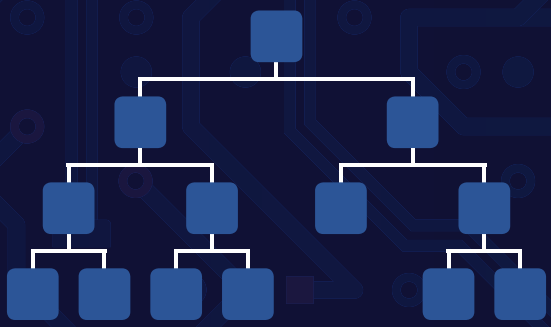

Rational Cybersecurity for Business

The Security Leaders' Guide to Business Alignment

Dan Blum

apress open

Rational Cybersecurity for Business

The Security Leaders' Guide to Business Alignment

Dan Blum

Apress open

Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment

Dan Blum
Silver Spring, MD, USA

ISBN-13 (pbk): 978-1-4842-5951-1 ISBN-13 (electronic): 978-1-4842-5952-8
https://doi.org/10.1007/978-1-4842-5952-8

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Jessica Vakili

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit http://www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/978-1-4842-5951-1. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

Table of Contents

About the Author

Dan Blum is an internationally recognized cybersecurity and risk management strategist. He provides advisory services to CISOs and security leaders and thought leadership to the industry. Formerly, he was a Golden Quill award-winning VP and Distinguished Analyst at Gartner and one of the founding partners of Burton Group.

He has over 30 years experience in IT, security, risk, and privacy. He has served as the security leader for several startups and consulting companies, and has advised 100s of large corporations, universities, and government organizations. He is a frequent speaker at industry events and has written countless research reports, blog posts, and articles.

During his tenure at Burton Group and Gartner, Dan Blum filled multiple consulting delivery and content leadership roles. He led consulting and research teams for Security and Risk Management, Identity and Privacy, and Cloud Security. He co-authored and facilitated Burton Group's signature Identity and Security Reference Architectures. He managed successive Program Tracks at the Catalyst conferences and spoke at Gartner's Security Summit and many other third party events.

A Founding Member of the Kantara Initiative's IDPro group and honored as a "Privacy by Design Ambassador", Mr. Blum has also authored three books, written for numerous publications, and participated in standards or industry groups such as ISACA, the FAIR Institute, IDPro, CSA, OASIS, Open ID Foundation and others.

About the Technical Reviewers

Christopher Carlson finished his 39-year career at The Boeing Company as an Associate Technical Fellow. He entered the computing security field in 1982, holding a variety of technical and management positions. Management highlights include leading the company-wide classified computing security program, creating the company's security control framework in 1991, and being the security manager for the 777 program and chief security officer for the Sonic Cruiser program, forerunner of the 787. Selected technical responsibilities include defining requirements for and leading implementation of a role-based access management system, introducing secure application development methods, system management of a governance, risk and compliance system, and leading selection and implementation of a data security and insider threat detection system.

C T Carlson LLC was established to provide information security writings and advisory services. His book *How to Manage Cybersecurity Risk: A Security Leader's Roadmap with Open FAIR* was published in December 2019. Chris also produces writings related to FAIR for The Open Group Security Forum.

Chris has a Master of Science in Computer Science from Washington State University. He is a Certified Information Systems Security Professional and is Open FAIR Certified.

Andrew Yeomans is a Chief Information Security Officer for Arqit Limited, which is leading a pan-European consortium building a secure quantum cryptography satellite network.

Andrew was on the management board of the Jericho Forum, an international thought leadership group solving the security issues of a collaborative deperimeterized world.

Previously, Andrew led Information Security Engineering, Architecture, and Strategy for Lloyds Bank, Commerzbank, and Dresdner Kleinwort Investment Bank for 18 years, after leading IBM's European technical sales for Internet security.

Acknowledgments

To my wife, family, and friends who make life worth living and whose support and encouragement make this work possible.

To all whom I've worked with over the years and interviewed for this book: Thank you for the knowledge you've shared.

And thanks to the security, business, and IT leaders interviewed for the book. Your stories and suggestions have enriched the work immeasurably.

Rational Cybersecurity Interview List

Security, Business, and IT Leaders

Adi Agrawal	Rick Howard	Tom Sinnott
Cathy Allen	Debra Lee James	Vaughn Sizemore
Iftach Ian Amit	Joey Johnson	James Tompkins
Dan Beckett	Jack Jones	Simon Wardley
Brad Boroff	Steve Katz	Tim Weil
Kirk Botula	William Kasper	Evan Wheeler
Kip Boyle	Diana Kelley	Mary Wujek
Craig Calle	Robert Kistner	Andrew Yeomans
Christopher Carlson	Omar Khawaja	
Robina Chatham	Thom Langford	
Anton Chuvakin	Alex Lawrence	
Rob Clyde	Jamie Lewis	
Fred Cohen	Tim Mather	
David Cross	James McGovern	
Johnathon Dambrot	Rick Mendola	

(*continued*)

Rational Cybersecurity Interview List	
Security, Business, and IT Leaders	
Deirdre Diamond	Harshil Parikh
Michael Everall	Joe Prochaska
Ed Ferrara	Kai Roer
Randall Gamby	Alex Rogozhin
Mike Gentile	Gary Rowe
Rocco Grillo	James Rutt
Doug Grindstaff	Greg Schaffer
Malcolm Harkins	David Sherry
Karen Hobert	Paul Simmonds

Introduction

This book is a Security Leaders' Guide to aligning with the business. If you are a Chief Information Security Officer (CISO), Head of Security with a similar title, a security manager, or a security team member providing leadership to the business, this book is for you.

Why Security Leaders Must Get the Business Fully Engaged

One of our Rational Cybersecurity interviews illustrated the challenge of a *disengaged* business.

THE BREACH WAS PREDICTABLE

Not long ago, the former CISO of a large US company related this story:

"We had a flat network between all our credit card processing sites and some other serious gaps. I went to my CIO with a request for funding, but here's the response: *'We're expanding into [an overseas location] next year and can't afford the projects you're proposing. In fact, we need to cut your budget by 50%.*'

After that, I put my resume on the market and left soon. The company retained an offshore managed security service provider (MSSP) with advanced malware detection tools, but only skeleton staff for security operations stateside. Within 6 months the alarms were ringing but they keep hitting the snooze button."

The rest is history as the company – a household name – suffered a bad breach and botched its messaging to the public during incident response. Direct and indirect costs mounted to tens and then hundreds of millions and the CEO resigned within 6 months.

I've seen way too many businesses with disengaged senior management like this. It takes two basic forms:

1) Security's not considered to be a priority.
2) Or, the organization has budgeted for security, hired staff, and deems it "handled." Executives delude themselves into thinking they've put security first even if in practice it is routinely put way behind other priorities.

We see the second, insidious, form of disengagement even at highly regulated businesses. Staff, even in the security department, are afraid to do anything other than put an optimistic spin on security issues reported up the chain.

Misalignment between security and the business can start at the top or happen at the line of business, IT, development, or user level. It has a corrosive effect on any security project it touches. As organizations transform themselves into "digital businesses," they fall under increasing IT-related risk and regulation. Aligning cybersecurity and IT with business leaders and business processes becomes exponentially more important to digital businesses.

The Rational Cybersecurity Journey

I chose to write *Rational Cybersecurity for Business* because, during my career as an IT research analyst and consultant, I've learned that successful cybersecurity isn't just about the technology, it's also about the people and organizations. I realized midway through this project, however, that I could write the book for security leaders as the primary audience or for business leaders, but not for both. Therefore, Table 1 summarizes what this book IS and IS NOT.

Table 1. *What the Book Is For*

THE BOOK IS	IS NOT
Written for the security leader audience and informed by interviews with business and IT leaders	NOT attempting to be an easy read for businesspeople without a background in IT
A leadership guide on how to align six Rational Cybersecurity priorities to the business	NOT a highly technical or comprehensive manual on everything in cybersecurity
Scaled to fit many types of businesses – from the very large organization down to ones that are small but still big enough to have a security department	NOT intended for tiny organizations with minimal security program needs

You won't find many security professionals disagreeing about the need to align security and the business. But although technical books on cybersecurity abound, there are relatively few business-focused ones, and none that I've found written specifically for security leaders with comprehensive and specific advice on how to align with the business.

I feel strongly that if we can improve their business alignment, security programs can be much more effective. A business's security team will be adequately resourced. It will have a seat at the table when IT or risk is part of any business decision or strategy and will be brought in early to review new projects, vendor relationships, or system designs. Security leaders won't act like "Dr. No" when a potentially risky business proposal or IT release lands on the table, and they won't emit fear, uncertainty, and doubt (FUD) like frightened octopuses spewing ink when challenged. Instead they'll quantify the risks and propose realistic alternatives. The security team can act as a coach to business or IT managers and staff. Together, business and security leaders can make the secure way to operate in the business also be the easy way.

Last but not least, I decided to open source the book's digital editions because cybersecurity-business alignment is such an important topic. I want to create an open information flow. Look for the pointers at the end of Chapter 10 on how readers can continue the discussion we're about to begin here.

How the Book Is Organized

Cybersecurity is a vast topic, and many kinds of businesses exist with different cultures, drivers, missions, models, and products or services. Facing a general problem statement of "How should security align with business?", one could easily get lost in the matrix of what to align with what.

It can be hard to stay focused on alignment while trying to explain just enough detail about many cybersecurity topics and to share so many good security practices for people, process, and technology. Therefore, this book applies the 80–20 rule (aka Pareto Principle[i]) to cybersecurity as its organizing framework.

The Cybersecurity Pareto Principle

How can security leaders get 80% of the benefit by doing 20% of the work?

To this question, I ended up choosing six priority focus areas to cover in the book's chapters. They are: security governance and culture, risk management, control baseline, IT and security simplification, access control, and cyber-resilience.

To stay focused on alignment within these areas, I also provide more than 50 specific *keys to alignment* within the narrative. These keys are called out as follows in the text.

1

Buy into the need for business and security alignment and get curious about what that means for security and business stakeholders.

Less often, I cite numbered *cybersecurity myths*, starting with this one.

1

*Cybersecurity is **just** a technical problem.*

Chapter Summary

Although the book isn't overly technical, it does require background in basic IT and security terminology. However, if you run into a term you're not familiar with or are curious about how I'm using a term, please check on the Glossary provided at the end of the book.

Here's how the book's ten chapters address the Cybersecurity Pareto Priorities:

- **Chapter 1: Executive Overview.** Defines Rational Cybersecurity, summarizes the book, and describes the six cybersecurity priority focus areas.
- **Chapter 2: Identify and Align Security-Related Roles**. Explains how the people in the business each contribute to the secure operation of the business and the various security-related roles they can fulfill.
- **Chapter 3: Put the Right Security Governance Model in Place.** Contrasts basic security governance structures that businesses can use and provides guidance on how to select one and make it work. It describes core elements of the security program such as steering committees and security policy lifecycle management. It also offers guidance on where the CISO should report in an organization.
- **Chapter 4: Strengthen Security Culture Through Communications and Awareness Programs.** Brings the cultural subtext that can make or break a cybersecurity environment into the foreground. It analyzes the components of security culture and provides guidance on how to devise a security culture improvement process and measure its effectiveness. User awareness, training, and appropriate day-to-day engagement with the business can all play a part in forging a constructive security culture.
- **Chapter 5: Manage Risk in the Language of Business.** Clarifies why risk management must be the brains of the security program. It must analyze, monitor, and communicate what potential losses or circumstances constitute the business's top risk scenarios. An effective tiered risk analysis process can efficiently address myriad

risk issues from multiple sources, help apportion accountability and responsibility, and prioritize controls or other risk treatments.

- **Chapter 6: Establish a Control Baseline.** Lists the 20 security control domains security leaders must consider when creating a minimum viable set and maps to control frameworks such as ISO 27001 and the NIST Cybersecurity Framework. It also details which business functions security leaders must align with to implement safeguards within the control domains, how to scale and tune requirements for different types of businesses, and how to share responsibility for delivering the controls with third parties.
- **Chapter 7: Simplify and Rationalize IT and Security.** Argues that security leaders have a stake in the IT strategy and provides guidance on how security leaders – who don't own IT – can still engage IT and digital innovation leaders to help develop and deliver on the strategy.
- **Chapter 8: Control Access with Minimal Drag on the Business.** Explains why access control is a critical balance beam for business agility, compliance mandates, and the security program. It addresses the need for information classification, data protection, and identity and access management (IAM) controls to implement access restrictions as required to reduce risk or attain regulatory compliance but do so in a way that enables appropriate digital relationships and data sharing with internal and external users.
- **Chapter 9: Institute Resilience Through Detection, Response, and Recovery.** Guides readers on how to formulate contingency plans, strategies, and programs for detection, response, and recovery which together comprise cyber-resilience.
- **Chapter 10: Create Your Rational Cybersecurity Success Plan.** Takes readers through an exercise to create a personalized "Rational Cybersecurity Success Plan" using the Success Plan Worksheet[1] as a template. This worksheet provides a template for readers to capture their assessments and improvement objectives for their existing

[1] "Rational Cybersecurity Success Plan Worksheet," Dan Blum, Security Architects LLC, May 2020, accessed at https://security-architect.com/SuccessPlanWorksheet

security environment. It's designed to be used over a 90-day period, but readers can extend it or create additional copies for new periods.

How to Get the Most Out of the Book

To maximize the value from this book, readers can

- Read Chapter 1 for a detailed summary of the book and note areas of immediate or special interest.
- Read or review all chapters for comprehensive guidance on the six Rational Cybersecurity focus areas for security to business alignment.
- Select the chapter(s) that corresponds most closely to current pain points or active projects as their priority topics for reading. For example, someone working in data governance or enterprise authorization for a financial service might concentrate their attention early on to Chapters 3 (governance), 5 (risk), and 8 (access control and data governance).

At the end of each chapter, a "Call to Action" section contains a quick summary of core recommendations and instructions for completing the next part of your personalized Rational Cybersecurity Success Plan Worksheet.

After completing the first nine chapters and/or your priority topics, turn to Chapter 10 and complete any parts of the worksheet that you haven't tackled during the earlier chapters.

Call to Action

This book can be a powerful resource for security leaders who believe that business engagement and alignment *is* one of their key performance indicators. Look back on your career path and think of at least three times a lack of business alignment has been a challenge for your security projects and also remember times when effective business alignment has enabled your projects to succeed.

Buy into the need for business and security alignment and get curious about what that means for security and business stakeholders.

And then read on to Chapter 1 for a deeper dive into what cybersecurity-business alignment means, an explanation of the six Rational Cybersecurity priority focus areas, and an executive overview of the book. Consider how the six priority focus areas could relate to your organization.

Note

i. "Pareto Principle," Wikipedia, accessed at https://en.wikipedia.org/wiki/Pareto_principle

CHAPTER 1

Executive Overview

To even begin to achieve the promise of cybersecurity, security and business leaders must align to rationalize cybersecurity. They must go beyond the myths – such as the one that cybersecurity is just a technical problem – that still mislead many in the market.

Myths aside, basic concepts of Rational Cybersecurity are already conventional wisdom. We've all heard that "Security is about people, process, and technology." But that can sound like overly general advice not calibrated to our type of IT environment or business. And where do we begin? Conventional wisdom advises starting with a security assessment and devising a plan for the security program.

Such conventional wisdom is fine as far as it goes, but security leaders need more detail. I propose to provide that with specific guidance for aligning security programs to the business through six priority focus areas

- Build a healthy security culture and governance model
- Manage risk in the language of the business
- Establish a control baseline
- Simplify and rationalize IT and security
- Govern and control access without creating a drag on the business
- Institute cyber-resilience, detection, response, and recovery

Although these priorities are a pretty good fit for most organizations, it's important to understand they're not an ordered list and they need to be scaled for a business's industry, size, complexity, level of security pressure, and maturity level.

