intellectual Property Management

- Gain control and transparency of your IP portfolio and workflows by deploying an IP Management System
- Reduce risk and cost by automating IP workflows
- Don't rely solely on outside counsels' databases; gain independence!

About Ipendo

IPENDO is a leading provider of a web-based IP Management solution, The Ipendo Platform™. It is a unique, user-friendly and vendor-neutral software, integrating the management of all types of IP rights. IPENDO was founded in Sweden in 2004 by IP and IT professionals who saw a need for an IP management system designed for companies' specific needs and workflows.

The Ipendo Platform™ is a solution enabling online collaboration and service exchange with outside counsels, agents, partners and PTOs. IPENDO streamlines and automates the IP workflows helping companies improve their portfolio management techniques and reduce risk while cutting legal and administrative costs. IPENDO customers save an average of 20-30% on their patent annuities and trademark renewals, EP validations and PCT filings when deploying the Ipendo Platform™.

The Ipendo Platform™ is an ideal toolbox for key decision-makers to gain the transparency and control they need with easy access to IP budgets, cost analysis, IP statistics and due diligence. The build-in country law database automatically gives advanced notice of important due dates. The Ipendo Platform™ is a powerful system, yet flexible and easy to use and customize. It supports all IP related workflows including Invention Submissions, Contract Management, Prosecution, Licensing, and Maintenance of IP rights.

minimizes corporate risk. This chapter will address mitigating strategies as they relate to IP management in general and to the US market in particular.

Let's face it: maintaining and managing intellectual property rights (patents, design patents, trademarks, trade secrets, copyrights and domain names) is both an art and a science, both expensive and time-consuming. However, an IP portfolio is a strategic investment for a business. It provides an entry barrier to a field or technology; it can block the launch of a product by a competitor and, in short, secures a competitive advantage for your company. As with any investment, the ultimate purpose is to build value for your company. For IP, however, the expense is incurred immediately and the return on the investment takes time. The ability to protect the market doesn't always show on the balance sheet, but it may be of critical importance to the company's ultimate survival. As risk and returns go hand in hand, the higher the returns, the higher the risk.

Intellectual property – part of the business strategy

Organizations often lack a complete overview of their IP portfolio and the competitive patent landscape, despite the fact that these considerations are an essential part of a winning business strategy. Since IP rights are strategic assets, they should be managed accordingly. Every department from marketing and finance to business development and operations should understand the scope of the company's IP rights. Traditionally, businesses have made IP decisions solely through their legal department rather than interdepartmentally in a transparent, cross-functional partnership. Owing to a limited and isolated strategy, important business opportunities are often overlooked. As the global marketplace becomes increasingly competitive, companies must recognize the risk of not having a strategic overview and management process in place for their intellectual assets.

Based on experience in working with companies that have IP, I have noticed that successful IP management incorporates a strong partnership with its outside counsel and cross-functional team members from the R&D, marketing, business development, management, financial and legal departments. Organizations that have a clear understanding of their IP portfolio and the competitive market environment are better prepared to handle IP risks. They are also better equipped to recognize and seize business opportunities. A successful business strategy aligns market needs and opportunities with a company's capabilities and IP protection.

Building an IP portfolio – geography and industry's IP intensity

The intellectual property environment varies between industries and technologies. Patent protection may be the most common IP type within certain industries, while trademarks may dominate other industries. If reverse engineering is possible, you

should seek patent protection. If it's not easy to counterfeit, such as food and chemistry, trade secrets may be an option. Possibilities are left for changing the trends in other fields where patents or trademarks have not been utilized. However, investing in keeping your trade secret a 'secret' needs to be a priority. You need to have secure processes and procedures in place for keeping your trade secret safe.

It is advisable to evaluate different protection strategies supporting your business model. In some industries or technology fields, being creative and using non-traditional IP protection may be a good strategy. Brand- and trademark-intensive companies commonly neglect patent and design protection, while patent-intensive industries are generally weak on trademarks. Although your technology may be similar to your competitors', by utilizing brand protection and brand enforcement your company can benefit from market recognition and increased sales.

It is important to understand each country's marketplace, competition and legal environment. Every country's jurisdiction offers alternatives for cost-effective strategies for minimizing risks and creating 'freedom to operate' for your company and customers. Generally, there is no need to protect each and every jurisdiction as long as you are blocking your competition in your most important markets. However, the global marketplace is shifting; therefore your IP strategy needs to be proactive and anticipate emerging markets. Always use your overall business strategy to determine which countries to enter, but keep in mind the realities of IP enforcement in a particular jurisdiction.

For example, if we look at the automotive industry, by obtaining IP protection in Japan, the United States, Germany and Brazil, you will probably block competition in your most relevant markets for your company's car and truck manufacturing today. Yet current global trends show that China, Canada, India and Korea have large emerging automotive markets that may rival the current automotive leaders. Therefore it may be important to seek protection in these jurisdictions to protect the future of your company.

Owning IP does not mean you have the right to commercially produce, use or sell your product, since it may infringe upon third-party intellectual property rights. Therefore, it's advisable for businesses to conduct a freedom-to-operate analysis or a patent landscape analysis to identify third-party patents that may affect development of your product. This research may help your company navigate through the patent landscape to avoid claims of infringement, identify licences needed and prevent spending on R&D that is unable to materialize into a viable product because of the IP rights of a competitor.

Risk assessment of IP operations

Inefficient IP operations affect the bottom line and, most importantly, the strategic management of the IP. When maintaining an IP portfolio, it's common to work with several law firms in different countries, have multiple licensing agreements and track maintenance fees and due dates with different patent offices. In addition, the administrative burden is escalating in the intellectual property field. The US Patent and Trademark Office has repeatedly increased the requirements on infor-

mation needed from applicants. For example, it is the applicant's responsibility to provide information disclosure statements (IDS), prior art, inventors' previous patents, etc. The list of requirements keeps growing, and your company needs to stay informed on the changes that may affect your business and have a response strategy that can be rapidly implemented.

Many organizations have yet to implement IP management software (IPMS) and still keep track of their IP in Excel spreadsheets or use cumbersome, non-user-friendly docketing databases. Not having an IPMS makes it difficult to work efficiently and will not provide the structured overview of your IP portfolio that is required when making informed decisions. Furthermore, IP managers and administrators are often overwhelmed owing to the lack of control of the portfolio. IP reports that make sense for other business functions are not being produced because of the absence of complete reporting capabilities, and the top management team is often unaware of these inefficiencies. Many organizations are simply not in control of their IP portfolio and are relying solely on their outside counsel's internal systems.

Case study: How proactive measures lead to strategic success and risk reduction – the case of the small high-tech company taking control of its IP portfolio

In the spring of 2009, a small US company in the high-tech industry decided to take control of its IP portfolio by implementing an IPMS. The portfolio was small, less than 50 patents; nevertheless, the strategic control was, for the company, a top priority. The company worked very closely with its outside counsel, an attorney at a well-known reputable US IP law firm. The company asked the attorney to use its new IPMS as a means of communication. By having the attorney upload all documents, correspondence and important due dates, the company saved time and, more importantly, achieved transparency in the prosecution process. Management reports were within easy access, and strategic information could be retrieved with one click, on the spot, during strategic planning meetings.

With this valuable information the company decided to deploy an aggressive patent filing strategy. Six months later, the company reached a critical stage in its patent prosecution. At the time, its outside counsel changed law firms. Normally, a change of firm would take time and it would be a cumbersome process retrieving IP case data and files, as well as important due dates. Since the company had been proactive and had an IPMS in place, it only had to update the new contact information for the attorney in the IPMS. Seamlessly, the company could continue with its important patent prosecution.

Litigation – an extended licensing tool

Licensing out technology may be a gold mine for returns on intellectual property investment. Nevertheless, successful licensing may take years to achieve and may be an area of great risk if not managed properly. IP owners need to be prepared to convince the external environment that they can protect their IP and withstand litigation. In some industries and countries there are underlying rules on 'when' or 'if' to litigate. Breaking those rules can create market confusion. Therefore companies need to study the specific market situation before making a decision to litigate. It is interesting to note that patent 'litigation' or the 'threat of litigation' is often considered a necessary licensing tool in the United States, and viewed as an extended licence negotiation and means for a company to evaluate its patents. The process can be expensive but is viewed as an investment in the IP portfolio, as it can add value to the IP.

Proactive measures are advisable, and companies should look at their IP investment at the early stages and plan their licensing strategy. Successful licensing agreements are 'win-win' arrangements for both the licensor and the licensee. Nevertheless, disagreement over royalty payments is among the most common reasons for IP lawsuits, so be practical and anticipate what is going to be asked from you.

Here are some areas to keep in mind to reduce risk in the licensing field:

- A 'grant' clause is the most important section in a licensing agreement. This section describes the business arrangement, ie 'who gets what'. State the IP rights clearly, eg the patent number, to avoid any misunderstandings on what the licensee is licensing. Focus on the grant clause and create a 'win-win' contract for the licensing parties.
- Remember that there is only one legal entity that can sign a licensing agreement. Which part of a large corporation should get the licence? What about subsidiaries? Make sure the licence can be transferable and put that into the agreement; otherwise you will need a written consent, and that can be costly.

It is a common misconception that the majority of patent infringements end up in court. That is not the case. In fact, patent infringement litigation is mainly on paper, and going to court is usually a last resort. Between 1997 and 2006, only 4 per cent of all US patent litigation cases went to trial. In recent years, however, there has been an increased activity by 'patent trolls', ie non-producing entities whose sole purpose is to exploit patent licensing fees from target companies. Companies have to manage this risk accordingly and respond to litigation warning letters and demands from patent trolls.

US changing legal and regulatory environment

The US patent system is changing, and there are a number of proposed rulings pending, including patent law reform legislation awaiting decision by the US Congress. In addition, some recent patent case rulings have been given a lot of attention, as they are changing the IP environment. The KSR case regarding patent

obviousness and the Bilski case are examples. The Bilski case regarding patentability of business methods is of concern since the Supreme Court may decide to void business method patents, a result that will erase the intellectual property rights of many patent holders. This decision could have a tremendous impact on the patent system and certain industries.

In addition, selecting the right venue for IP trials can be of importance for litigation. It is vital to stay informed of the changing US regulations, as they may affect your business and industry. Companies should work closely with attorneys who are knowledgeable about intellectual property rulings in the United States.

Insurance for intellectual property

Because intellectual property issues can be a huge liability, insurance coverage can be obtained. Specific IP insurance may be necessary if the field of your company is IP intensive. IP insurance can be used for different purposes: 1) offensive: providing support to litigate in an offensive manner and defend your own IP rights when you suspect others may have infringed upon them; and 2) defensive: defending your company against external attacks when being sued for infringing upon others' IP rights.

What businesses must do – best-practice approach to IP risk avoidance

Mitigating internal risk

1. Streamline IP operations so that they are cost efficient and less time-consuming, enabling 'proactive' rather than 'reactive' management.
2. Gain a holistic overview of your portfolio and map the portfolio on your business strategy (eg connect your IP to products, technology areas, competition and so forth).
3. IP due diligence: keep your IP records and database updated, including patent ownership and inventorship, and know what IP your company owns rather than licenses. Always keep inventors' addresses current and keep a record of maintenance fees paid. Missing IP records and out-of-date addresses are factors that can impede a business transaction – such as a merger and acquisition.
4. Re-evaluate the intellectual property portfolio. What is the cost versus benefit of maintaining each patent family? A review of the entire portfolio should involve organizational departments such as R&D, marketing and finance, in addition to the legal department and outside counsel.
   - How does the patent family relate to the current business strategy and objectives?
   - What IP is protecting 'core technology' as against non-core technology?
   - What is the return on investment of maintaining the IP portfolio? Forecast the budgets for maintenance, eg the official fees, renewal fees (annuities) and other legal fees.

- Consider monetizing on non-core technology, licensing or selling IP.
- Is research and development conducting research in the relevant subject matter?

Mitigating external risk

1. Understand the external environment – how IP works in your industry and the countries of your market. Is it common with litigation, or cross-licensing, and are there patents in this industry?
2. Freedom to operate: obtain independent studies from various law firms to make sure your company has the freedom to operate.
3. Monitor the marketplace to detect any infringements or misuse of licences.
4. Work closely with the United States. Counsel should focus on strategic issues and insights in the shifting legal environment. Reduce fees associated with employing outside counsel by managing the workflow efficiently, discarding tasks that are non-strategic, and employing online collaboration and direct reporting in your IP management software.
5. Insurance: consider obtaining IP insurance in the United States.
6. Patent trolls are on the rise in the United States, and it's common to receive warning letters. Know when threats are real or fake by being prepared to defend your IP and by knowing your IP portfolio. Have all prior art documents in order and monitor your industry's patent landscape.
   - What does your IP protection cover? For example, what products and parts of the products are the IP rights protecting?
   - Patent mapping: core technologies versus non-core technologies.
   - Which competitor is the IP blocking?

Conclusion

Companies need to be in control of the operational management of intellectual property and integrate it with the business strategy. The IP portfolio should be managed like any other strategic asset and evaluated on a regular basis by a cross-functional team.