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8_1

This chapter provides an executive overview of the book's content in the following sections:

- Understand the Rational Cybersecurity context
- Start the Rational Cybersecurity journey (by defining security for *your* business and beginning to gain executive support and align with stakeholders)
- Set Rational Cybersecurity priority focus areas for the security program
- Scale security programs to your organization type

Let's begin by understanding why cybersecurity-business alignment on a well-defined, prioritized security program is so critical.

1.1 Understand the Rational Cybersecurity Context

As security leaders, you may not need a cybersecurity backgrounder. But stick with me: I'll keep it short, and I think we'll find it worthwhile to get on the same page about our overall challenge in defending the business and how it's exacerbated by some "myths of cybersecurity."

Let's start with the word "cybersecurity" on which our profession is founded. We often use it synonymously with "IT security," "information security," or "security." What's so special about it?

Figure 1-1. *Etymology of the Term "Cybersecurity"*

The common dictionary definition of the root term "security" includes "freedom from risk or danger." Hmm… not likely in cyberspace, or in physical space. What about the word "cyber"? It comes from the Greek term kybernḗtēs meaning "helmsman" or "steersman." Doesn't that seem to connote forward-looking, or future-looking? "Cyber" was also popularized from the word "cyberspace," first coined by scifi writer William Gibson in the book *Neuromancer*, which 30 years later is still a great read. Cyberspace means *the space where people and machines converge*.

The words cyber and cybersecurity have been sensationalized by politicians and the media for public consumption without much clarity. That's why I've coined the term Rational Cybersecurity, which I define as

---

Rational Cybersecurity "An explicitly-defined security program based on the risks, culture, and capabilities of an organization that is endorsed by executives and aligned with its mission, stakeholders, and processes."

1.1.1 Risk and the Digital Business

As of 2019, much of the business world had been actively discussing the "digital transformation" for well over 5 years. Gartner, Inc. (the world's premier IT research and advisory service and my former employer) calls this trend digitalization. According to surveys from Gartner, more than 87% of senior business leaders say digitalization is a company priority. But Gartner cautions that only 40% of organizations have brought digital initiatives to scale.[1]

In early 2020, the global response to the COVID-19 pandemic forced most businesses to send their staff home to "shelter in place" or shut down in-person operations such as malls, movie theaters, or manufacturing plants entirely. A great many of the business processes that continued operating did so only through digital processes and telecommuting. As the crisis continues, not only are massive numbers of employees working at home, but many business processes are shifting online in order to operate at all. It is as if COVID-19 has pressed the gas pedal on the digital transformation.

Digital transformation demands more cybersecurity, not just because it means "more IT" but also "riskier IT." Newer technologies – such as mobile devices, social networks, cloud computing, artificial intelligence (AI), and the Internet of Things (IOT) – are all seeing accelerated adoption during the pandemic. Unfortunately, new technologies often emerge without adequate security built in. Deeper blends of the virtual, physical, and social worlds merge into something new, often with profound security implications. In extreme cases, digital outages or cyberattacks could stop elevators, crash vehicles, start fires, explode pipelines, or turn off medical devices.

---

[1] "Accelerate Digital Transformation," Gartner, Inc., 2020, accessed at www.gartner.com/en/information-technology/insights/digitalization

Cyberattackers can steal vital trade secrets and purloin personal identity records from business databases for use in credit card fraud and identity theft exploits. They also conduct extortion schemes, such as ransomware attacks which encrypt digital information and demand payment for the key to unlock it. Even mature remote access systems, web-based applications, and business processes can be highly vulnerable when deployed without adequate testing, hardening, and procedural controls. The early days of the COVID-19 crisis saw increased cyber-fraud as business processes such as accounting or payroll underwent forced digitalization. For example, a member of this book's marketing team reported that his Head of Admin received a fake email purportedly from him requesting a change to his direct deposit account number. Luckily, she called his home office to verify the request rather than putting it through.

THE SURPRISING STORY OF NOTPETYA AND AN UNLIKELY DIGITAL BUSINESS

Imagine shipping containers piled on the docks of Hoboken, New Jersey, with nowhere to go. During the NotPetya ransomware epidemic, global shipping giant Maersk discovered it literally could not deliver or send on unloaded shipping containers without access to the electronic manifests.[2] *You wouldn't consider a maritime tanker company a digital business, but clearly it is in part. Digital businesses cannot operate without IT.*

Note The ransomware problem is getting worse since the NotPetya events of 2017. Many small or medium businesses (SMBs) in the United States affected by ransomware have been forced to cease operations.[3]

Cybersecurity for the digital business addresses "information risk," which includes both "cyber-risk" (from attacks on IT) and "IT operational risk" (from IT errors, failures, and outages). It's the security leader's job to propose controls or workarounds to protect the business, whenever possible in a way that doesn't impede or slow innovation. It is the business leader's job to work with security to balance opportunity and risk.

[2] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Andy Greenberg, *WIRED*, September 2018, accessed at www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[3] "Wood Ranch Medical Announces Permanent Closure Due to Ransomware Attack," HIPAA Journal, December 2019, accessed at: https://www.hipaajournal.com/wood-ranch-medical-announces-permanent-closure-due-to-ransomware-attack/

1.1.2 Compliance and the Duty to Protect

Regulatory obligations also create digital business risk. They spell out duties to protect personal privacy, health-care or financial information, critical infrastructure, and more. Courts of law haggle over liability. For example, did a breached business follow "reasonable" protection practices, did it even uphold its own policies, or should it have invested more money in security?

What are your business's protection objectives? See Table 1-1 for a list of some regulations covering various vertical industries to give you some idea. Note that although we tried to hit the main regulatory topics (privacy, critical infrastructure, health, finance, and public company accounting), Table 1-1 shows only a small sampling. However, it's a safe bet that your business is subject to some of these or to similar regulations in countries all over the world.

Table 1-1. *A Small Sample of Compliance Regulations*

Industry	Regulations
All US public companies	Sarbanes-Oxley Act (SOX) requires companies to report on internal controls over accounting and other critical IT systems. The Securities and Exchange Commission (SEC) guidance pushes companies to report material cybersecurity risks to shareholders and potential investors.
All business in personal data	EU General Data Protection Regulation (GDPR) and various other countries' privacy regulations protect personal information; they require informed consent for using the information along with other individual rights. US state laws require organizations to report loss of sensitive personal or financial information and offer victims free credit reporting services. Violating any of these regulations leads to fines, liability, and reputation damage. The California Consumer Privacy Act (CCPA) brings GDPR-style regulation to the USA.
All electronic records	The US Federal Rules of Civil Procedure (FRCP) sets requirements for retention and accessibility of electronic records for use in legal proceedings' discovery or evidentiary processes.

(*continued*)

Table 1-1. (*continued*)

Industry	Regulations
Banking and financial services institutions (FSIs)	US Gramm-Leach-Bliley, the Singapore Monetary Authority, and other national regulations protect personal financial information. Other regulations: New York Department of Financial Services (DFS) Cybersecurity Regulation, anti-money laundering (AML) and know your customer (KYC) regulations in multiple countries, Payment Card Industry (PCI) Data Security Standard (DSS). The Basel 3 accords require reporting of operational and other risks and require capital to be set aside to cover those risks.
Health care	US Health Insurance Portability and Accountability Act (HIPAA) addresses privacy and requires covered entities like hospitals and insurance companies (and third-party business associate companies) to protect patient privacy and give patients some control over their records. The US Food and Drug Administration (FDA) Code of Federal Regulations (CFR) Title 21 Part 11 regulates handling of electronic records and signatures in drug manufacturing, clinical trials, and other applications.
Utilities (critical infrastructure)	The NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) plan is a set of requirements designed to secure the assets required for operating North America's electrical grid. Utilities are required to identify and protect critical assets, perform risk assessments, enforce IT controls, and maintain contingency plans for protection. In Europe, the Directive on Security of Network and Information Systems (NIS Directive) specifies legal measures to boost the overall level of cybersecurity in the EU.

Information risks (compliance related or otherwise) are far from the only risks that businesses must deal with. Businesses also face financial risks, operational risks, market risks, project risks, and even the risk of NOT embarking on new strategies. Business success or even survival may depend on the ability to undertake bold digital transformation initiatives. For example, many retailers failed to excel at online commerce (yesterday's digital transformation). Today, many of them are gone or in decline. In general, businesses that are further along with digitalization are more likely to survive disruptions such as the "COVID-19 shutdown."

1.1.3 Taking Accountability for Risk

After walking through the digital business risks and compliance issues, one would think it should be easy to gain executive-level support and information risk ownership. But as we'll see in the "Address Common Challenges" sections of Chapters 2 and 4, cybersecurity still isn't considered strategic by many executives.

What is creating this "cybersecurity deficit"[4] not only in executive awareness but in security programs themselves? I believe the core reasons are the lack of specific and actionable guidance on how to align security with the business and some common misconceptions (or myths) about information risks. *Simply put, risk is the core topic for Rational Cybersecurity.* It is so important that I'll do a bit of a deep dive on risk up front.

We read about information risk scenarios daily. Over the last few years, we've seen hackers compromise or disrupt the US Office of Personnel Management (OPM) staff database, some UK National Health System hospitals, the Maersk shipping line, and countless other organizations catalogued at the "World's Biggest Data Breaches & Hacks" website.[5] We've learned that Intel or AMD chips in every computer could be vulnerable and experienced exploits against virtual machines, C programming language libraries, Windows, Linux, and all operating systems almost without exception.

With all the news coverage of cyberattacks and vulnerabilities, there's a sense of drowning in information risk, that cybersecurity is getting worse. But there's no clear accounting of how bad it is, how we can fix it, how much that should cost, and what we should do today.

What if we *could* account for information risk? Imagine risk appearing on a business's future- or forward-looking accounting ledger or forecast, as shown in Figure 1-2. Much as forecasted operating assets and revenues comprise the "assets" side of the ledger, outflows from risks that could materialize into losses could join forecasted business expenses on the "liabilities" side.

[4] "Cybersecurity Deficit: More than a Skills Shortage," by Dan Blum, January 2020, accessed at https://security-architect.com/cybersecurity-strategy-deficit/

[5] "World's Biggest Data Breaches & Hacks," David McCandless, *Information is Beautiful*, accessed at www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

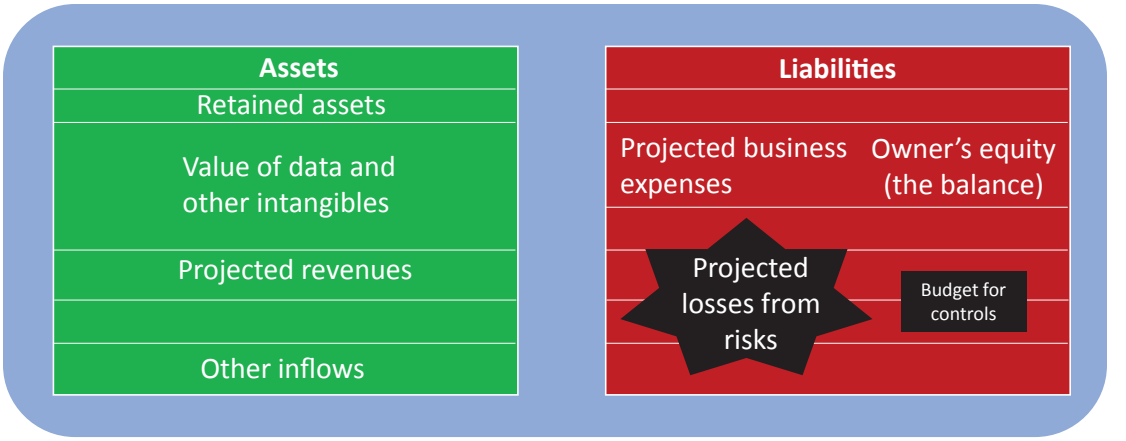

Figure 1-2. *Risk on a Conceptual Accounting Ledger*

The typical business doesn't actually have a ledger like the one in Figure 1-2. However, risk is the context and raison d'etre for security programs. What's less well understood is that just as business executives are accountable for the financial bottom line, they're also accountable for information risks. Business leaders – such as the CEO and lower-level line of business (LOB) leaders – are the "risk owners." (The CEO is accountable to the public, and lower-echelon risk owners are accountable or responsible to the CEO). Risk owners must ensure that actual losses remain at a tolerable level, and to do that, it requires risk management.

1-1

Place accountability for information risk at the business leadership level where the resources, budget, and fiduciary responsibilities lie. Then manage risk in the language of business.

Some businesses do track risks at the enterprise level using a "risk map" or "risk register." The risk map is a common tool used in enterprise risk management (ERM) to represent the top risks to the business. Top risks may be presented as a simple list from 1 to N or displayed on a graph ranking each one's likelihood of occurring and the potential impact. For example, a large manufacturing company might consider the failure of a sole-source factory that produces a critical component to be one of its top concerns. One information risk scenario that security leaders could weave into the risk map would be ransomware infecting that same factory's controllers and logistics systems to cause the failure.

Standing in the way of making information risk more transparent and manageable to business leaders, however, is our second myth of cybersecurity.

2

It is not possible to quantify information risk in any useful way.

Ten or fifteen years ago, myth #2 might have been generally true. We didn't have a good risk quantification model, tools, or much actuarial data then. I can remember starting a security research service for Burton Group (a company later acquired by Gartner) around 2004. At the time my research team of security experts all agreed quantifying risk wasn't useful.

Fortunately, we now have the model and some tools to work with for the purpose of calibrating risk estimates. The Factor Analysis of Information Risk (FAIR) model has been standardized by The Open Group.[6] Open FAIR provides a taxonomy for calculating risk as *the probable frequency and magnitude of future* loss, which can also be described as *annualized loss expectancy*. These calculations aren't trivial, and it is still necessary to have subject matter experts who can be used to develop calibrated estimates on the frequency of attacks, effectiveness of controls, and magnitude of losses. However, we've made tremendous progress with FAIR.

1.1.4 Aligning on Risk

We'll delve deeper into risk frameworks in Chapter 5. For now, just recognize that we're looking specifically at loss events that occur due to the action of a *threat agent*, such as a person or a force of nature. The threat acts against *vulnerabilities*, and, if it can overcome the target's *resistance strength* (and in-place controls), the business experiences adverse *impacts*.

Figure 1-3 makes a critical point: Security program alignment to the business begins with alignment on accountability for risk and with assigning roles and responsibilities for risk management. Quantitative risk management is a core competency for alignment.