Figure 5.3.1 A successful IP risk assessment process contains both analysis from the internal perspective (IP operational processes, IP coverage, etc) and analysis of the external environment (eg benchmarking your portfolio against your competitors', understanding the IP landscape)

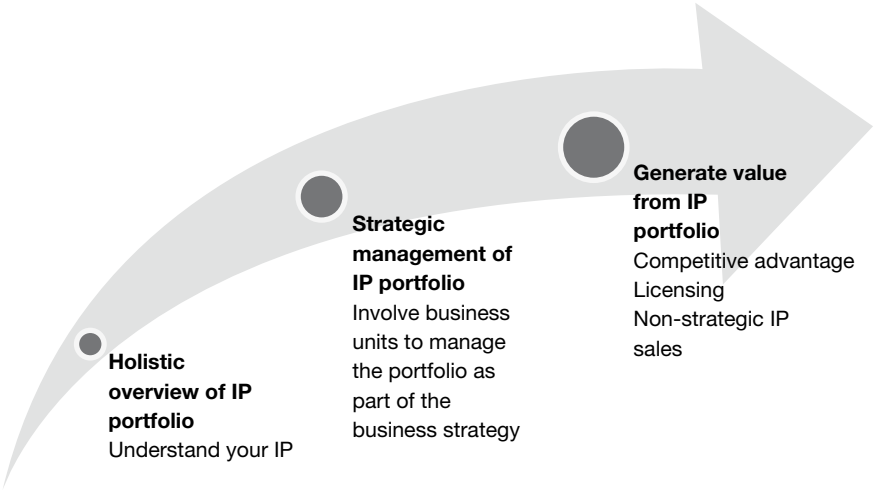


Figure 5.3.2 Companies need first to gain a holistic overview of the IP portfolio and manage IP as a strategic asset in order to maximize IP value

An uncomplicated IP management system should be in place to use as a tool for control and ROI analysis. Companies can reduce risk and cost by using a proactive approach and having all necessary IP information accessible.

References

United States Patent and Trademark Office, www.uspto.gov
American Intellectual Property Law Association, www.aipla.org

5.4

The European patent system

Marco Serravalle, Serravalle sas

In 1978 a new era began for patents in Europe. On 1 June 1978 it became possible to file a single patent application, which, after a centralized search and examination process, would become a national patent in a number of member countries of the European Patent Convention (EPC).

In 31 years, the growth of the European Patent Office (EPO) has been spectacular. If we compare 1997 with 2007, we can see that the number of EP filings (either direct or through the PCT treaty) doubled from 72,000 to 140,000. In the same period, the number of national filings in the UK remained stable at about 12,000 a year.

Nowadays, it is a common practice for most companies to seek protection for their inventions in Europe through the EPO. It is therefore useful to have a look at the most important aspects of the EPC, especially in the light of the changes introduced with the new revision (EPC 2000).

The PCT route

Another major change in the international approach to patents has been the enormous success of the Patent Cooperation Treaty (PCT) system. A PCT application repre-

sents a centralized process for an international application and delays the decision of which states to cover with the application for up to 30 months from the priority date. It represents a delay of 18 months over the alternative classical route, filing of a priority and extension of the patent within 12 months from the priority date.

The PCT route allows the filing of a single application, which keeps the way open for more than 100 countries where it will be possible to obtain a patent, postponing the decision of where to file the patent to the 30th month from the priority date. This result is obtained by paying about €5,000, which is an average cost for filing a PCT application.

In 1987 about 8,000 PCT applications were filed worldwide, rising to 50,000 in 1997 and to about 150,000 in 2007. Thus, it is a very common practice nowadays to obtain protection for inventions from a PCT application, which enters its European phase with the EPO.

How to obtain a patent

Most applicants choose the PCT for international filing and obtain a European patent starting from a PCT application. However, it is not advisable to file the PCT application directly. It is more convenient to file a priority application and then, after 12 months, the PCT application. There are two main reasons. First, a patent lasts 20 years from filing; thus the priority application will expire 12 months before the PCT application. Second, annual fees are paid counting from the date of filing. Thus, if we file the priority on 3 June 2010 and the PCT application on 2 June 2011, we will have to pay the third annuity for the priority filing in June 2012, but for the application that originates from the PCT only in June 2013.

There are two possible options for the priority filing. Traditionally, the first option is that applicants file the priority document with the national patent office. However, the second option is to file an application with the EPO, after filing and receiving an authorization from the national office. My advice is to file a priority with the EPO, since this produces two advantages: the extended European search report about five months after filing, and the reimbursement of the search fee when filing the PCT application.

The extended European search report corresponds to the traditional search report, plus the first communication that the EPO will issue when starting the examination. This service provided by the EPO is very interesting, since in this way the applicant is already fully aware of the future objection five months after the priority date.

The different steps to obtain a patent

Let us imagine the different steps for a new invention to acquire a national patent in several countries. As we did before, let us imagine filing a priority application at the EPO on 3 June 2010. In November, we will probably receive the extended European search report, which will inform us of the most relevant prior art and will

formulate the novelty and inventive step objections that the examiner will move if we do not amend the application. Based on this extended search report, we will decide whether to continue and, supposing we do decide to file a PCT application, we will file it close to the deadline of 3 June 2011, say on 2 June 2011.

After two to three months, the EPO will issue the PCT examination report and written opinion. If we have not amended the application, they will be identical to the extended search report of the priority filing, and we will receive, within a few months, the reimbursement of the EPO search fee.

From 1 April 2010, it will be compulsory to reply to the written opinion, whereas reply was optional before that date. After 30 months (or 31 months for most countries) it becomes necessary to enter the national (or regional in the case of organizations like the EPO) phases to obtain national patents.

For each country there are different rules. I will just outline the EPO procedure, which is probably the most interesting for us.

New EPO rules

After a certain time (from a few months to a few years) the EPO will issue an examination report to which the proprietor, possibly through his or her agent, will have to reply.

Until now, the EPO policy has been very client friendly. This was partly attributable to historical factors, since the EPO faced very strong competition from national offices in the early years of its existence. Nowadays, the EPO probably feels more confident about its position and has adopted more severe rules for applicants. These rules are intended to reduce the time required for examination without decreasing the stringency of the examination.

A first important change relates to divisional application. A divisional application is an application having an identical description but different claims when compared with the originally filed (parent) application. It might derive from an objection of lack of unity of the examining division. At present, it is possible to file a divisional application if the parent application is still pending, in effect up to the day before publication of grant. From 1 April 2010, it will be possible to file a divisional application within 24 months from the first non-unity objection from the examining division.

Another important change concerns the possibility of amending the application. The EPC contains a rule stating that only the first amendment can be made by the applicant of its own volition; however, I do not remember any case where an examiner refused to accept amendments. Recently, I have received a first communication stating that ‘the Division will only give its consent to one further set of claims’. This probably indicates that EPO examiners will tend to limit their official communications in the near future, aiming at a grant or refusal ruling with a more limited number of official communications.

When the examining division is satisfied with the amendments or arguments submitted, it will issue a communication informing the applicant of the intention to grant the patent on the basis of a text.

The applicant will have to provide the translation of claims into the two other official languages (French and German if the application is in English) and pay the proper fees within four months. Then the applicant will be notified of the date of grant of the patent. Within three months from that date, the applicant will have to take the necessary steps in order to validate the patent in the selected countries.

The London Agreement

An important step in the direction of reducing the cost of a European patent was the coming into force of the London Agreement. At present, the agreement has been signed by 15 countries: Croatia, Denmark, France, Germany, Iceland, Latvia, Liechtenstein, Lithuania, Luxembourg, Monaco, the Netherlands, Slovenia, Sweden, Switzerland and the United Kingdom.

The agreement aims at reducing the costs relating to the translation of European patents. The consequence is that, in those countries, there is no need to file a translation if the patents have as an official language one of English, French or German; otherwise, only the translation of the claims has to be filed.

Opposition to a granted European patent

Within nine months from publication of the mention of the grant of the European patent, any third party can file opposition to that patent. The opposition can be based on the following grounds:

1. The patent lacks novelty or an inventive step in view of the prior art.
2. The patent does not disclose the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art.
3. The patent contains subject matter that extends beyond the content of the application as filed.

Statistically, a third of the oppositions terminate with revocation of the patent, a third with the patent being upheld and a third with the patent being maintained in amended form. The decision of the Opposition Division can be appealed by any party negatively affected by the decision.

With the last revision of the EPC (EPC 2000), the possibility has been introduced for the proprietor of the patent to limit its patent by an amendment of the claims. In the early years of the EPO it was considered possible for a proprietor to oppose its own patent. In fact, the EPC states that ‘any person’ can oppose a patent. However, this statement was interpreted as excluding the proprietor in 1994. Thus, it became impossible for a proprietor who became aware of a document invalidating its patent to limit the claim in order to re-establish patentability of the patent. The new provision of the EPC takes into account this need and introduces the possibility of a proprietor requesting limitation of its patent.

The decision of the Opposition Division and eventually of the Board of Appeal and the results of the limitation proceedings are effective in all countries where the patent was validated. If the patent had been obtained by the traditional national route, it would have been necessary to start court proceedings in each state to revoke the patent or limit it.

Thus, opposition to a European patent represents a much cheaper option than court proceedings. It has to be noted that, in the case of maintenance of the patent by the EPO, it is still possible to start national revocation proceedings.

The judicial system remains the only aspect that has been fully maintained at a national level. However, there is a considerable movement towards the creation of a European patent court comprising a court of first instance, with a central division and a number of regional divisions, and a court of appeal, with jurisdiction to deal with infringement and revocation actions concerning European patents. The creation of a European patent court would represent the completion of the European patent system started with the formation of the EPO.

Conclusions

I think that the growth of the EPO has been an important unifying factor for patent law in Europe and a very positive element. Of course, as with every large body, there are areas for improvement in the EPO's way of working, but the story of the EPO shows that, when Europe acts as a single player, it can have a very important role in the world. The EPO has been able to influence patent policy even in the United States, which traditionally has a very different approach, but is more and more willing to harmonize with Europe and the other industrialized countries.

5.5

Patent infringement and damage claims – a new era in Europe in terms of business risks

Armin K Bohmann, bohmann || bohmann (Bohmann & Loosen)

From both the number of patent filings and an increased number of disputes on patent-related matters, it is obvious that companies focus on intellectual property rights these days more than ever. One reason is that competition has been and still is becoming fiercer than ever since the beginning of the information age. Basic and even advanced technical skills are widely available and no longer limited to established economies. Therefore, companies try to resort to intellectual property rights so as to protect their own technological assets and their markets. Patents link the industrial age to the information age.

However, seeking for and obtaining patent protection is only the first step. The second step is enforcing the rights conferred by patents. Particularly in times when

bohmann | bohmann

When IP matters…

European Patent and Trade Mark Attorneys
German Patent and Trade Mark Attorneys

in the capital of European IP law

bohmann| bohmann
Nymphenburger Str. 1
80335 Munich
Germany

www.bohmann-law.com contact@bohmann-law.com

budgets are tighter than usual, companies tend to enforce their patent rights. Enforcement of patent rights in Europe, however, has to take into consideration the particularities of Europe.

Obtaining patent protection in Europe

Basically, various ways exist to gain patent protection in Europe. Apart from national patent applications, the patent system under the European Patent Convention (EPC) is available for regional protection. However, the term 'European patent' might be misleading to a certain extent, as it gives the impression that, as with national patents such as, for example, US patents or German patents, an office grants a patent for a given jurisdiction and the granted patent thus is, as such, enforceable in the said jurisdiction. This, however, is not the case with European patents.

European patents are granted by the European Patent Office, and the procedures before the European Patent Office are governed by the provisions of the EPC. Once a European patent has been granted, it splits into national parts, which constitute independent and separate national patent rights conferring the same rights as national patents granted by the respective national patent authorities. Such national patent rights are enforceable in accordance with the national provisions, and the claims and their scope of protection are interpreted by national infringement courts rather than by a European infringement court. The concept of a truly European patent, which is granted by the European Patent Office and is enforceable effectively all over Europe by the decision of a single European infringement court, is basically that of the Community patent, which, however, has not yet been put into practice.

However, the EPC makes it very clear that a European patent will, in each of the contracting states for which it is granted, have the effect of and be subject to the same conditions as a national patent granted by that state. In other words, whichever route is chosen to get patent protection in a European country, the effects arising from such a patent are the same.

Claim interpretation under the national laws governing the national parts of a European patent

As outlined above, claim interpretation for deciding whether or not an embodiment is actually falling within the scope of protection of a claim is governed by national law, more specifically by the national law governing the national part of a European patent. Accordingly, for example for the German national part of a European patent, German national law is applicable in deciding on whether or not an embodiment is infringing the German national part.

Despite harmonization efforts, such as Article 69 EPC and the Protocol on the Interpretation of Article 69 EPC, to date no legal provision exists that would be

binding in this respect and would provide the courts dealing with patent infringement matters with a clear guideline on how to interpret the claims of a European patent. Part of the underlying problem might be that the contracting states of the EPC are not identical to the European Union and that the EPC has not been created by the European legislator, ie the European Parliament. Therefore, the mutual understanding of the national courts and judges dealing with patent infringement matters and their willingness to provide for a unitary and consistent interpretation of the claims of a European patent are setting the pace, which should ultimately allow a person to know what is covered by a European patent.

Given the long-lasting traditions on claim interpretation in at least some European jurisdictions and albeit there are the above harmonization tendencies, there remain significant differences in the interpretation of the claims of a European patent, which have to be taken into consideration and which inherently create a momentum of uncertainty as to whether a product or process is actually covered by a patent. Because of this, doing business in Europe is still something of a legal patchwork task when it comes to patents and assessing their effects in terms of coverage.