[6]"Open Group Standard: Risk Analysis (O-RA) (C13G)," The Open Group, 2014. Accessed at www2.opengroup.org/ogsys/catalog/C13G (free registration and login required)

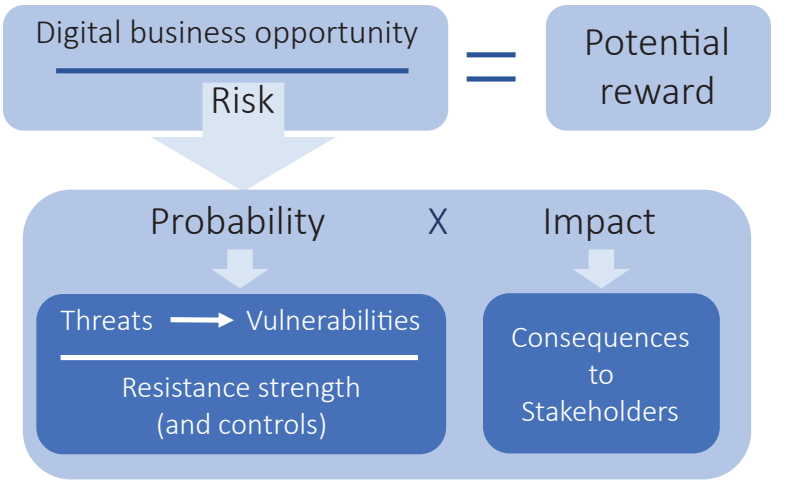

Figure 1-3. *Reward – Risk Analysis for Digital Business*

The components of information risk are

- Business information assets including tangible servers, applications, and bank accounts as well as less tangible intellectual property, reputation, or brand equity
- Vulnerabilities of information systems or assets to all kinds of logical (technical) or physical attacks or social engineering exploits against authorized users
- Threat actors
- Countermeasures or controls protecting the assets
- Potential losses to stakeholders from adverse events on the assets

Threats: Broadly speaking, some of the major threat actors include everything from criminals, hacktivists, and nation-state attackers to disgruntled insiders and to forces of nature such as hurricanes, fires, and pandemics. Even well-meaning users on your business's staff can, without meaning to, damage digital assets through errors. They may also create a breach by sharing business information with the wrong people.

Vulnerabilities: These come with the IT territory, and few systems are invulnerable. Vulnerabilities in people and process are just as common as vulnerabilities in technology. Vulnerabilities are so numerous that we must any discussion of them by calling out yet another myth.

3

The technical security department can close off all our vulnerabilities by implementing all the controls in our compliance checklist.

Cyberattacks: There's been so much publicity about hacking, malware, and so on that many people in business, or the general public, have veered from the myth that all vulnerabilities can be fixed to an opposite, defeatist extreme called out in myth #4.

4

We (or they) were hit by an advanced persistent threat (APT) and could not have prevented it.

In fact, most cyberattackers are not APTs and most exploits don't use sophisticated "zero days" or high-tech gadgets. In most cases, cyberattackers can succeed by exploiting known technical vulnerabilities and credulous users through commodity tools and age-old con artist tricks.

Countermeasures and Controls: The good news is that businesses can deploy people, processes, or tools as countermeasures to mitigate every single threat-exploiting-vulnerability scenario described. Good operational security in the form of governance, training, third-party management, and configuration management can drastically reduce the incidence of error and abuse events. On the cybersecurity side, good operational security can often deter or prevent hacking or malware from gaining a foothold. Even if a cyberattacker does compromise a password or malware does take over an computer, an organization with good security monitoring tools and processes should be able to detect the attacker and block further progress. When attackers compromise a valuable objective, the organization should have cybersecurity response processes to contain the compromise and recovery processes to restore damaged systems from backups, collect cyber-insurance, and so on.

1-2

Weave information risks into the enterprise risk map presented to executives. Engage business and IT managers to develop assumptions on potential business impacts and make security concerns more transparent to the business.

Just as business and security leaders must align on risk management (the Big Why), managers and staff down the organizational ladder must align on identifying assets at risk, their vulnerabilities, and the threats to them (the Big What) as well as security countermeasures and controls for managing the risk (the Big How).

1.2 Start the Rational Cybersecurity Journey

Earlier in the chapter, we defined information risk and discussed why digital business heightens this type of risk. And yet, many top business executives don't treat cybersecurity and risk as a top business priority even though it can, in fact, wreak havoc. Why is that?

1.2.1 Define Rational Cybersecurity for *Your* Business

According to one security leader who's worked as a Chief Information Security Officer (CISO) for almost 20 years, a lot has changed in the security space by 2020, but two things remain the same:

1. Senior executives don't prioritize cybersecurity enough for security programs to be fully effective.
2. The reason for (1) is not that executives don't care – they do, and they don't want their name in the headlines after a breach – but that they lack a clear definition of security.

Let's face it, the dictionary definitions of "security" or "cybersecurity" – as well as more technical definitions based on the confidentiality, integrity, and availability triad of security objectives – are much too vague to either give top executives a concrete sense of what could be at stake or to build a working security program.

Therefore, this book describes the process through which business and security leaders can create a state of Rational Cybersecurity – *an explicitly defined security*

program based on the risks, culture, and capabilities of an organization that is endorsed by executives and aligned with its mission, stakeholders, and processes – as follows:

- **Chapter 2's "Clarify Security-Related Business Roles"** includes a high-level Responsible, Accountable, Consulted, Informed (RACI) matrix.
- **Chapter 3's "Charter the Security Organization"** recommends creating a security charter document endorsed by the CEO and defining the security program's mission, operating principles, governance, and reporting structure.

1.2.2 Gain Executive Support and Risk Ownership

The security program will rise and fall in direct proportion to its level of executive support, the business risk owners' sense of accountability for risk, and the priority they give to security. Therefore, security leaders must work through the challenges described in the following sections:

- **Chapter 2's "Cybersecurity Not Considered Strategic"** explains that even many larger organizations don't have a CISO in place, don't consider cybersecurity strategic, and may lack enough business experience with cybersecurity on their Board of Directors to exercise effective oversight.
- **Chapter 4's "Business Executives Not Engaged at the Strategic Level"** cites research showing that although business executives have a high threat awareness, they have a low sense of mastery over cybersecurity and self-assess as not being personally or professionally well prepared.

The book provides plentiful guidance on improving security-related communications to business executives and getting top-down support:

- **Chapter 2's "Head of Security or CISO"** explains that the CISO (or Head of Security by whatever title) must act as the authoritative "champion" for cybersecurity. CISOs must continually educate executives on what they need to know about cybersecurity from the business perspective, but frame the communication in terms of business risks, impacts, or opportunities.

- **Chapter 5's "Board Communication"** offers guidelines on how CISOs can communicate most effectively with the Board of Directors.

In addition, some of the guidance on communication skills and strategies in the next section, "Align Stakeholders on the Security Program," may be effective with the C-Suite. But I can't promise that gaining executive support and risk ownership will be easy. Business executives may limit security leaders' access to them or resist good advice for any number of reasons. In the worst case:

- **Chapter 3's "Perverse Incentives"** details scenarios where top executives are blind to risk, are indifferent to risk, or pursue plausible deniability by ignoring or suppressing reports of risk.

However, in most environments where business executives are working in good faith for the good of the business, your efforts will eventually be rewarded with understanding and acceptance. As security leaders, we must play the long game, always working to increase executive support and stakeholder alignment as we pursue prioritized security projects.

1.2.3 Align Stakeholders on the Security Program

The need for the CISO to function as more of a business leader and communicator than a technologist and to align security with the business is well understood. What's less well documented is that CISOs must also lead their security teams to engage and align with the business at *all* levels, as shown in Figure 1-4.

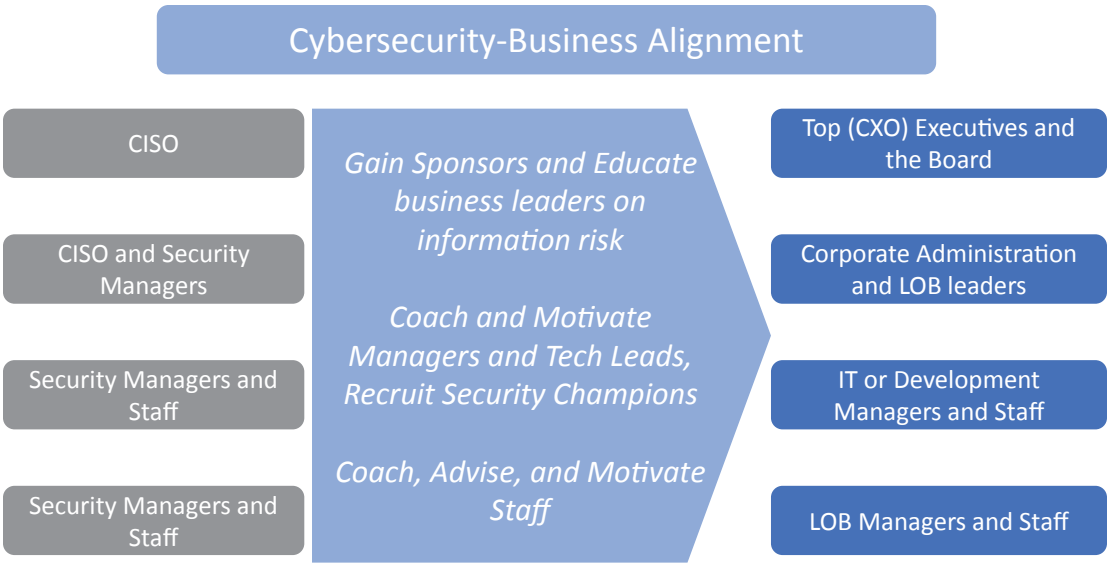

Figure 1-4. *The Cybersecurity-Business Alignment "Stack"*

Once business leaders and staff see cybersecurity for the strategic program that it is, and perceive the security team as a business partner, security leaders will be more able to count on businesspeople to perform the security-related duties related to their roles. Business risk owners can also be coached to make better information risk decisions. The book provides plentiful guidance on improving role definitions, processes, and communications in pursuit of better cybersecurity-business alignment.

Chapter 2 will define our alignment problem space as follows:

- **Cybersecurity-Business Alignment** "A state of agreement or cooperation among persons or organizations with a common security interest. It is enabled through security governance structures, processes, communications skills, and relationships that engage the business. When in a state of alignment all business leaders, staff, and security-related processes act in accordance with clear roles and responsibilities to support the security program and strategy."

1.3 Set the Rational Cybersecurity Priorities

Information risk has multiple components – too many threats to assess individually, too many vulnerabilities to patch all at once, and many choices among controls. Where to start? What's the priority? In his book "Advanced Persistent Security",[7] Ira Winkler tantalizes readers with the notion that it should be possible to get 95% of the benefit expected from a security program for 5% of the work. Winkler works in the area of security awareness, so it's no surprise he believes the low-hanging fruit grows in the field of developing a healthy security culture.

I don't disagree with Winkler about the importance of security culture and have devoted a whole chapter to the topic. But I think there are at least five other areas where businesses can take action to make the difference between a Sisyphean slog uphill to cybersecurity mediocrity versus an opportunity to quickly reduce the most severe risks and run a strong, business-aligned program for the long haul.

Can we find a way to gain 95% of the benefits for 5% of the work in cybersecurity? Or even just the proverbial Pareto Principle, aka the 80-20 rule? I think that we (security leaders) can, if we align with the business on the core Rational Cybersecurity priority areas shown in Figure 1-5.

Figure 1-5. *Rational Cybersecurity Pareto Priorities*

[7] "Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies," Ira Winkler and Araceli Treu Gomes, Syngress, 2017.

Mastering all these priorities is a long-term effort. Which one to do first, in what order, what granular controls to focus on, and how far to take the effort depends on the type of business and its process-level maturity. However, significant improvement can be made for most businesses by working on them incrementally.

Like most 80-20 rules, the Cybersecurity Pareto Priorities are a generalization to which there are some exceptions. For example, any business whose primary product, service, or mission requires intensive software development must elevate the Secure Software Development and Application Security Control Domain (see Chapter 6) right to the top of the list. Similarly, an electrical utility or gas pipeline operator must prioritize the Physical Security Control Domain. However, I'm confident that these six priorities should be top of mind for most businesses.

The following sections explain each priority and end with quick chapter overviews. The chapter overviews start with the chapter titles and summarize the chapters. The quoted text in each summary contains a partial list of section titles in each chapter and will be hyperlinked to the section if the digital book platform supports that.

The final chapter in this book – Chapter 10 – encourages security leaders to create a success plan using a worksheet I've provided. Using the instructions for the worksheet in Chapter 10, security leaders can kill two birds with one stone by reviewing the book as they create a personalized action plan with metrics on how to employ the Rational Cybersecurity guidance.

1.3.1 Develop and Govern a Healthy Security Culture

To paraphrase Winkler, a security culture is a set of customs and behaviors shared by a community, the correct practice of which minimizes the risks of being subverted or targeted for sabotage.

Too often, business leaders subscribe to our myth #1 that cybersecurity is just a technical problem to be left entirely in the hands of technical people. They don't seriously consider security and risk in their interactions with other executives and managers. This indifference weakens the business's ability to find synergistic security solutions, set ambitious goals to reduce or avoid its most serious risks, or even enforce its own security policies and compliance requirements.

On the other hand, business and security leaders and staff can treat cybersecurity as an important requirement. They can cooperate to **define what Rational Cybersecurity means for their business**. They can do this by developing a set of governance structures,

management processes, and defined roles or responsibilities which then improve security-related attitudes and behaviors at various levels of the organization.

Chapter 2, "Identify and Align Security-Related Roles": Introduces some core concepts that Chapters 3 and 4 build on to describe how businesses can develop and govern a healthy security culture**.** Chapter 2 discusses psychological and behavioral factors in the "people pillars" of cybersecurity. The following sections advise using positive messaging and creating a sense of efficacy to accomplish the following goals:

- "Earn Trust and Cooperation from Users"
- "Hire, Motivate, and Retain Key Security Staff"
- "Clarify Security-Related Business Roles"

Chapter 3, "Put the Right Security Governance Model in Place": The security-related roles discussed in Chapter 2 must be enacted in security governance and established in security policy. Chapter 3 describes trade-offs between centralized, decentralized, and matrixed security governance models. It explains security governance functions and the importance of aligning the security governance structure with the organizational structure, culture, executive intentions, and maturity levels. It also describes the components of security governance and how to optimize security governance activities. It advises security leaders on how to

- "Understand and Apply the Optimal Security Governance Model"
- "Reset (or Define) Security Governance"
  - "Charter the Security Organization"
  - "Specify CISO Reporting"
- "Institute Cross-Functional Coordination Mechanisms"
- "Manage Security Policy Libraries, Lifecycles, and Adoption"
- "Budget in Alignment with Risk and the Governance Model"

Chapter 4, "Strengthen Security Culture Through Communications and Awareness Programs": Recommends that security leaders make enhancing communication a top priority and use targeted awareness training programs both to improve security behaviors and, strategically, improve the security culture. Note that improving security culture is a two-way street, requiring "attitude adjustments" both

in the business and in the security team itself. The following sections advise security leaders to

- "Make Enhancing Communication a Top Security Team Priority"
- "Target Awareness Campaigns and Training Initiatives"
- "Coordinate Awareness Messaging with Managers and Key Influencers in Target Audiences"
- "Commit to Improving Security Culture"
- "Measure and Improve"

1.3.2 Manage Risk in the Language of Business

Simply put, risk is the core topic for Rational Cybersecurity, I wrote earlier. For business risk owners to step up to taking accountability or responsibility for information risk, they will need to understand it in business terms like time to market, monetary losses, opportunity cost, and the brand.

In their book *How to Measure Anything in Cybersecurity Risk*,[8] Douglas Hubbard and Richard Seiersen call a rigorous approach to risk management "the one patch most needed for cybersecurity." In my experience, not quite all security professionals would agree. Some dispute whether a small business, or a business in its early stages of maturing a cybersecurity program, really needs to focus on risk management to the extent of building formal processes.

"Threats are all around us," they might say. "We can't predict exactly what they'll do. Shouldn't a security program just focus on implementing a good control baseline to fix the vulnerabilities?" That's a great question, but in my view it's never too early to begin risk management, and no organization is ever too small to need it, at least at a basic level.

Risk management is a top priority even for small organizations or security programs in their early stages for the following reasons: Without enough attention to risk analysis and risk management, business leaders can't effectively assume accountability. Security leaders can't make a rational case on spending and priorities. They can't make

[8] *How to Measure Anything in Cybersecurity Risk*, Douglas Hubbard and RichardSeiersen, John Wiley & Sons, 2016

defensible arguments on which risks to accept or avoid or even prioritize which security controls to implement first within their discretionary budgets.

The risk management models and processes we'll discuss in Chapter 5 give the business the tools to determine which risks to care about and to quantify those risks in business terms such as the potential time and money impact of a breach against a new product launch or one of the business's key customers.

Chapter 5, "Manage Risk in the Language of Business": Begins by discussing how to address common challenges such as the lack of consistent information risk terminology, subjective qualitative analysis methods, and a myopic focus on controls. It recommends adopting the quantitative FAIR model within the ISO 31000 risk management framework and working with business and IT leaders to implement an information risk management program. It provides guidance for security leaders on how to

- "Establish the Context for the Risk Program"
- "Define Accountabilities, Risk Appetites, and Risk Processes"
- "Implement Tiered Risk Assessment"
- "Treat Risks Holistically"
- "Monitor Issues and Risks Continuously"
- "Communicate Risk to Stakeholders Effectively"

1.3.3 Establish a Control Baseline

To mitigate risks that could materialize into losses, businesses must establish a set of baseline controls. The optimal controls will vary for different types of businesses. The key thing to recognize is that there is some subset that your business should implement as a matter of basic security hygiene. Put another way, if any of these controls were completely absent, the business would be a sitting duck exploitable by any adversary with a room temperature IQ.

Chapter 6, "Establish a Control Baseline": Covers common challenges such as lack of a unifying control architecture or risk models and the need to avoid instituting controls out of line of the business culture. It introduces control standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the International Organization for Standardization (ISO) 27001 series. It guides security leaders to

- "Select a Control Baseline from the Essential Control Domains"
- "Serve up a Balanced Diet of Controls" (per NIST Cybersecurity Framework's Identify, Protect, Detect, Respond, and Recover categories)
- "Develop Architectural Model and Plans for Control Implementation"
- "Use a Two or Three Lines of Defense Model for Control Assurance"
- "Apply a Shared Responsibility Model to the Control Baseline"
- "Scale and Align the Control Baseline"

1.3.4 Simplify and Rationalize IT and Security

What you cannot manage, you cannot secure. A control baseline can't be fully or efficiently implemented across a chaotic IT environment. Many IT organizations have accumulated technical debt by not rationalizing their infrastructure platforms and application portfolios. A former colleague of mine once characterized IT organizations as "curators of their own IT museums." They have too many platforms, too many applications performing similar functions, and too many vendors. The systems don't interoperate unless stitched together by complex integration tools, some developed in-house but often undocumented and unmaintainable once their original programmers depart.

A large organization may have multiple business units running parts of multiple IT stacks in silos. The security issues – especially those created by the integration between systems maintained by different groups – may be neglected. Security budgets go to waste building a security infrastructure that rivals the IT infrastructure in complexity.

Chapter 7, "Simplify and Rationalize IT and Security": Shows how security leaders can, just by doing their job well, be a catalyst for IT improvement and thereby help security's cause. It advises security leaders on how to

- "Help Develop a Strategy to Consolidate and Simplify IT"
- "Learn from Digital Initiatives"
- "Provide Security for a Governed Multicloud Environment"
- "Include Security Services in the IT Service Catalog"
- "Upgrade IT Operations with DevSecOps and Disciplined Agile"

1.3.5 Control Access with Minimal Drag on the Business

Every business has rules and requirements for how information assets should be accessed, shared, or used. The business should determine these requirements based on its needs and opportunities primarily, risk and compliance secondarily, and only then based on IT constraints and dependencies. Regulations such as GDPR have made the control domains concerned with identity and access management (IAM) as well as data governance even more critical. But IAM has always been a challenging domain for businesses to master because it requires cross-functional engagement across silos from businesses that lack the maturity in security or access governance to do this well.

Chapter 8, "Control Access with Minimal Drag on the Business": Explains IAM and data governance models. It identifies challenges such as the typical organization's immaturity and/or outdated deployments. It describes a tendency for some business cultures to emphasize prescriptive rules for access and others to give staff overly broad privileges to "get the job done." It recommends that security leaders work with their organizations to

- "Balance Access Control and Accountability"
- "Modernize IAM to Enable Digital Business"
- "Take a Proactive Approach on Privacy"
- "Monitor Identity-Related Events and Context"
- "Build Up Identity, Privilege, and Data Governance Services"
- "Risk-Inform Access Management Functions"

1.3.6 Institute Resilient Detection, Response, and Recovery

According to the 2018 Verizon breach report,[9] the "dwell time" for cyberattackers or malware once having penetrated a business network was measured in "months" for 68% of breaches. As similar numbers had been reported in previous years, these reports contributed to the perception of omnipotent organized cybercriminals and nation-state

[9] "2018 Data Breach Investigations Report," Verizon, Inc., April 2018, accessed at https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

attackers always overrunning hapless defenders ("you've already been breached, you just don't know it yet" or "it's not a question of 'if' it's a question of 'when'").

Although there is some truth in these cautions, the good news is that businesses can and should aspire to keep (notionally) 98% of the attackers out of their networks, detect and eradicate most that do penetrate within minutes or hours, and at all times keep them away from the business's "crown jewels." Even top-shelf cybercriminals and nation-state operatives (the 2%) can be resisted, detected, and delayed for some time by the right set of cyber-resilience measures.

Chapter 9, "Institute Resilience Through Detection, Response, and Recovery": In addition to the "dwell time" challenge, it highlights issues with business unpreparedness for response, difficulty staffing state-of-the-art security operations center (SOC) functions, and the lack of visibility to all IT systems. It describes good practices for security monitoring in a broad sense, including processes to coordinate defense with users, business stakeholders, and external parties. It also provides guidance on how a cross-functional Computer Security Incident Response Team (CSIRT) should respond to incidents in alignment with groups such as security operations, public relations (PR), legal, HR, and (in some cases) business continuity management (BCM). The BCM team must also enable the business to recover from incidents whether they are caused by IT outages or cyberattacks. It advises security leaders on how to

- "Identify Critical Business Assets, Risk Scenarios, and Contingency Plans"
- "Detect Cybersecurity Events Consistently and Promptly"
- "Coordinate Detection with Users, Business Stakeholders, and External Parties"
- "Respond to Incidents"
- "Plan for Incident Response"
- "Establish the IR Program"
- "Evolve the IR Program for Cyber-Resilience"
- "Recover from Incidents Caused by Cyberattacks and Operational Outages"
- "Activate Business Continuity and Disaster Recovery Plans"

1.4 Scale Security Programs to your Organization Type

Cybersecurity isn't a one-size-fits-all proposition. Executives and Boards of Directors always want to know: How much is enough? What approaches to cybersecurity are right for us? There aren't easy answers to these questions; however, common sense dictates one must scale the cybersecurity effort to the kind of business one is in and the IT realities of the business.

Throughout the book, we'll use the following cybersecurity scaling factors to help guide readers' thinking about how this material applies to their own businesses:

- Size of the organization
- Complexity of the IT infrastructure
- Security pressure
- National and industry origins
- Maturity

1.4.1 Size of the Organization

As a rule of thumb, "large" organizations have more than $2 billion in revenue, "medium" organizations have from $200 million to $2 billion, and "small" organizations have less than $200 million. One can also gauge size by the number of employees. Overall headcount affects organizational complexity, security governance structures, and available resources for protection. In most cases, the larger the revenues, the larger the headcount and facility footprint of the business as well.

Larger organizations have more IT and security staff and more systems. This means that they need more security infrastructure, processes, and policies and that they have resources to manage them. This book is intended for security leaders, managers, or architects in organizations with at least two people dedicated to work on security. That is still a small business or organization, but it probably has between at least 50 and 200 employees depending on its industry and technology footprint.

1.4.2 Complexity of the IT Infrastructure

Complexity of the business itself (number of regions, lines of business) tends to increase the complexity of IT as each part of the business generates unique requirements for and may build or operate part of the IT infrastructure. We also consider

- The number of infrastructure platforms
- The number of applications
- The number of integration tools exchanging data between platforms or applications, monitoring, or applying centralized policy
- The degree to which an organization develops custom applications for its line of business

What makes one organization have "low complexity" vs. another have "high complexity?" All else being equal, organizations that customize off-the-shelf tools or services – or build new ones unique to their lines of business – are more complex than organizations that stick to standard configurations and off-the-shelf solutions. Also, an organization with many duplicate infrastructure platforms or applications (e.g., running both SAP and Oracle ERP suites) tends to be more complex than one that has standardized on a single infrastructure or application solution for each business need.

1.4.3 Security Pressure

An organization under **"high" security pressure** is one continually targeted by top-tier threats and/or subject to intense regulatory requirements or public scrutiny. Financial services, government agencies, high technology, and other businesses with high value digital assets tend to experience high security pressure, as may some critical infrastructure operators, telecommunications, energy businesses, or health care. A few organizations – such as the military and intelligence agencies – fall under **"very high" security pressure**. They must stay on constant alert for cyberattacks and often engage in offensive security measures or counterattacks not legally permitted to most other businesses. (Those scenarios aren't covered in this book.)

Organizations in retail, business services, manufacturing, and other industries may have **"low" security pressure** so long as they have a relatively low dependence on IT and are in lines of business with relatively few compliance concerns.

Organizations that don't fit the profile for "low" or "high" security pressure can be characterized as having **"medium" security pressure**.

1.4.4 National and Industry Origins

What countries or regions of the world the business operates in, where it has its headquarters and sources executive leadership, are likely to drive business culture and therefore the security culture. Chapter 4 includes some discussion on the effects of national origins and other cultural factors on the security program.

1.4.5 Maturity

In the short term, the level of maturity at a business will determine what cybersecurity measures it can successfully undertake. For example, we might not recommend advanced data governance or matrix security governance for an organization with low maturity levels.

When we scale recommendations or guidance to maturity in a few of the chapters, we'll use the cybersecurity maturity model shown in Figure 1-6. The maturity levels cited are used for my security architecture consulting practice and are like those defined by the Carnegie Mellon Institute's Capability Maturity Model. I describe the security maturity levels in more detail on my blog.[10] As Figure 1-6 suggests, the model is holistic in that as consultants we measure a capability's maturity based not just on technology but also on people and process. At higher maturity levels, we expect to see an alignment between the security, business, and IT functions; to score as "managed," a capability should be well supported by affected business leaders as well as the security organization.

Most businesses can operate comfortably with some capabilities at the "Defined" and others at the "Managed" level. Businesses with higher levels of security pressure require higher levels of maturity; the larger the mismatch, the worse for them. However, few if any need to take all their capabilities at all locations to the "Optimized" level. The required level of maturity must – like everything else in cybersecurity – be linked to risk.

[10]"How to Assess Security Maturity and Make Improvements," Dan Blum, Security Architects Partners, February 2019, Accessed at: https://security-architect.com/how-to-assess-security-maturity-and-roadmap-improvements/

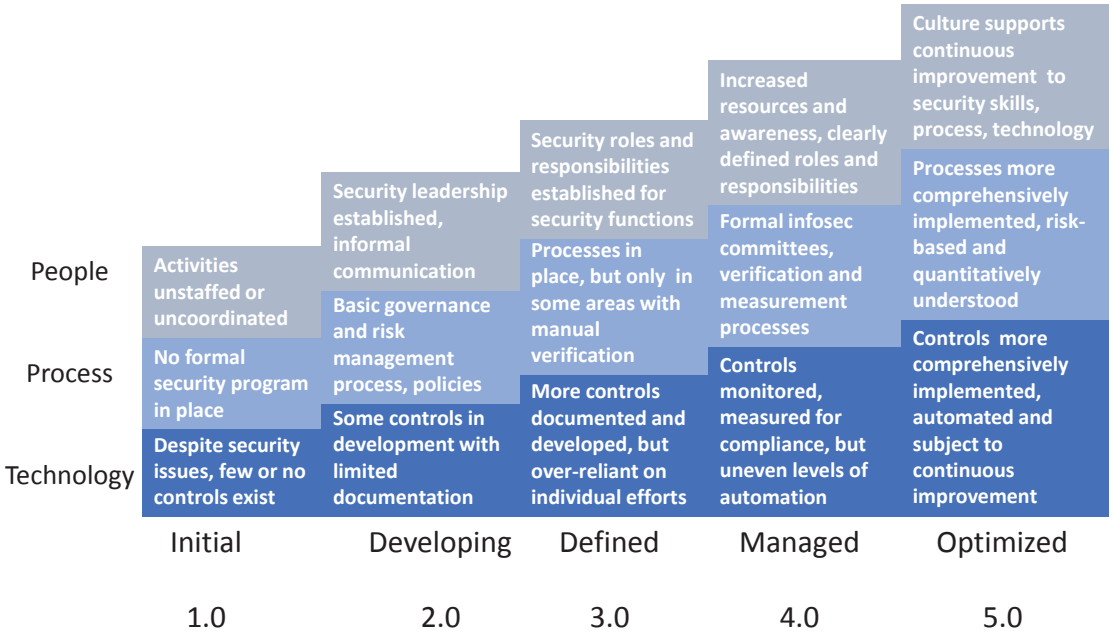

Figure 1-6. *The Rational Cybersecurity Maturity Model*

1.5 Call to Action

The core recommendations for security leaders from this chapter are to

- Establish Rational Cybersecurity; i.e., an explicitly defined security program based on the risks, culture, and capabilities of an organization that is endorsed by executives and aligned with its mission, stakeholders, and processes.
- Create shared accountability and responsibility between business leaders and security leaders as the starting point for alignment on information risks. Business leaders *own* the risks, and security leaders should *manage* risks under the business direction.

Get Started with the Success Plan Worksheet

The Rational Cybersecurity Success Plan Worksheet[11] is provided in a Microsoft Word file as a template for readers to record their progress pursuing cybersecurity-business alignment. The Success Plan uses a simple methodology with just a few steps:

1. Scope out priority focus areas (using the six Pareto Priorities in this chapter)
2. Identify stakeholders (in security-related business roles)
3. Make a quick assessment of your current state
4. Define improvement objectives (within your priority focus areas)
5. Identify metrics
6. Track progress

Scope Out Your Priority Focus Areas

The Success Plan Worksheet is structured to help readers work on improving cybersecurity-business alignment through projects related to any or all the six Pareto Priorities. Here's how to decide whether to focus on all of them or just some.

New Heads of Security, new CISOs, or CISOs with a mandate to expand or reshape the security program should consider acting on all six Rational Cybersecurity priorities. Other security leaders – such as well-established CISOs just wanting to tweak their program, part-time interim CISO caretakers, or security managers under the CISO – should primarily focus on the priorities within their own area of responsibilities or where they see the greatest gaps and opportunities.

Action

Check mark your Priority Focus Areas in Table 1, Section 1, of the Success Plan Worksheet. Although most security leaders at most businesses should not need to add additional rows, some should. If you need to, add additional rows for priorities such as "Secure our customer-facing services" to the table.

[11] "Rational Cybersecurity Success Plan Worksheet," Dan Blum, Security Architects LLC, May 2020, accessed at https://security-architect.com/SuccessPlanWorksheet

CHAPTER 2

Identify and Align Security-Related Roles

Most technical security controls, or processes, do little without people in control. Firewalls require administrators to install and configure them. Access request systems need managers to review who should have access to the target application or database. Secure software coding depends almost entirely on the coders learning the right practices and testing or scanning tools. Everyone in the business has some part to play. Therefore, this chapter introduces some core concepts that Chapters 3 and 4 will build on to describe how businesses can improve security governance and security culture.