Rights conferred by a patent in Europe

As is evident from the above, the national legislator and the national courts define the scope of protection and harmonization in terms of a single country jurisdiction, and consistent interpretation of the scope of protection conferred by a European patent may still take years, not to say decades. However, as to the rights conferred by patents in Europe and the enforcement of such patents, significant progress has been made recently by the European legislator.

One might take it for granted that the rights conferred by a patent in Europe are well defined and actually enforceable, for example by filing a patent infringement action or a request for a preliminary injunction. However, this is not necessarily the case, as major economic and thus also legal activities in Europe are no longer concentrated in the big and traditional economic powerhouses such as the United Kingdom, Germany and France, with their long-standing traditions in both the granting and the enforcing of patents. Rather to the contrary, the European Union, in its efforts to create similar, not to say uniform, living conditions and living standards in its territory, heavily subsidizes the creation of new industries and jobs in the hitherto less powerful economies. However, the lack of legal means to enforce IP rights such as patents in at least some of these economies could jeopardize this goal.

Consequently, the European legislator has prepared Directive 2004/48/EC on the enforcement of intellectual property rights. Owing to its legal character, this directive had to be implemented by the national legislators by 29 April 2006, rather than immediately being binding national law as in the case of an EC regulation. For the time being, not all of the national legislators seem to have enacted the directive and, despite a desire to provide for a uniform legal basis in the internal European Market, the way those national legislators who enacted the directive

have done this is, at the least, somewhat divergent. This is not at all surprising and was clearly anticipated by most legal practitioners, who would have felt more comfortable with an EC regulation.

Basic considerations of Directive 2004/48/EC

The directive requires all member states of the EC to apply effective, dissuasive and proportionate remedies and penalties against an infringer of IP rights including patents. As a matter of fact, the measures foreseen by the directive are a minimum standard and do not preclude the national legislator from implementing an even more stringent legal system for the enforcement of patents.

According to the directive, a patent holder may actually apply for evidence regarding an infringement that lies in the hands of the other party to be presented. Basically, the only prerequisite for such an application is that the applying party presents 'reasonably available evidence sufficient to support its claim' to the courts. In the case of an infringement committed on a commercial scale the judicial authorities may order, on application of a party, the communication of banking, financial or commercial documents under the control of the alleged infringer, subject to the protection of confidential information. Measures for preserving evidence include effective provisional measures including the detailed description, with or without the taking of samples, or the physical seizure of the infringing goods and, in appropriate cases, the materials and implements used in the production and/or distribution of these goods and the documents relating thereto.

The above is only a short outline of the measures available for patentees or their licensees to enforce their patent rights. As a matter of fact, all parties involved, ie patentees, alleged infringers and the courts, are still on a learning curve as to the applicability of these extremely powerful means. For one thing is certain: the European Union is not a place to ignore IP rights such as patents.

The access to any factual information of an alleged infringer puts any patentee in a very powerful position. Similarly to the discovery proceedings in the United States, all aspects of a patent infringement can be uncovered. Two aspects thereof might be of particular importance to the management of companies. First, a patentee, who is usually also a competitor to the alleged infringer, gets to know the costs of goods and the profit margin of the alleged infringer; second, the patentee also gets to know the internal decision-making process as to the infringing product. (The same, of course, applies to patent-protected methods.)

Knowing the costs of goods and the profit margin, respectively, of a competitor is definitively advantageous. In cases where the competitor is the infringer of a proprietary patent, the damage claims can now be more accurately calculated. This may put the infringer in a delicate position; in a case where there is a significant price difference between the product of the patentee and that of the infringer, such as in a dispute between a pharmaceutical company and a generic production company, the patentee may base its damage claims on the method of calculation most favourable to it, typically its loss of profit. This can easily result in a scenario

where the infringer actually has to pay more to the patentee than its profit gained from the patent infringement activity.

Knowing the internal decision-making process may also yield an interesting insight into the organization of a competitor. From a patent attorney's point of view, this might also be enlightening in so far as one may determine whether or not the management can be found guilty of wilful patent infringement. Wilful patent infringement is no longer regarded in the EC as a peccadillo, but a crime that may be prosecuted under the criminal law.

Summary

In Europe, national patents and European patents still coexist, basically conferring the same rights to the patentee in a member state of the EC. However, the interpretation of patent claims is not yet harmonized, providing a sometimes fragmented European picture of the effect of such patents. Directive 2004/48/EC on the enforcement of intellectual property rights now provides a basic uniform legal system for the enforcement of IP rights including patents. This basic uniform legal system allows, among other advantages, immediate access to an infringer's banking, financial and commercial documents. Based on such documents, a damage claim can be optimized.

5.6

Strategies for coordinating acceleration of international patent prosecution

Andrea Schüssler, Huber & Schüssler

In the early 1980s, faced with an increase in the number of filings, the Trilateral Offices (US Patent and Trademark Office, USPTO; European Patent Office, EPO; and Japanese Patent Office, JPO) devised specific measures tailored to manage the increasing workload. Each office implemented new technologies to economically store, efficiently process and rapidly distribute very large amounts of data. In particular, the Trilateral Offices started to cooperate by exchanging know-how and establishing standards for exchanging data files. In addition, the USPTO established a 21st Century Strategic Plan to transform the USPTO into a more productive organization.

Creating new ideas is your business.

Protecting these ideas is ours.

HUBER & SCHÜSSLER provides highly qualified expertise in handling intellectual property. Our Attorneys have the technical and legal expertise to protect, license and enforce your patents, trademarks, utility models, designs and copyrights.
We are specialized in all relevant fields of life sciences, pharma, biotechnology and medical devices.

HUBER & SCHÜSSLER
patentanwälte · patent attorneys

Huber & Schüssler, Truderinger Str. 246, 81825 Munich/Germany | phone:*49.89.437788-0 | fax:*49.89.437788-99
eMail: info@patservice.de | www.patservice.de

Patent Prosecution Highway

One of the specific action items of the 21st Century Strategic Plan was the implementation of the Patent Prosecution Highway (PPH), which should help to accelerate patent grants and coordinate global patent strategy. It is well known that, in the Trilateral Offices, which process the greater part of all patent applications filed worldwide, including PCT applications, the number of pending examination cases has increased to more than 2 million. This has caused a dramatic backlog of work, and it is not unusual for patents to be granted only after pendency of five years or longer. By using searches that have been conducted by the other patent offices and by taking advantage of the initial examination process of the other patent offices, the PPH aims to make the overall process in each of the participating patent offices more efficient. In other words, the PPH was established to enable an applicant whose claims are determined to be patentable/allowable in the office of first filing (OFF) to have the corresponding application filed in the office of second filing (OSF) advanced out of turn for examination while at the same time allowing the OSF to exploit the work results of the OFF.