Cybersecurity requires leadership. It cannot operate in a silo and be effective but must be aligned with many different business functions. Therefore – especially in large or mid-sized businesses – multiple business and IT leaders have security-related roles to play. The core security leadership role is often given to a Chief Information Security Officer (CISO), but strong leaders must also be in place for risk management, business continuity management, compliance, and audit. A few of those functions may report to the CISO, but others usually do not.

Cybersecurity works best when the business explicitly acknowledges its cross-functional reality and gives security leaders the resources and support structures required to be effective. Many businesses haven't got to this point. It takes an enlightened executive (such as the CEO) and/or a charismatic, determined, and knowledgeable CISO to impress this realization on the business and sometimes on his or her own staff. Thus, the security leaderships' "soft" communication skills (e.g., CISO to Board of Directors' presentations) can be just as important as their "hard" technical skills.

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8_2

In general, the security team should improve its communication skills and learn a bit of practical psychology to engage businesspeople and earn their trust. Spreading awareness of the shared mission (the definition, or Why?) of cybersecurity and clarifying security-related roles are vital. Business managers and staff can be motivated and trained to support the security program and make intelligent risk decisions, such as which vendors to work with and when to share or not share sensitive data with partners.

The chapter provides guidance for security leaders on how to

- Recognize the people pillars of cybersecurity defense
- Understand business and security-related roles
- Address common challenges
- Hire, motivate, and retain key security staff
- Make engaging the business the first order of business
- Clarify security-related business roles
- Earn trust and cooperation from users

2.1 Recognize the People Pillars of Cybersecurity Defense

A business can't run a security program by dint of the security team's efforts alone. Business leaders need to communicate the importance of supporting security to the whole organization. Table 2-1 provides a brief layout of basic security functions across the organization. The rest of this chapter goes into much more detail, breaking out these functions and how they work together.

Table 2-1. *The Broad Security-Related Role Categories Throughout the Business*

People Category	Business Leaders	Security Leaders	Security Staff	Business Staff
Job titles or roles in the business	Board of Directors, C-level and business unit executives, corporate department heads, internal audit, compliance	Chief Information Officer (CIO), Chief Information Security Officer (CISO) or other Head of Security, security directors	Security architects, security engineers, security administrators, team leads	Line of business or corporate administration managers and staff throughout the organization
Business functions	Oversee cybersecurity. Set budgets and strategic priorities	Run cybersecurity programs. Represent the business cybersecurity function internally and externally.	Design, implement, or operate cybersecurity capabilities	Build or operate LOB or business administration functions effectively and securely with the help of security staff

The security program rests on the shoulders of many people with security-related roles. These roles must be aligned. For the purpose of Rational Cybersecurity, we define alignment as follows.

CYBERSECURITY-BUSINESS ALIGNMENT

"A state of agreement or cooperation among persons or organizations with a common security interest. It is enabled through security governance structures, processes, communications skills, and relationships that engage the business. When in a state of alignment all business leaders, staff, and security-related processes act in accordance with clear roles and responsibilities to support the security program and strategy."

2.2 Understand Business and Security-Related Roles

Although security leaders head up the security function, they also report to a business leader such as the CIO or CEO. In general, top business leaders are responsible for "owning" information risks as part of enterprise risk management, overseeing the operations of security leadership, and setting cybersecurity budgets and strategic priorities for their areas.

To effectively carry out their security oversight functions, business leaders must understand the business impacts of information risk and the value of cybersecurity as a business enabler that helps organizations grow, or operate, with confidence. Business leaders set the "tone at the top" which determines whether business staff will treat security policies as mandatory requirements or as optional ones to be followed when convenient. Senior business executives must also adjudicate any disputes between the security function and business managers or staff.

Unfortunately, business leaders don't always understand what's needed for them to control and oversee the security function. After all, this wasn't on the Business School curriculum at university in the 1970s, 1980s, or 1990s when most of them got their degrees; digital businesses and organized cybercrime simply did not exist at the time.

2.2.1 Board-Level Oversight

Historically, not all business leaders understood the need or importance of cybersecurity oversight, and many considered or still consider cybersecurity as just a technical issue. Fortunately, that myth is starting to be dispelled by none other than the US National Association of Corporate Directors (NACD).

SELECTED NACD PRINCIPLES FOR CYBER-RISK OVERSIGHT[1]:

- "Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue
- Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas
- Directors should set the expectations that management will establish an enterprise-wide cyber risk management framework with adequate staffing and budget"

NACD Director's Handbook on Cyber-Risk Oversight

How closely Boards follow NACD's guidance varies regionally and by industry. Boards of many larger companies in regulated industries are formally instituting these kinds of practices. Overall, we see an increase in Board accountability and awareness for cybersecurity.

However, many Boards continue to lack the expertise or structure that would enable them to actively oversee cybersecurity. Professor James Tompkins, Kennesaw State University, performed in-depth interviews with 20 Board Risk Committee Chairs. He found that many Boards did not have a Risk Committee, did not have a formal process for categorizing and reviewing risks, and lacked the ability to quantify risks. Citing examples such as Enron's accounting and Wells Fargo's prefinancial crisis mortgages, Tompkins said, "Any major corporate scandal may be an example of poor risk oversight."

[1]"NACD Publishes Five Cybersecurity Principles Every Board Director Needs to Know," Christophe Veltsos, Security Intelligence, February 2017, accessed at https://securityintelligence.com/nacd-publishes-five-cybersecurity-principles-every-board-director-needs-to-know/

2-1

Although the Board of Directors should not manage details of security programs, it should have a good understanding of what information risks mean to the business and a committee structure through which it can set direction for risk management.

2.2.2 Chief Executive Officers (CEOs)

The buck stops with the top business executive, whether he or she is called the Chief Executive Officer (CEO), President, University Dean, Head of Agency, and so on. Chief executives are the captains of the cybersecurity ship. They can delegate to security leaders but remain accountable to the Board and general public for any serious failure.

As the number of cybersecurity breaches has increased in the 2000s and 2010s, so have the consequences for CEOs. In recent years CEOs from companies such as Equifax, Sony PlayStation, Target, Ashley Madison, and Experian in the United States resigned or were forced out after a breach. Globally, senior executives from Austrian aerospace parts manufacturer FACC, the Bangladesh Central Bank, and doubtless many others lost their positions as well.[2]

CEOs are beginning to understand they could be held accountable for cybersecurity, but many are still failing even to ensure a "defensible" cybersecurity stance for their business. In a blog post, Gartner cites eight common CEO-level failings, such as leaving cybersecurity "buried in IT" or not establishing transparent and quantitative risk management or accountability.[3]

Although cybersecurity begins with the proverbial "tone at the top," CEOs' responsibilities go beyond just setting the tone. CEOs must also address cybersecurity-related objectives with their direct reports and ensure the right people are in place and managing cybersecurity. This gives us our next key to cybersecurity-business alignment.

[2] "Cyber Security Breach CEO Retired, Fired, Gone," Ultimate Business Continuity, 2017

[3] "Keep Your Job After a Cyberattack," Susan Moore, Gartner, July 2019, accessed at www.gartner.com/smarterwithgartner/keep-your-job-after-a-cyberattack/

2-2

CEOs should think of cybersecurity as a business as well as a technical problem, oversee a sound security program by appointing an empowered security leadership, and if necessary, intervene to ensure their direct reports are supporting the security program.

2.2.3 Head of Security or CISO

Although the CEO is accountable for security, almost all technical and operational functions must be delegated due to their complexity. Therefore, in almost every sizable modern business, there is some recognized CISO, or "Head of Security" going under another title, responsible for the core security organization.

The CISO operates and communicates as the champion for cybersecurity. He or she should continuously educate executives on what they need to know about cybersecurity from the business perspective, but always frame the communication in terms of business risks, impacts, or opportunities.

In smaller organizations, the CISO may be the proverbial jack of all trades, that is, serving as the line manager for risk, operations, and more. In a large company with multiple divisions, multiple business information security officers (BISOs) may serve as liaisons to business units for the CISO or work more or less autonomously.

Important This book often uses the terms "CISO" and "top security leader" interchangeably with "Head of Security." It uses the term "security leader(s)" to refer to functions that *could* be handled either by the CISO or another security manager or staff member taking a leadership role.

Using these titles interchangeably is OK if we remember that the "CISO" title implies a "chief officer" role as well as a security role. It creates an expectation that the titleholder can represent the security program to the Board of Directors, external regulators, and other stakeholders as well as sit in on top business and IT leader meetings as a peer. Top security leaders without the CISO title *might* have similar executive visibility, but there's less of a presumption that they will.

In fact, many businesses don't have a person with the CISO title. Even among large private companies in the United States, one survey found that 38% of the *Fortune 500* didn't have a CISO and fewer than 4% of those who did listed the CISO on their

company's leadership pages.[4] Leaving aside so-called Virtual CISOs (V-CISOs), it's a safe bet that the majority of smaller organizations probably don't have a person with the CISO title and the role that it implies.

Giving a security leader the CISO title and providing him or her with the business access and visibility the role presumes comes at a higher cost than retaining just any technically qualified security leader. But businesses need a top security leader with strong business acumen as well as managerial and technical skills. I strongly recommend that large or mid-sized businesses under medium or higher security pressure as well as any smaller businesses under high security pressure formally anoint the top security leader with the "CISO" title.

2.2.4 Other Chief Executives (CXOs)

Operational executives – such as the Chief Operations Officer (COO), Chief Financial Officer (CFO), or other "CXOs" – often proxy for the CEO internally to the company. Although CEO *accountability* can't be fully delegated, the CXO may take some *responsibility* for cybersecurity oversight from the CEO. This can be successful if it is a stable arrangement and the CXO has, and is seen to have, the CEO's full backing.

The Chief Information Officer (CIO) or other "heads of IT" often report to a CXO below the CEO. Even if the CIO reports to the CEO, the position is usually one level down from the CEO's inner circle in terms of power and influence in the organization.

2.2.5 Audit, Compliance, and Other Security-Related Functions

Beyond the basic business-security leadership hierarchy, organizations have many additional security-related functions. Figure 2-1 illustrates some of these functions and their relationship to business stakeholders. The figure shows stakeholders on the outer edge of the circle closest to the functions that affect them.

[4] "Fortune 500 Faces Major CISO Challenges," DH Kass, MSSP Alert, October 2019, accessed at www.msspalert.com/cybersecurity-talent/fortune-500-ciso-challenges/

Figure 2-1. *More Security-Related Functions and Business Stakeholders*

The five additional security-related functions in the figure work as follows:

- **Risk management** plays out at multiple levels. Some businesses have a formal enterprise risk management (ERM) practice to deal with financial, market, project, business continuity, and other risks in addition to information (i.e., IT and cybersecurity) risks. ERM may be headed by a Chief Risk Officer (CRO). A large organization under significant security pressure may have a whole team dealing just with cybersecurity and IT operational risk.
- **Computer Security Incident Response Team (CSIRT)** coordinates with law enforcement, Information Sharing and Analysis Centers (ISACs), Computer Emergency Response Teams (CERTs), and managed security service providers on monitoring cyberattacks and other threat intelligence. Often part of the security organization, the CSIRT leads the response to major incidents and during those emergencies may take temporary control of security operations staff and other functions.

- **Business continuity management** works with IT operations to assure availability and reliability in the event of cyberattacks, logical or physical system failures, or errors on the part of staff. It ensures that business services comply with their service-level agreements (SLAs) to internal or external customers and partners. It develops business continuity/disaster recovery (BC/DR) plans. It oversees backup systems, and warm or cold standby data center or cloud computing capacity. It tests contingency plans that utilize the standby sites or other emergency facilities. It monitors the SLAs of the service providers and vendors the business depends on.
- **Privacy and compliance management** works to ensure that personal information is protected and that other compliance requirements are met. Recall Table 1-1 (compliance regulations) from Chapter 1; most businesses have sector-specific regulations that may cause the compliance function to work closely with security operations, business continuity, or both. The team works with internal or external Data Protection Officers as required by regulations such as GDPR for privacy. It provides guidance and tools to support compliant customer-facing sales, marketing, and operations processes. In health care, pharmaceutical, and some manufacturing operations, the compliance function must also work with internal and external quality control or safety inspectors.
- **Audit management** concerns itself with many corporate functions, including IT and security. Most regulated organizations – any large public company or university in the United States, for example – have an internal audit team. Audit management also manages the communication between business executives, IT, and external auditors. Audit is an important "check and balance" on the other IT security functions.

A large organization typically has many security, business, and IT leaders performing these functions with entire departments under them. Medium or small organizations may just have one person performing each of these functions. In the extreme case, one security officer might handle all of them.

2.2.6 Corporate Administration

Executives from corporate administration functions such as human resources (HR), finance, legal, facilities management, and sales and marketing have specialized roles to play in cybersecurity. Many organizations also have a centralized program management and vendor (or third-party) management offices.

In smaller organizations, each of these functions tends to be a small group, and the CISO (or other team members) may deal with the functional executives directly.

In larger organizations, these functions tend to contain many people. The CISO can sometimes interact with the functional executives via a security steering committee (see Chapter 3's section "Institute Cross-Functional Coordination Mechanisms"), *and* managers or staff under the CISO should work directly with counterparts to handle incidents or issues, define policies or processes, and run projects. In a decentralized business, the security team may need to work with multiple corporate administration functions distributed across LOBs.

Human resources (HR) performs background checks on new hires and has a role in onboarding all new staff as well as hiring staff for the security team. It also has oversight of or provides input and approval for the following security-related functions:

- Personnel-related security policy (e.g., for acceptable use policy or bring your own device (BYOD) policy)
- Security-related roles and responsibilities (e.g., do they comply with personnel policies, union rules)
- Disciplinary actions for security policy violations
- Incentive programs to promote better risk management or security behavior
- User awareness training content

Finance approves or manages the security budget and typically has input and approval on the following security-related functions:

- Sarbanes-Oxley Act, Payment Card Industry Data Security Standard (PCI DSS), American Institute of Certified Public Accountants (AICPA) Service Organization Control 2 (SOC 2), and other financial audits which cover internal controls

- Quantitative risk management models used for information risks
- Estimating financial risk
- Cyber-insurance policy procurement and interaction with the carrier
- Procurement of IT and security tools and services
- Vendor management or contractor management

Legal approves or manages security-related content contracts with employees, third parties such as vendors and contractors, and the participants in mergers, acquisitions, and joint ventures. It has input and approval on the following security-related functions:

- Audit, compliance, and HR-related security issues
- Breach investigations, response, and notifications
- Security policies
- Estimating liability risk

Facilities management provides physical security for business's physical plant, including offices, data centers, and other operational facilities.

Sales and marketing are on the front line, simultaneously generating revenue *and* creating information risk for the business. Marketing may have an internal communications group that can support the security team's user awareness and training programs. A public relations (PR) department within marketing needs to be engaged in security incident response.

2.2.7 Line of Business (LOB) Executives

LOB executives may function as CEOs of subsidiaries or operate departments with considerable autonomy. In private companies, they may have P&L accountability for their group or at least major responsibility for the LOB (aka business unit) strategic and operational decisions. Larger LOBs sometimes dominate the IT function of the parent organization; the CIO from the largest or most profitable business unit may even provide shared services to the others. LOBs often contain their own corporate administration functions that operate in a fully or partially autonomous manner.

2.3 Address Common Challenges

Common challenges with people and organization in cybersecurity on the business side include

- Business and security leaders working at cross-purposes
- Cybersecurity not considered strategic
- Poor coordination between security-related functions
- Security leaders struggle with stress and overwhelm
- Frustrated and under-resourced security teams

2.3.1 Working at Cross-Purposes

A core challenge in the 2020 cybersecurity landscape is that business and security leaders – each of whom has a part to play – often work at cross-purposes. This puts the business at risk and distracts from productive business operation and growth.