From July 2006 to January 2008 the USPTO partnered with the JPO to establish the first pilot PPH, and from January 2008 to January 2009 the USPTO partnered with the Korean Patent Office (KIPO) to establish a further pilot PPH. Since the trial phases had a positive outcome, the respective offices recently began to fully implement the PPH programme into their patent systems.

In the meantime, the USPTO has also commenced separate PPH pilot programmes with the United Kingdom Intellectual Property Office (UK IPO), the Canadian Intellectual Property Office (CIPO), IP Australia (IPAU), the Danish Patent and Trademark Office (DKPTO), the European Patent Office (EPO), the Intellectual Property Office of Singapore (IPOS), the German Patent and Trademark Office (GPTO) and most recently the National Board of Patents and Registration of Finland (NBPR). These PPH pilot programmes are based on the same, or a similar, framework as the first PPH between the USPTO and JPO. PPH programmes also exist between several other countries. The KIPO, GPTO, UK IPO, IPOS, NBPR and DKPTO have the PPH relationship not only with the USPTO but also with the JPO. In addition, the JPO has implemented pilot PPH programmes with the Austrian Patent Office (APO), the Hungarian Patent Office (HPO) and the Russian Federal Service for Intellectual Property, Patents and Trademarks (Rospatent). There has also been a PPH relationship between the DKPTO and the KIPO since March 2009. This area of coordinating patent examination among several countries is changing rapidly as more countries implement PPH programmes, and therefore, in order to maximize the efficiency of acceleration of patent grants in specific jurisdictions, it is important to be aware of the different relationships of the patent offices involved.

In order for an application to be eligible for accelerated examination through the PPH, certain requirements have to be met. For example, there are specific requirements about what types of priority claims are acceptable and which documents and requests have to be filed for applications using the PPH. The specific requirements,

documents and requests for each of the PPHs are described in detail on the participating countries' patent office websites.

As a general guideline, a patent application to be processed under a PPH programme may claim priority to a national patent filing in the OFF, a PCT application having no priority claim, a PCT application claiming priority to another PCT application that then has no priority claim, or a PCT claiming priority to a national filing in the OFF. However, it should be noted that there might be differences regarding the priority question in the various PPH programmes, since the PPHs are bilateral contracts between two countries.

A rough outline of the documentary and filing requirements is as follows (also subject to exemptions and special requirements in some of the PPH programmes):

- An application filed with the OSF validly claims priority to one or more applications filed with the OFF.
- The OFF application(s) has at least one claim determined by the OFF to be patentable/allowable.
- All claims in the OSF application for which a request for participation in the PPH programme is made must sufficiently correspond to or be amended to sufficiently correspond to the patentable/allowable claims in the OFF application. Claims will be considered to sufficiently correspond where, accounting for differences due to claim format requirements, the claims are of the same or similar scope. The applicant is also required to submit a claim correspondence table, which must indicate how all the claims in the OSF application correspond to the allowable claims in the OFF application.
- The examination of the OSF application, for which participation in the PPH programme has been requested, has not begun.
- The applicant must file a request for participation in the PPH programme. Request forms will be available from the participating countries' patent office websites.
- The applicant must submit a copy of all the office actions for each of the OFF application(s) containing the allowable claims that are the basis for the request.
- The applicant must submit copies of all the documents cited in the OFF office actions and sometimes translations thereof in the language of the OSF.
- Where the request for participation in the PPH programme is granted, the applicant will be notified and the OSF application will be advanced out of turn for examination. In those instances where the request for participation in the PPH programme does not meet the requirements, the applicant will be notified and the defects in the request will be identified. The applicant will be given one opportunity to correct the request in a renewed request for participation. If it is not corrected, the applicant will be notified and the application will await action in the regular turn.

Accelerated examination in the United States

Irrespective of whether a PPH programme may be used, any applicant can accelerate examination of a US application by filing a petition to make it special under 37 CFR 1.102. The rules for accelerating examination in the United States have been changed recently and now provide the means for applicants to accelerate examination of their application under any circumstances and not, as before, only if the invention was deemed of peculiar importance to some branch of public service and a governmental department head requested immediate action, or if the applicant was over 65 years of age or ill, or if the invention would materially enhance the quality of the environment or contribute to terrorism defence.

This new programme guarantees a final decision on patentability (ie a final office action or a notice of allowance) within 12 months of the petition.

Under this new programme, applicants must file a complete petition along with the appropriate fees, the patent application, an information disclosure statement, an examination support document, and a declaration and power of attorney using the online filing system. In order to request accelerated examination, applications must be limited both in the number and in the scope of the claims. The applications may only have 20 claims, with no more than three independent claims. Applicants must conduct and submit the results of their own patentability search at the time of filing. (However, even though applicants are required to submit a search, this does not mean that the patent examiner will not conduct his or her own search as well.) The applicant's search must utilize acceptable national and international databases and must cover the subject matter of all of the claims, including dependent claims. The applicants also must characterize the search results in writing. Both the search itself and the characterization must be carefully considered to avoid later traps when trying to enforce the resulting patent. Thus, if a patentee failed to disclose certain references as not being material, and a competitor recognizes that the references should have been disclosed, it may be asserted that the patent was obtained with inequitable conduct and therefore the patent is unenforceable.

However, accelerated examination has the disadvantage that applicants must pay high fees and do a significant amount of their own work in order to use this programme. This is due to the costs of conducting a patentability search and attorneys' fees to prepare the written characterization of the search results and information disclosure statements.

Nevertheless, it makes sense under certain circumstances to use the accelerated examination programme. This is the case, for example, if a quick patent grant with a narrow claim set is necessary because of a specific competition situation. However, it may be advisable to also have a co-pending application with a much broader claim scope. Therefore, if prosecution in the accelerated examination case is not moving in a good direction or if the narrow claims granted are not sufficient, another case will be pending with broader claims. This co-pending application also may be used to file another continuation application and request accelerated examination for claims covering different subject matter to the first accelerated application.

Accelerated examination in Europe

The Programme for Accelerated Prosecution of European Patent Applications (PACE) in the European Patent Office was created to decrease pendency of applications in Europe. It involves a simple process in which merely a one-page form is submitted. Use of the PACE programme is quite common, and in some instances an applicant can obtain a first examination within six months of filing the request. One important consideration when using this programme is that the applicant must be able to respond quickly. If the applicant does not respond within the defined specific time limits under the PACE procedure, eg four months after the mailing of the office reaction, the application will lose its special standing and its examination will be significantly postponed.

The accelerated prosecution in the PACE programme has several implications. One is that, if a patent does in fact issue from the application, then the applicant may provide several translations and pay nationalization costs to validate the EP bundle patent in the desired designated states. Furthermore, the patentee may face oppositions within a nine-month period. Therefore, applicants must be aware of these potential developments in order to consider budgetary constraints and strategic considerations before choosing to use the PACE programme for their applications.