The illustration to the right shows a **dysfunctional situation** that's all too typical, especially for small to medium business (SMBs). Business staff may reflect the leader's indifference, and security staff may be demoralized.

In the **ideal situation** business and security leaders collaborate and cooperate to balance protection with business needs and constraints. Security leaders talk in terms of business impact and do their best to educate business leaders. Security staff try to make protection as easy as possible for business staff. Business staff reward them with cooperation.

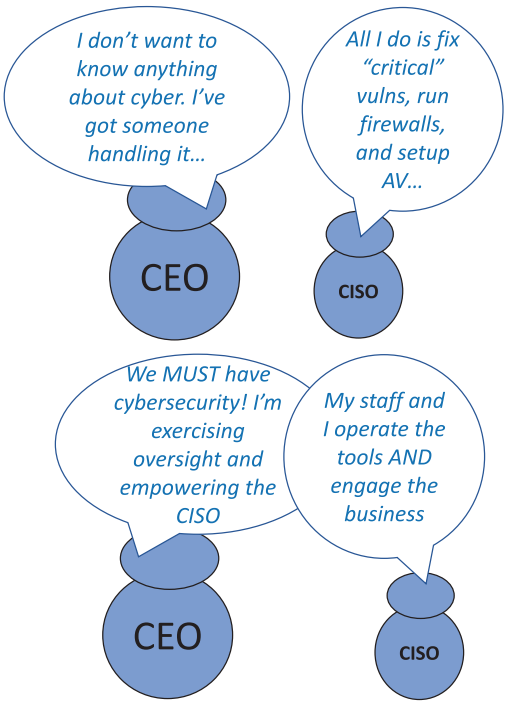

Figure 2-2. *Is Your Security Culture Functional or Dysfunctional?*

A 2017 Information Security Governance survey[5] conducted by Gartner, Inc., found that LOB executives or managers rarely (<15%) constitute the primary membership of organizations' cybersecurity governance bodies, such as an Information Security Steering Committee. Business unit engagement in developing the content of security policies that *will* affect them, such as information classification, isn't much higher. Gartner interprets such low engagement as reflective of the continuing difficulties security leaders have in convincing business leaders on the value of cybersecurity and the necessity of support from administration functions such as legal, HR, finance, and supplier management as well as LOBs.

Speaking plainly for the cybersecurity industry as of early 2020, security leaders have a sense of overwhelm, and many business leaders are disengaged. Why is that?

In their seminal book on "CISO Soft Skills",[6] authors Ron Collette and Mike Gentile teamed up with sociologist Skye Gentile to diagnose cybersecurity's core people problem as one of apathy, myopia, the struggle for political primacy, and a state of relative infancy in society's understanding of the cybersecurity space. The authors also describe security programs using system theory, in which the dysfunctional mindsets they have identified are both polluted inputs to the program and toxic exhaust from it. They pinpoint poor communication, a sense of powerlessness, and disruptive changes as being among the causes of these problems.

Often, the trouble begins at the top.

2.3.2 Cybersecurity Not Considered Strategic

Although numerous surveys and observations show increased Board of Directors and Executive concern for cybersecurity, many business leaders don't consider cybersecurity strategic. According to PwC's "Global State of Information Security Survey 2018",[7] only 44% of survey respondents say their corporate boards actively participate in

[5]"Survey Analysis: Information Security Governance, 2017," Wam Voster, Gartner, October 2017

[6]"CISO Soft Skills": *Securing Organizations Impaired by Employee Politics, Apathy, and Intolerant Perspectives*, Ron Collette, Mike Gentile, Skye Gentile, CRC Press, 2009

[7]"Global State of Information Security Survey," PWC, 2018, accessed at www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

their companies' overall security strategy. A survey of CISOs[8] by Nominet, a UK-based provider of network security services, echoes PwC's findings. Of the 460 CISOs Nominet surveyed, 65% cited the lack of senior management buy-in to the advice of security employees as a problem, and only 6% reported having ANY Board member "highly knowledgeable" about cybersecurity.

Rather than despairing at these kinds of statistics, security leaders should help raise business leader awareness. It's critical, anyway, for security leaders to cultivate the necessary communication and business engagement skills per sections "Make Engaging the Business the First Order of Business" and "Earn Trust and Cooperation from Users."

2.3.3 Poor Coordination Between Security-Related Functions

The level of commitment and experience that leaders or staff performing any of the security-related functions outside of the core security organization have also varies. In a mid-sized or large organization with high security pressure and a mature security program, it's likely that auditors, risk officers, privacy officers, and so on will be experienced, certified, and committed. In a large organization with decentralized IT or security governance, however, the security-related functions may be heavily duplicated across different business units, and staff experience, commitment, and process maturity can vary widely; in these and smaller organizations, some functions may be missing entirely or be occupied by inexperienced personnel.

As businesses become more dependent on digital technologies that blur logical/physical and social/technical lines, cybersecurity risk spills further into business functions. Like the CISO, leaders of centralized or LOB-level security–related risk, compliance, and other functions must have "soft" business and communication skills as well as technical skills as they may be called upon to perform advisory or consulting roles to LOBs. These leaders also need specialized, industry sector–specific skills.

[8] "Life Inside the Perimeter: Understanding the Modern CISO," Nominet, February 2019, accessed at https://media.nominet.uk/wp-content/uploads/2019/02/12130924/Nominet-Cyber_CISO-report_FINAL-130219.pdf

The degree of direct control that the CISO has over security-related functions outside of the core security organization varies. Some CISOs have control over all security operations and policies, others just over policy or just over operations. With the increasing complexity and uneven maturity of security-related functions scattered across the business, coordination is a major cross-functional challenge.

2.3.4 Security Leaders Struggle with Stress and Overwhelm

The Nominet survey echoed PwC's findings that cybersecurity is not considered strategic from the perspective of 460 CISOs interviewed.

SELECTED FINDINGS FROM NOMINET'S "LIFE INSIDE THE PERIMETER SURVEY"

"BOARDS STILL DON'T UNDERSTAND, CREATING JOB INSECURITY," Nominet.

CISO's surveyed believe too few board members have an in-depth understanding of cybersecurity and do not accept it's strategic importance. Although 60% of CISOs think the board understands a breach is inevitable, many expect to be fired or disciplined should a breach occur. Most CISOs remain in the job for less than 3 years.

"CISOs FIND IT HARD TO DISCONNECT AND ARE EXPERIENCING DAMAGING STRESS LEVELS," Nominet.

CISOs unanimously agree the role is stressful. Almost all live with moderate to high stress and 60% report that they rarely disconnect. "Worryingly," writes Nominet, "A quarter think the job has had an impact on their mental or physical health, with the same stating that it has had an impact on their personal and family relationships. Nearly 17% of CISOs are either medicating or using alcohol to deal with job stress."

The average CISO's job tenure is, depending on what source you believe, at best about 18–30 months. An effective CISO may tend to want to stay somewhat longer. However, according to the "Life and Times of Cybersecurity Professionals" survey from the Enterprise Strategy Group (ESG) and Information Systems Security Association

(ISSA),[9] two of the top three reasons CISOs leave are "organization does not have a culture that emphasizes cybersecurity" and "CISO is not an active participant with executive manager and/or Board of Directors."

Another Nominet report called "Trouble at the Top"[10] surveyed business executives rather than CISOs. On the positive side, the report found that executive awareness of cyber threats and a sense of breach inevitability are increasing. However, many executives still lack basic knowledge of cybersecurity and are not empowering CISOs to take charge during breaches, not providing enough financial resources, and not making CISOs (who are under stress and overworked) feel valued and supported.

2.3.5 Frustrated and Under-Resourced Security Teams

Besides the CISO, security managers and staff design, implement, operate, or oversee cybersecurity capabilities for the business. Security architects, engineers, administrators, and other security specialists also play critical roles in the business.

Below the CISO level, the stress level is likely less than detailed in the Nominet report. But other ISSA/ESG survey findings shown in Figure 2-3 are troubling.

[9] "The Life and Times of Cybersecurity Professionals," Jon Oltsik, Enterprise Strategy Group (ESG) and Information System Security Association International (ISSA), April 2019, accessed at www.esg-global.com/esg-issa-research-report-2018

[10] "Trouble at the Top: The boardroom battle for cyber supremacy," Nominet, June 2019, accessed at www.nominet.uk/boardroom-battle-for-cyber-supremacy/

Figure 2-3. *Security Teams' Frustration with the Business (Source: ISSA/ESG survey)*

A chronic global shortage[11] of an estimated 3 million skilled cybersecurity managers and staff doesn't help matters. The lack of adequate security staff and training of nontechnical employees has been found to be a leading cause of security incidents and breaches. Hiring qualified security engineers can take up to six months. In the meantime, the security team is under-resourced, and it must overwork the security staff it has or put unskilled workers on the job. When a business also has "security tool sprawl" (see Chapter 7, on overly complex IT and security environments), the problem worsens.

Only about 39% of staff security respondents from the ISSA/ESG 2019 survey reported being "very satisfied." Most are solicited by recruiters at least a few times a month in what the survey authors called "a 'seller's market' for cybersecurity talent along with salary inflation, high attrition, and cutthroat competition for skilled applicants" in which "the three-year research trend clearly indicates that organizations are not improving their ability to deal with the cybersecurity skills shortage."

[11]"Cybersecurity Skills Shortage Soars, Nearing 3 Million," (ISC)², October 2018, accessed at https://blog.isc2.org/isc2_blog/2018/10/cybersecurity-skills-shortage-soars-nearing-3-million.html

2.3.6 Crisis Conditions

I'd be remiss not to mention that as this book goes to print, much of the world's economies are partially shut down as entire states and countries seek to contain the spread of the COVID-19 virus by restricting people's ability to move or gather. This book will be read (hopefully) long after the quarantine is over, but the effects of the pandemic will likely be felt in reduced economic activity and revenues for some time.

Many of us old enough to recall the 2008 financial crises or the dot-com bust in the early 2000s well know what comes next: IT and security budget cuts. To generalize this challenge – under crisis conditions – businesses may need to find new products, services, or ways to compete in the market. Severe cost pressures may hinder efforts to work or think strategically. Even on the security team, individuals' priorities may shift from "information security" to "job security." Fortunately, these crisis conditions aren't always in effect and they will pass, but while they are here, the common challenges of security programs multiply.

Security leaders may need to sacrifice some projects, meetings, or activities once considered important. But they should not compromise on getting a clearer perspective on risks and protecting what matters. Continue to take opportunities to align with your business executives and their risk assumptions. Try to understand their concerns and how cybersecurity can be part of the solution.

2.3.7 Bottom Line

To address the challenges of dysfunctional security programs and struggling security leaders and staff, businesses will need to

- Hire, motivate, and retain security staff
- Make engaging the business the first order of business
- Clarify security-related business roles
- Earn trust and cooperation from users

2.4 Hire, Motivate, and Retain Key Security Staff

If the core security organization is not well led and staffed by motivated people, it's difficult to see how to address this chapter's list of formidable security challenges. One

hopes that organizations have a strong and motivated CISO in place. The CISO must then hire, motivate, and retain the right security staff.

According to the ISSA/ESG survey, the top factors for motivating and retaining security resources are

- An environment enabling cybersecurity staff to advance their careers
- Competitive salaries and compensation
- Business management commitment to strong cybersecurity
- The ability to work with highly skilled and talented cybersecurity staff

The following example indicates reducing stress levels and increasing the effectiveness of the security program itself are important to morale and retention.

HEALTH-CARE CISO'S STORY

"Over 2 years ago in my current role, I had to learn a lot about people and how to be a leader. When I came into the organization, there were major challenges with turnover. I had a 42% annual attrition rate before my first anniversary. I brought in a change management expert to see what was causing the problem. The expert found two primary issues:

- *No clear vision for security*
- *Staff overworked*

We worked with the department in a 9-month process to define a future state with 4 traits:

- *Risk-based rather than compliance-driven*
- *Frictionless processes*
- *Modernized access technology (aka zero trust in every context)*
- *Realization-focused culture that measures results to get the value from tools or processes*

Results are highly encouraging since putting the program in place with 7 months of 0% attrition."

Anonymous CISO

It remains to be seen whether the health-care CISO's impressive attrition improvement can be sustained over time or if other organizations can duplicate it. It seems likely that many if not most organizations will continue to have turnover. In addition to reducing the level of turnover – businesses need an active hiring program. Some recommendations for effective hiring and retention are

- Train from within to retain relatively junior security staff and provide them the opportunity to advance up the ladder to more responsible positions
- Create a "security championship" program in IT (see Chapter 7) with opportunities for transfer into the security organization
- Work with internal and external recruiters with a strong emphasis and track record for being effective at matching the business's cybersecurity needs with the right people
- Supplement scarce resource pools from additional diverse talent sources
- Reduce staffing needs where possible through judicious use of automation and outsourcing to external service providers

SECURITY STAFFING: A RAY OF HOPE?

Staffing expert Deidre Diamond cites statistics that over 70% of cybersecurity professionals are open to leaving their current employers and 89% are interested in hearing from a recruiter. "*In my experience, the root cause is almost always not seeing an opportunity to advance, due to a lack of succession plans (or career tracks), burn out from doing more than one person's job, insufficient time or budget for training, and/or lack of support or respect from leadership.*

These facts create opportunity for a hiring manager. If you are a leader that has a story about how you will take care of the people that work for you and help them develop and grow you can hire and retain if you're true to your word. If you are that leader – and you can get staff to be productive and hold them accountable through transparent expectations for roles and projects – you can hire! You can take your pick from 84% of the labor market right now because the labor market wants a better home."

Deidre Diamond, Founder and CEO of CyberSN and Secure Diversity, a nonprofit

Another major success factor to building a sense of effectiveness for the security team and throughout the business is to align security functions (inside and outside the security organization) with the various security-related business roles.

2.5 Make Engaging the Business the First Order of Business

To increase business engagement with security programs, leaders on both sides of the aisle who "get the picture" should work together to spread the meme that "business leaders own the risk, security leaders provide the tools to manage it."

As I see it, CISOs often have two related engagement challenges to overcome:

1. Getting chief executives to consider cybersecurity more strategic and prioritize it
2. Clarifying security-related roles and responsibilities

RISK MANAGER'S STORY SHOWS CYNICISM IS ALIVE AND WELL IN OUR PROFESSION

"Increasingly its politics. The further up the chain the more dysfunctional risk management gets. British Petroleum CEO Tony Hayward was elected by the Board after proposing to cut costs. He politically screwed with risk management and that may have been a precipitating factor in the disastrous Deepwater Horizon oil spill.

The Risk Officer watching these things happen can only document, escalate, and try to get executives to sign a Risk Acceptance memo. During the credit crunch, the only thing that saved ***me*** *at the Fund Company where I worked was asking the following question in writing: 'What do we have for margin calls?'* ***As for CISOs, they can align with the ISO 27000 methodology, even just a lean version of it. Nobody will fault you for trying to do the right thing.****"*

Anonymous Risk Manager

Making cybersecurity strategic: Suppose you're a CISO, or on the CISO's management team, in a business whose executives don't consider cybersecurity strategic. You believe that the too low priority on security significantly blocks you from

doing the work that needs to be done. Then, as a diligent professional who wants to be effective, you have two choices:

1. Stand on the position that you're diligently identifying the risks and implementing the controls that you're budgeted for.
2. Become an agent of change.

I would suggest CISOs take both these choices; do the work that you can do in the organizational climate while protecting your career, but also make efforts to change the climate for the better. To gain mindshare, CISOs can try to get more of the security and risk message in front of Executives and the Board. Seek auditors, third-party assessors, and external Board–level speakers who are known for advocating a more active Board role in cybersecurity and a strong executive tone at the top.

CISOs can also pursue either a low-key or overt organization change strategy. At the low-key level, keep doing what CISOs should do anyway:

- Create a sense of urgency by identifying cybersecurity's many risks and opportunities.
- Look for support from business mentors and key influencers in the executive ranks.
- Develop and sell a cybersecurity vision and strategy.
- Engage with LOB leaders or their direct reports in security-related roles. (In larger businesses, the major LOBs tend to have their own business information security officers (BISOs) as well as finance and legal executives.)

For additional communication tips and advice on security culture change strategies, see Chapter 4.

2.6 Clarify Security-Related Business Roles

Part of the security leaders' job is to work with the business to clarify their own, and business leaders', security-related roles. Security leaders should work to increase buy-in from executives and also endeavor to push the cybersecurity message down and across the ranks.

Security-related roles should be formalized in security policy and reinforced through awareness, training, and communications programs. Although in an ideal world business and IT leaders or staff would comply with all security policies, they often don't. However, security leaders can follow up with business leaders to ensure they understand and buy into policy. Clarifying security-related roles in itself gets business and security leaders much more engaged. See Chapter 4's section "Or Your Best Opportunity?" for a vision of what it looks like when the players understand and fulfill their security-related roles in a healthy security culture.

"Take away the places where apathy likes to hide. Nothing eliminates the 'It's not my job' mentality faster than clarity of definitions, roles, responsibilities, and milestones."

Source: *CISO Soft Skills*

Use Responsible, Accountable, Consulted, Informed (RACI) matrices; they are useful tools for creating better role definitions. Even if policies don't actually contain a RACI, they can be more effective if they contain the kind of specific role information a RACI provides. Moreover, business and security leaders can take already-existing RACIs from the COBIT 5[12] standard and scale or adapt them to the needs of the business.

As an example, Table 2-2 provides a RACI for the four highest-level risk and security management practices discussed in Chapter 1, where you'll recall establishing business ownership for risk is a major emphasis. This RACI clarifies the roles that security, IT, corporate administration, and other business leaders should have for managing business value, risk, the security program, and security operations.

[12]COBIT 5, International Systems Audit and Control Association (ISACA), 2012, available to ISACA members at https://cobitonline.isaca.org/about

Table 2-2. *Responsible, Accountable, Consulted, Informed (RACI) Matrix*

Management Practice	Board of Directors	Corporate Executives	Chief Digital Officer	LOB executives	Chief Risk Officer	CIO	CISO	Human Resources (HR)	Compliance and Audit	Security Ops Manager	EA/ARB	CTO/Dev	IT Operations	Service Manager	Security Incident Response	Business Continuity
Maximize IT business value	A	R	R	R	I	R	I		C		C	I	I	I		
Ensure risks are managed	A	R	I	R	R	R	C	C	C	I	C	I	I	I	I	I
Manage security program		C		C	C	R	A		C	R	I	I	I	I	C	C
Manage security operations				I	I	C	A		C	R	I	C	R	R	R	I

This RACI is loosely based on the role assignments from COBIT 5's Evaluate, Direct, and Monitor (EDM) and Align, Plan, and Optimize (APO) practices to Ensure Benefits Delivery, Direct Risk Management, Manage Risk, and Manage Security. I have simplified the COBIT roles somewhat to scale the discussion for mid-sized as well as larger businesses. Even so, many businesses won't have *all* these roles. That's OK. Focus on the ones you have.

2-3

Understand and get general agreement on which persons or departments fulfill security-related roles. Describe security-related roles and responsibilities in policy as a starting point for security governance.

Now that we've covered some of the CISO's top priorities for engaging the business leadership, we'll turn to the challenge of engaging staff or users. We'll also come back to the topic of working with business and IT leaders on security alignment to IT, security culture, and security governance at more depth in later chapters.

2.7 Earn Trust and Cooperation from Users

(Nonsecurity) business staff members and managers (aka users) also have security roles to play. Users should follow the business security policies, such as those for password and credential management, or acceptable use of business resources. They should exercise caution in their daily interactions with email, web browsing, and the Internet to avoid contracting malware on their PCs or smartphones.

As emphasized earlier, it is important for security leaders to gain top executives' support and to formalize security-related roles and responsibilities in security policy. The goal is to get IT or business managers and staff to always follow the desired security policies or practices.

But some policies are more clear-cut than others, and sometimes it's difficult for the user to judge whether the policy applies. For example, sales staff must understand whether a particular product plan is confidential or not and what is the information classification policy, or else they are likely to share product plans with prospects to make the sale they are incentivized to make for the benefit of the business.

When an IT or businessperson doesn't understand what the policy requires in a complex, real-world situation, will they ask the appropriate security, compliance, or corporate administration team for guidance? Very often, the answer is no. But if they believe the security team has their back, that it is looking for ways the businesspeople can get the job done with less risk, then they're more likely to ask. Security teams can increase the likelihood businesspeople will come for guidance by earning their trust and cooperation.

As a security leader, you must understand the users' perspective. Going about their day-to-day business, users have a job to do and that is their priority. Studies (such as a behavioral economics experiment[13] simulating bank account login, strong authentication, and risk of losing money to cyberattacks) have found that more than 50% of participants make rational (e.g., utility optimal) decisions on how much of their personal time to spend reducing an expected amount of security risk.

Security professionals at *all* levels must "communicate effectively" and with a "sense of efficacy." Treat users as the rational and supportive team members you need them to be. That could mean explaining *why* they should always follow the policy without question, or how to calculate the risk and decide, or the importance of escalating the question. Explain the risk as best as possible in terms of the users' business function and the reason why it is important to follow the policy or accept other security requests and tasks. Send positive messages that by following the security team's recommendations, users can make a real difference to their personal security as well as the business's cybersecurity posture. Chapter 4 provides more guidance on user awareness programs.

[13] "Dancing Pigs or Externalities? Measuring the Rationality of Security Decisions," Elissa M. Redmiles, Michelle L. Mazurek, and John P. Dickerson, University of Maryland, 2018, accessed at https://arxiv.org/pdf/1805.06542.pdf

A CYBERSECURITY MEETS HUMAN NATURE STORY

Language is key. In an article for Educause, Jessica Barker argues that fear-based messaging puts security leaders on the wrong side of five mental heuristics: social proof, the optimism bias, the psychology of fear, the stereotype threat, and self-efficacy. In phishing tests, for example, Barker writes: "Do you say that 30 percent clicked on the link (bad!), or do you say that 70 percent did not click on the link (good!)…Next time, join your colleagues in being part of the majority."

Given research that 80% of people are wired toward being optimistic, no matter how many dire statistics are thrown at them, many will believe the dire impact will not happen to them. "*While using a tone that is more optimistic and more empowering, cybersecurity professionals can tell people: 'The threat is real, but you can do a lot of things that are quite straightforward and that will bring the threat down to a great degree.' Even though optimism is generally more powerful than facts, when people feel that there is a point to changing their behavior, that they can actually make a difference [i.e., be efficacious] in their level of cybersecurity, they are more likely to engage in the behaviors we recommend.*"

Jessica Barker, Chair, ClubCISO from "The Human Nature of Cybersecurity"[14]

2.8 Call to Action

The core recommendations for security leaders from this chapter are to

- Develop strong business communication skills in the security organization.
- Actively work to hire, motivate, and retain security staff.
- Endeavor to engage the business and to elevate the level of cybersecurity discussions. When necessary, become an agent of change.

[14]"The Human Nature of Cybersecurity," Jessica Barker, Educause, May 2019, accessed at https://er.educause.edu/articles/2019/5/the-human-nature-of-cybersecurity

- Rather than using technical or fear-based messaging, convey a sense of efficacy ("we can do this") and partnership to earn trust and cooperation from the business.
- Work to get business leaders' security-related roles clarified in security policy and clearly understood.

Identify and Prioritize Stakeholders to Align With

Section "Clarify Security-Related Business Roles" and Table 2-2 contain a list of typical stakeholder roles. In a small business, some of the roles may not exist and others will be combined in a few people. In a large business, multiple people may fill some of the same roles across business units.

The Rational Cybersecurity Success Plan Worksheet[15] provides a structure for security leaders to identify stakeholders to align with. Depending on the size and complexity of the business, and a security leader's priority focus areas, it may be necessary to prioritize relationships with many stakeholders or with just a few covering the priority focus areas.

Action

Fill in the name of the person holding each role identified in Table 2 of Section 2 in the worksheet. If a role doesn't exist or is called something else at your organization, then remove, edit, or annotate the row. In the Contact Plan column, note whether the person should be contacted now or later and who will be the relationship manager (i.e., you or someone else from the security team). Fill in the Topics to Cover column with any known issues, projects, or pain points to cover with the stakeholder.

[15] https://security-architect.com/SuccessPlanWorksheet

CHAPTER 3

Put the Right Security Governance Model in Place

Just as a Constitution sets forth how to govern a nation, security charters and policies can formally define security-related roles and responsibilities for a business. Security governance is a set of processes and capabilities operated jointly by security and business leaders. The combined leadership manages cybersecurity risk, policy, budgets, and reporting to executives or stakeholders.

When security governance is well defined, the CISO has the right balance of authority and responsibility. Business and security leaders can handle security issues in a collaborative manner. Executive security steering committees, or forums, enable security and business leaders to align responsibilities and projects or resolve issues.

This chapter contains recommendations on how security leaders can

- Address common challenges
- Understand security governance functions
- Understand and apply the optimal security governance model
- Reset (or define) security governance
- Institute cross-functional coordination mechanisms
- Manage security policy libraries, lifecycles, and adoption
- Budget in alignment with risk and the governance model

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8_3

3.1 Address Common Challenges

Failures of business and IT teams to engage in the security-related activities relevant to their security-related roles are often failures of security governance. Perhaps the security function in the organization isn't structured right, or the security policy doesn't reflect the business priorities. Symptoms of security governance model challenges, or lack of maturity, include disengaged business units and perverse incentives for the security program.

3.1.1 Security Governance Model Not Aligned with Organizational Structure or Culture

I've seen three basic types of security governance models: centralized, decentralized, and matrixed. Which one is optimal? Generally, the model should align with the way that the business itself is governed and/or the way it provides IT services. For example, if the business has subsidiaries each operating their own IT fiefdoms, security cannot be fully centralized.

Many medium and large, complex organizations are tending to become more decentralized in the age of the digital business. To fulfill enterprise security requirements, they tend to need some form of matrixed security governance. For example, a CISO might provide overall security leadership, while operations are farmed out to IT groups in various business units. The CISO position itself could report to IT, or it could report to another executive business function such as the CEO or the Chief Risk Officer (CRO). There are advantages and disadvantages either way, and the right answer must be aligned with the business and IT culture and any operational or regulatory requirements.

Friction with business units can result from having the wrong security governance model, and security-related activities become more difficult to accomplish.

3.1.2 Lack of Security Governance Maturity

As we'll see in the section "Understand and Apply the Optimal Security Governance Model," a matrixed model is often the best solution for a complex organization, such as a multinational company. However, operating matrixed security governance requires more sophisticated (or mature) security management committee structures, cross-functional alignment, and security policies. Without the maturity, matrixed governance may fail to govern.

3.1.3 Security Leadership Disengaged from Business Units

In Chapter 7, we identify digital business and cloud-first strategies as trends that tend to weaken business unit engagement with traditionally minded IT departments. The security organization may be tightly embedded under an IT department riven by technical debt and hollowed out by shadow IT. Business units are rapidly adopting cloud solutions, and the overall IT environment is becoming more decentralized. Cybersecurity still is, and should be, a management concern, but the security department may have no room to maneuver because of any (or all) of these reasons:

- The security leadership lacks credibility, or it is discouraged from engaging LOBs to support their initiatives.
- No matrix governance structure exists to engage LOBs.
- The security organization is swamped with the work of protecting the shared IT environment and legacy core applications. It has no bandwidth or mandate to support LOBs.

As described in Chapter 7's section "Discern the IT Strategy and Align the Security Road Map to IT," security leaders can take advantage of the inherently cross-functional nature of security to work with IT to develop IT and security strategy, align security priorities with strategic platforms, and engage with LOB initiatives.

However, the security governance function may need a reset (see the section "Reset (or Define) Security Governance" in this chapter).

3.1.4 Perverse Incentives

Even when business leaders are aware of cybersecurity issues, they are often subject to perverse security incentives. It's possible for business executives to place such strong demands on staff for secure outcomes that they create a perverse incentive for insecure behavior. A former financial services company CISO we interviewed (who prefers to remain anonymous) recalled that "The business and security staff at my employer from the Chief Counsel on down were more afraid of the CEO and the Board reaction to regulatory reports than they were of breaking the law."

> "Ironically," our ex-CISO colleague continued, "I don't think the executives were even conscious that they were pushing staff towards making false reports. As far as they were concerned, they'd put security first. They'd granted the full budget we asked for."

This is a tough challenge! More alignment in top-level thinking will probably be needed to pull off a successful security governance reset. Security leaders who choose to stick around and face the challenge can take a leaf out of the "crucial conversations"[1] book I keep out on my office reading stack; it provides useful scripts to prepare for difficult discussions. It could also be helpful to engage an executive change management consultant or another senior mediator.

3.2 Understand Security Governance Functions

What does security governance govern or do? Its main functions are to

- **Charter or mandate the security program:** Define "security" or "cybersecurity" for an organization in terms of its mission, governance, reporting structure, and operating principles. Formally specify which organizations or roles within the business have authority over security strategy, policy, projects, budgets, committees, and operations.
- **Manage, control, and report on risk:** Identify, track, manage, and report information risks to the executive level along with other enterprise risks. Ensure the security strategy and project portfolio are aligned with business risks and risk appetites.
- **Coordinate security projects and manage issues:** Set up, sponsor, and chair forums engaging multiple stakeholders including the CISO, CIO, CRO, head of audit, and LOB executives critical to the success of projects and processes. Mediate issues escalated to the business cybersecurity governance level.

[1] "Crucial Conversations: Tools for Talking When the Stakes are High," Patterson & Greeny & McMillan & Switzler, McGraw Hill, 2012

- **Manage security policy:** Work with the business, IT, and other areas to develop security policies, standards, processes, and procedures; gain agreement and formal adoption; and manage the policy lifecycle.
- **Allocate security budgets and resources:** Decide how to pay for security program capital and operating expenses (CAPEX and OPEX). Allocate funds and resources to the security organization and other groups responsible for delivering security projects or services. Approve proposed budgets and major expenditures.

3.3 Understand and Apply the Optimal Security Governance Model

The security organization is just one organization in the business. It must work with executives, IT, development, corporate administration, and LOBs. As discussed in Chapter 2, many security-related roles must be carried out by business leaders and staff outside the core security organization.

The security governance model, or structure, defines the way the security organization and the security program relate to the rest of the business. There are fundamentally three security governance models:

- Centralized
- Decentralized
- Matrixed

Any of the three models can work if applied in the right way in the right place. However, in some cases security governance structures result more from happenstance and personalities than from well-thought-out organizational thinking and thus may not be properly aligned with the business culture. Figure 3-1 shows the three models and the way that each of them can thrive.

Figure 3-1. *The Three "Pure" Security Governance Structures*

3-1

The security governance model should generally follow the IT organizational structure unless management supports the notion that security should act as a matrix function over decentralized IT units. Both security and IT governance models should align closely to the business culture or management intentions for the culture.

3.3.1 Centralized Models

In a centralized security governance model, one person or department makes all the important decisions, controls operations, resolves disputes, and sets the strategy and the budget for security. Responsibilities can be delegated but managers still report directly to a single leader who serves as a central authority. Centralized governance with strict hierarchy is typical of military and often civilian government and some corporate organizations.