Strategic considerations in using the PPH and/or accelerated examination

The applicant must choose carefully where PPH acceleration should begin, particularly with respect to choosing the best jurisdiction for the types of claims that the applicant is interested in pursuing. The applicant must consider whether claims can be successfully reformatted to suit the laws of each patent office. When considering entry into the PPH, the applicant's counsel should forward claims that are close to allowance, for example in Europe, to a colleague in the United States to review and suggest an acceptable claim format for the United States. This proactive measure can minimize potential inefficiencies in the PPH system because, once the PPH entry is triggered, the claims must be in proper format for allowance. By engaging in this proactive discussion, the applicant will consider at an early stage whether it is willing to accept claims of a particular scope.

There are also disadvantages in using the PPH programme. As discussed above, this process involves significant costs up front, for example in terms of attorneys' fees for putting the case in the proper condition to enter the PPH, governmental fees for requesting examination and, possibly, translation fees associated with preparing and submitting information on the office action(s) of the OFF to the OSF. Another disadvantage is that typically the claim scope will be limited, ie restricted to the allowable subject matter in the first application. Therefore, if this is not acceptable to an applicant in a particular case, then the PPH would not be the best approach.

The same applies to the new accelerated examination programme in the United States, because there are significant up-front costs associated with accelerated examination. Therefore, this option may not be in the best interest of certain applicants' businesses. For example, new companies may or may not want to spend the extra money. Early-stage companies may need more time to generate funds for prosecution and may not be able to handle the significant resulting costs if accelerated examination is successful (eg translation fees for the claims upon grant in Europe, validation fees and translation costs in different countries in Europe).

Another reason not to pursue accelerated examination is if the applicant's company needs more time for research and development to provide convincing data for jurisdictions requiring proof of licence to practise or for the creation of actual data in animals or humans.

Another important factor is how well the company really knows its business and its long-term direction. For example, if the company's resources are very limited, it may be problematic to spend significant money on accelerated examination in certain applications. This is particularly so if the pursued claims would not cover the later core products and services, which often change for a company in the early stages. Therefore, if the company spends all its resources in one of its technology areas using accelerated examination and then the company has to shift business direction, there might not be sufficient resources remaining to properly protect the inventions involved in the new business direction.

On the other hand, other businesses cannot afford to wait. For example, if a company has a blockbuster compound or some kind of software technology that might not have a long commercial life, it may be important to take advantage of these acceleration options.

Summary

As a conclusion, in a competitive technical field and if the applicant has an allowable claim that is sufficient to cover the desirable subject matter, the use of the existing PPH programmes and acceleration programmes can be a very efficient and quick way to get patents in other jurisdictions. Using the PPH and/or accelerated examination in the United States or Europe will allow applicants to more quickly reach a conclusion on the prosecution of an application. This resolution can reduce competition, enhance licensing value and increase shareholder value. These advantages should be carefully weighed up against the disadvantages, which are particularly on the cost side.

Appendix: Contributors' contact list

Appleyards
Appleyards House
72 Brighton Road
Horsham
West Sussex RH13 5BU
Tel: +44 (0) 8705 275201
Contact: Allan Robinson
e-mail: allan.robinson@appleyards.co.uk
www.appleyards.co.uk

Bird Goën & Co
Klein Dalenstrat 42A
B-3020 Winksele
Belgium
Tel: +32 (0) 1648 0562
Fax: +32 (0) 1638 0528
Contact: William Bird
e-mail: ipadmin@birdgoen.com
www.ipadmin@birdgoen.com

bohmann || bohmann (Bohmann & Loosen)
Nymphenburger Strasse 1
D-80335 Munich
Germany
Tel: +49 (0) 8951 5564
Contact: Armin Bohmann
e-mail: akb@bohmann-law.com
www.bohmann-law.com

Borenius & Co Oy Ab
Tallberginkatu 2A
00180 Helsinki
Finland
Tel: +358 (0) 9686 6840
Fax: +358 (0) 9686 68444
e-mail: mail@borenius.fi
www.borenius.fi

Brann AB
Box 17192
Västëtagatan 2
104 62 Stockholm
Sweden
Tel: +46 (0) 8 429 1000
Fax: +46 (0) 8 429 1070
Contact: Peder Oxhammar or Hampus Rystedt
e-mail: peder.oxhammar@brann.se or hampus.rystedt@brann.se

CCH, Wolters Kluwer
145 London Road
Kingston upon Thames
Surrey KT2 6SR
Tel: +44 (0) 20 8547 3333
Fax: +44 (0) 20 8547 2638
Contact: Richard Pike
e-mail: Richard.Pike@wolterskluwer.com
www.cch.co.uk

Centre for Effective Dispute Resolution (CEDR)
International Dispute Resolution Centre
70 Fleet Street
London EC4Y 1EU
Tel: +44 (0) 20 7536 6000
Fax: +44 (0) 20 7536 6001
Contact: Andy Rogers
Direct line: +44 (0) 20 7536 6044
e-mail: arogers@cedr.com
www.cedr.com

Chartered Institute of Purchasing and Supply (CIPS)
Easton House
Easton on the Hill
Stamford PE9 3NZ
Tel: +44 (0) 1780 756777
Fax: +44 (0) 1780 751610
Contact: Trudy Salandiak
e-mail: trudy.salandiak@cips.org
www.cips.org

Control Risks
Cottons Centre
Cottons Lane
London SE1 2GQ
Tel: +44 (0) 20 7970 2100
Contact: Corene Crossin or James Smither
Fax: +44 (0) 29 7970 2222
e-mail: graconsultingprojects@control-risks.com
www.control-risks.com

Deposix Software Escrow GmbH
Infanteriestrasse 11a
D-80797 Munich
Germany
Tel: +49 (89) 9901 3654 or +49 (700) ESCROW-DE
Contact: Stephan Peters
e-mail: stephan.peters@deposix.com
www.deposix.com

Federation of European Risk Management Associations (FERMA)
Avenue Louis Gribaumont
1/B-4 – 1150 Brussels
Tel: +32 (0) 2761 9432
Fax: +32 (0) 2771 8720
Contact: Florence Bindelle
e-mail: info@ferma.eu
www.ferma.eu

Field Fisher Waterhouse LLP
35 Vine Street
London EC3N 2AA
Tel: +44 (0) 20 7861 4000
Fax: +44 (0) 20 7488 0084
Contact: Aymen Khoury
e-mail: aymen.khoury@ffw.com
www.ffw.com

Holme Patent A/S
Vesterbrogade 20
1620 Copenhagen V
Denmark
Tel: +45 (0) 3324 2121
Fax: +45 (0) 3324 9121
Contact: Annelise Holme
e-mail: ah@holmepatent.dk
www.holmepatent.dk

HSBC Operational Risk Consultancy
Bishops Court
27–33 Artillery Lane
London E1 7LP
Tel: +44 (0) 735 7661 2335
Contact: Gavin Temple
e-mail: gavintemple@hsbc.com
www.insurancebrokershsbc.com

Huber & Schüssler
Truderinger Strasse 246
81825 Munich
Germany
Tel: +49 (0) 8943 7788 0
Fax: +49 (0) 8943 778899
Contact: Andrea Schüssler
e-mail: info@patservice.de
www.patservice.de

Institute of Risk Management (IRM)
6 Lloyd's Avenue
London EC3N 3AX
Tel: +44 (0) 20 7709 9808
Fax: +44 (0) 20 7709 0716
Contact: Steve Fowler
e-mail: steve.fowler@theirm.org
www. theirm.org

Ipendo AB (Global Headquarters)
Södergatan 15
SE-211 34 Malmö
Sweden
Tel: +46 (0) 4012 0540
Fax: +46 (0) 4012 0542
e-mail: info@ipendo.com
www.ipendo.com

Ipendo Inc
7825 Fay Avenue
Suite 200
La Jolla
CA 92037
USA
Tel: +1 858 456 5509
Fax: +1 888 490 4675
Contact: Helene Vik
e-mail: helene.vik@ipendo.com

Kolster Oy Ab
PO Box 148
Iso Roobertinkatu 23
FI0021 Helsinki
Finland
Tel: +358 (0) 9 6188 2209
Contact: Anne Suutala
e-mail: anne.suutala@kolster.fi
www.kolster.com

KPMG LLP
8 Salisbury Square
London EC4Y 8BB
Tel: +44 (0) 20 7311 8790
Fax: +44 (0) 20 7311 8080
Contact: Simon Evans
e-mail: simon.db.evans@kpmg.co.uk

Liberty International Underwriters
3rd Floor, Two Minster Court
Mincing Lane
London EC3R 7YE
Tel: +44 (0) 20 7860 6600
Fax: +44 (0) 20 7860 6290
Contact: Matthew Hogg
e-mail: matthew.hogg@libertyin.com
www.liueurope.com

Lloyd's Register Quality Assurance (LRQA)
LRQA Centre
Hiramford
Middlemarch Office Village
Siskin Drive
Coventry CV3 4JF
Tel: +44 (0) 24 7688 2387
Fax: +44 (0) 24 7630 6055
Contact: Alex Briggs
e-mail: alex.briggs@lrqa.com
www.lrqa.com

Lucidus Consulting Limited
90 Long Acre
Covent Garden
London WC2E 9RZ
Tel: +44 (0) 20 7060 2196
Fax: +44 (0) 20 7060 2198
Contact: Ruth Murray-Webster
Mobile: +44 (0) 7974 943443
e-mail: ruth@lucidusconsulting.com
www.lucidusconsulting.com

Maikowski & Ninnemann
Kurfürstendamm 54–55
10707 Berlin
Germany
Tel: +49 (0) 30 881 8181
Fax: +49 (0) 30 882 5823
Contact: Dr Gunnar Baumgärtel
e-mail: office@maikowski-ninnemann.com
www.maikowski-ninnemann.com

Marsh Ltd
Tower Place East
London EC3R 5BU
Tel: +44 (0) 20 7357 1000
Fax: +44 (0) 20 7929 2705
Contact: Fredrik Motzfeldt
e-mail: Fredrik.Motzfeldt@marsh.com
www.marsh.com

Moetteli & Associés SàRL
St Leonhard-strasse 4
CH-9000 St Gallen
Switzerland
Tel: +41 71 230 1000
Fax: +41 71 230 1001
Contact: John Moetteli
e-mail: moetteli@patentinfo.net
www.moetteli.com

NanoCentral
The Centre for Process Innovation
Wilton Centre
Wilton
Redcar TS10 4RF
Tel: +44 (0) 1642 442464
Contact: Stephen Cash
e-mail: stephen.cash@nanocentral.eu
www.nanocentral.eu

Norland Managed Services Limited
City Bridge House
57 Southwark Street
London SE1 1RU
Tel: +44 (0) 20 7871 9221
Contact: Paul Saville-King
e-mail: paul.saville-king@norlandmanagedservices.co.uk
www.norlandmanagedservices.co.uk

Nortech Control Systems Limited
42 Llantarnam Business Park
Cwmbran
South Wales NP44 3AW
Tel: +44 (0) 1633 485533
Fax: +44 (0) 1633 485666
Contact: Keith Hardy
e-mail: keith.hardy@nortechcontrol.com
www.nortechcontrol.com

Rings & Spranger Patentanwälte
Rauchstrasse 8
81679 Munich
Germany
Contact: Rolf Rings
Tel: +49 (0) 8990 77 823 0
Fax: +49 (0) 8990 77 823 22
e-mail: info@rs-patent.de
www.rs-patent.de

Serravalle sas
Via Matteotti 23
26584 Comegliano L. (LO)
Italy
Tel: +39 0371 495771
fax +39 0371 956840
Contact: Marco Serravalle
e-mail: marco.serravalle@serravalle.eu
www.serravalle.eu

Tampereen Patenttitoimisto Oy
Hermiankatu 1B
FIN-33720 Tampere
Finland
Tel: +358 (0) 10 227 2600
Contact: Kim Simelius
e-mail: kim.simelius@berggren.fi
www.berggren.fi

Towergate Corporate
Blenheim House
Newmarket Road
Bury St Edmunds IP33 3SB
Tel: +44 (0) 1284 756565
Fax: +44 (0) 1284 750525
Contact: Dominic Roe
e-mail: dominic.roe@towergate.co.uk
www.towergate.co.uk

UKAS
21–47 High Street
Feltham
Middlesex TW13 4UN
Tel: +44 (0) 20 8917 8458
Fax: +44 (0) 20 8917 8500
Contact: Jon Murthy
e-mail: jon.murthy@ukas.com
www.ukas.com

Version One Limited
Pentland House
Village Way
Wilmslow
Cheshire SK9 2GH
Tel: +44 (0) 1625 856500
Fax: +44 (0) 1625 856501
Contact: Julian Buck
e-mail: julian.buck@versionone.co.uk
www.versionone.co.uk

Wolters Kluwer
PO Box 1030
2400 BA, Alphen aan den Rijn
The Netherlands
Tel: +31 (0) 172 641400
Fax: +31 (0) 172 474889
e-mail: info@wolterskluwer.com
www.wolterskluwer.com

XL Insurance
XL House
70 Gracechurch Street
London EC3V 0XL
Tel: +44 (0) 20 7933 7000
Contact: Nigel Bamber
e-mail: nigel.bamber@xlgroup.com
www.xlinsurance.com

Index

THIS PAGE IS INTENTIONALLY LEFT BLANK

Index of advertisers

THIS PAGE IS INTENTIONALLY LEFT BLANK

THIS PAGE IS INTENTIONALLY LEFT BLANK