CENTRALIZED NETWORK SECURITY GOVERNANCE STORY

I was subcontracted recently to perform a network segmentation architecture for a large financial services company in the United States. In the first draft of our current state analysis, my engagement partners and I noted the company needed better processes for making security zoning more risk based. However, the client told us risk management was out of scope; network security should be based on prescriptive rules only. We learned that the CISO of this company has a legal background and runs security "very much behind the door."

That is, risks and high-level decisions about them aren't generally discussed in a transparent fashion even within the security organization itself.

This kind of centralized security governance model is suitable for some security cultures and industries. But outside of those, it may face challenges as digital businesses become flatter, more decentralized.

3.3.2 Decentralized Models

In the decentralized model, multiple organizational units operate security programs independently. This is common among multinational organizations or businesses that have grown by acquisition. Each organizational unit in this model has its own security team.

The decentralized model doesn't preclude the business from requiring units to coordinate on developing shared services or from following some common standards. But if a decentralized organization has a CISO at the enterprise level, this CISO will tend to be in a weak position. Don't be fooled by the "Group CISO" title you sometimes see in this case. In the decentralized model, each line of business (LOB) manages IT and security according to its own needs.

STORY OF CONSENSUS-BASED STANDARDS IN A DECENTRALIZED IT ORGANIZATION

In the early 2000s, I worked with a team of consultants to help a large pharmaceutical company develop a network architecture and, later, an identity and access management (IAM) architecture. These turned out to be large projects with high visibility because the company governed IT through a biweekly half-day CIO council meeting. The executives would come together as equals and decide on standards to make their autonomous systems work together. We spent a few months on each project facilitating consensus with extended teams of architects from the different units. Ultimately, the CIO council approved the architectures.

3.3.3 Trade-offs

If we were to imagine a continuum between highly centralized and decentralized security governance models, we wouldn't have to go too far toward either extreme before seeing issues and disadvantages.

Too centralized means rules for security governance may be too rigid. Some LOBs need more flexibility and, in the end, may not cooperate with security strictures. Too decentralized and LOBs will likely duplicate security efforts (or make inadequate efforts) creating inconsistent security controls that make it hard for the business to respond coherently to common threats or compliance requirements.

STORY OF DECENTRALIZED FIREWALLS PUTTING A UNIVERSITY AT RISK

In early 2015, I worked on a security assessment for a large US-based university that did not have a centralized firewall infrastructure. Each of more than 50 colleges and other units had its own firewall; without a core network security competency, many of the firewalls were found to have an insecure configuration, and some were beyond product end of life.

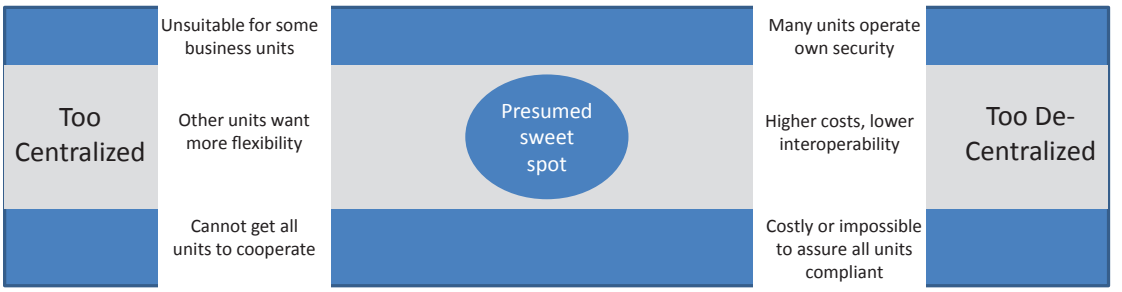

Figure 3-2. *Trade-offs Between Centralized and Decentralized Models*

Given the trade-offs between centralized and decentralized models, organizations often turn to the matrix model in search of a sweet spot.

3.3.4 Matrix Models

Matrix security governance structures can coordinate the management of cybersecurity for very large organizations. Figure 3-3 illustrates an example that operates governance at four levels.

- Lines of business and IT services
- Cross-functional working groups
- Executive committees
- Board (and executive-level) meetings

Let's decompose how the matrix works at each level.

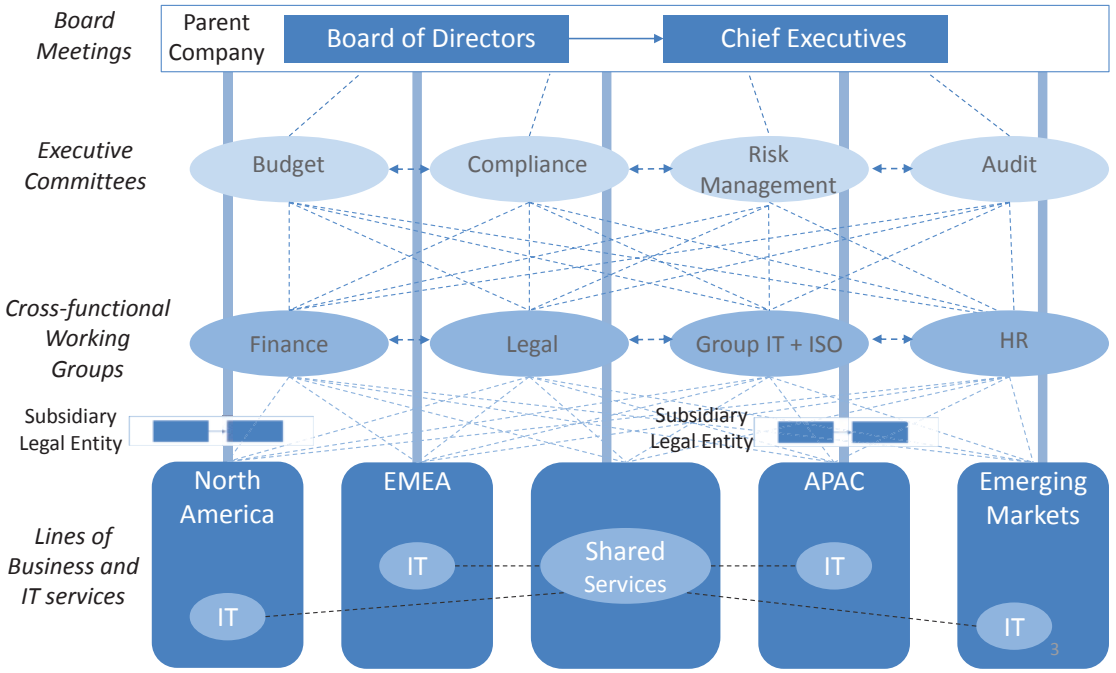

Figure 3-3. *The Matrix Model*

Lines of business and IT services: At the lowest level, LOBs or regions in Figure 3-3 run their own IT functions; however, some commoditized services such as email systems and endpoint anti-malware may be shared. LOBs and regions may also use cloud computing services from diverse vendors.

More strategically in the matrix model, local business units can plan for future iterations of the applications and shared services they need. They may share in the costs for shared services. There may be representatives from the CISO function on liaison to the business units, or business unit staff may have a dotted line responsibility to the Group CISO.

Cross-functional working groups: Moving up a level, matrixed organizations typically have an enterprise CISO and CIO function, for example, a "Group CISO." However, larger business units beneath them may also have CISOs. Note that the diagram is drawn to put the Group CISO and CIO together for graphical convenience and is not meant to suggest this reporting structure is universal. Exact titles vary between companies, as do reporting structures.

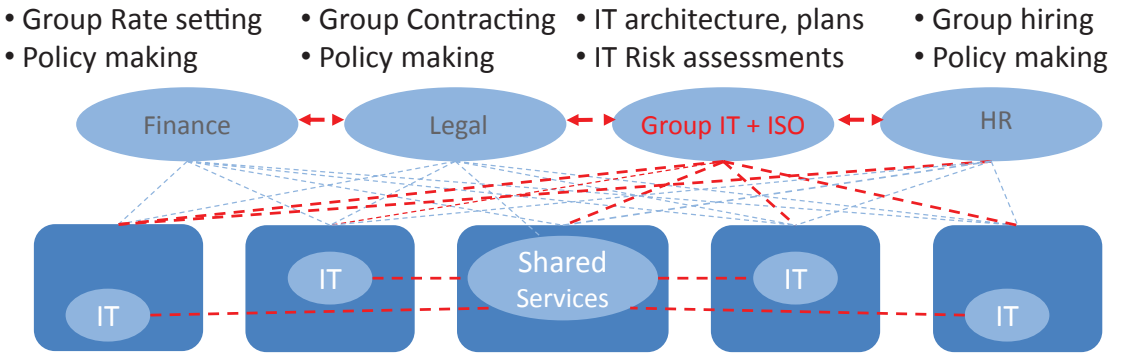

Figure 3-4. *Cross-Functional Working Groups*

The Group CISO/CIO organizations provision and protect the shared services. They continually interact with the local functions to enable, approve, or coach the lower echelon security management. The Group CIO manages the architecture and operations for shared services, and either the CIO or CISO manages security services or security components of shared IT services.

Executive committees: The Group CIO and CISO also interact on a peer-to-peer basis with the heads of business administration, that is, HR, legal, and finance, to address share budgeting and procurement processes. Cross-functional working groups may exist permanently or form temporarily to undertake major risk assessments, approve changes, or develop new architectures. The executive committees report up to the Board and executive levels. For complex organizations - such as multinational corporations with subsidiary legal entities - multiple layers of reporting may be required.

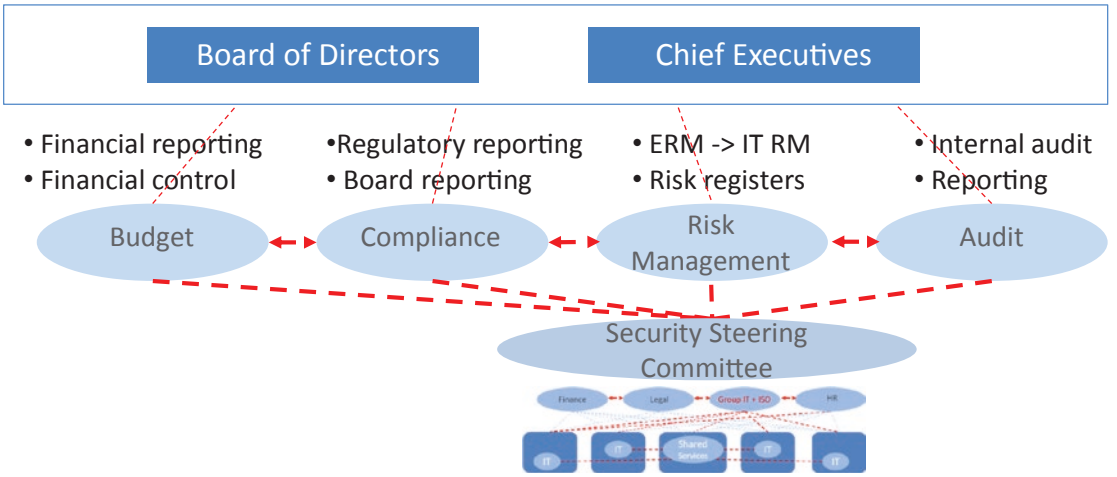

Figure 3-5. *Cross-Functional Working Groups, Executive Committees, and Executives*

As with the centralized governance model a security team or department reports to the CISO. But in the matrixed model, some members of the team may work for other functions but have "dotted line" reporting to the CISO.

In general, matrix structures require well-articulated cross-functional and cross-divisional roles and working groups, processes, accountabilities, and lines of communication and control. Key questions: Is the matrix structure well designed or not? Does it suit the organization's culture?

Operating a matrix organization is challenging precisely because of the cross-functional dimensions. Research suggests that most cross-functional teams are dysfunctional.[2] Why then do so many organizations adopt the matrix model and then struggle with it? The answer: Once an organization gets to a certain size, or a certain level of complexity, there may not be an alternative. Perhaps, for large or complex organizations, one might repurpose an old joke about democracy: "Cross-functional governance is the worst form of governance there is except for all the others."

[2]"75% of Cross-Functional Teams Are Dysfunctional," Behnam Tabrizi, *Harvard Business Review*, June 2015, accessed at https://hbr.org/2015/06/75-of-cross-functional-teams-are-dysfunctional

Another interesting point: Many matrix governance structures are not pure; they don't look like those in Figure 3-3. Organizations often have hybrid or composite governance models. An organization with composite governance could be decentralized as a whole but contain one or more large lines of business that operate in a centralized or matrixed manner. Each LOB might be large enough to form an enterprise. Corporate conglomerates and large national or state governments often have composite governance.

3.4 Reset (or Define) Security Governance

If business units aren't fulfilling security-related activities, or if the security leadership itself isn't aligned across an organization, a security governance "reset" may be required.

A well-defined security program should have a charter documented as security policy and approved by the CEO, a security policy library, and a security governance function scaled to the business's size and circumstances. The governance structure should operate at maturity Level 3 or higher. Security leaders at businesses without these process artifacts, operating below Level 3, or experiencing some of the common challenges can directly use this chapter's recommendations to reset the program. Security leaders at businesses with more mature security governance can check their status against the governance practices described herein and use this guidance to fill any gaps.

3.4.1 Choose the Appropriate Security Governance Model

Occasionally businesses just decide "we're going to have centralized, decentralized, or matrixed IT or security" and then have a big reorganization. More often, one of those structures simply results from how lines of authority and decision rights are allocated over time. Nevertheless, understanding which governance structure a business has vs. which structure it should – perhaps – have is a useful thought exercise.

Security leaders rarely if ever get to choose the governance model themselves, but they should always be ready to discuss the matter intelligently. Which is the right security governance model: centralized, decentralized, or matrixed?

Most small organizations can use a centralized model and most large ones should make some attempt at formal or informal matrixed governance. But it would be a cop out to stop at that, because there's much room for variance with different businesses. The decision tree in Figure 3-6 provides a more nuanced answer than "small equals centralized, larger equals matrixed" by using criteria based on the structure and maturity of the business.

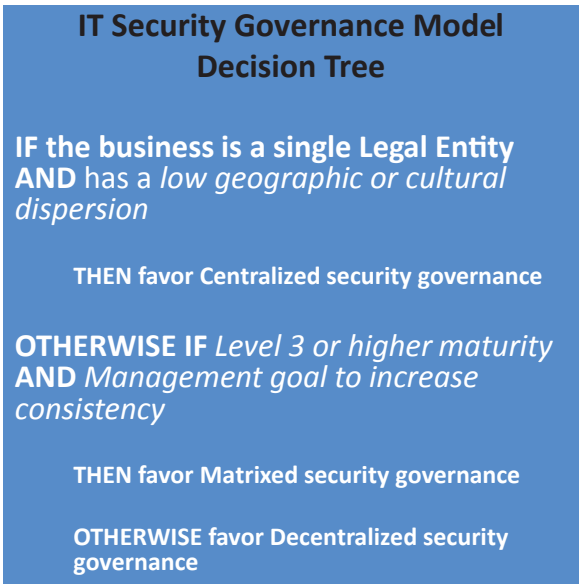

Figure 3-6. *Choosing a Security Governance Model*

Per the decision tree, a small organization or a large one with a hierarchical and relatively homogeneous structure (and culture) might go the centralized route for greater control and efficiency. A larger, more complex business tends toward decentralization; however, if management seeks to drive greater consistency and control, it can push toward the matrixed model as IT and security programs gain maturity. Any decentralized security arrangements should be buttressed with clear accountability for all security leadership and operations functions.

3.4.2 Charter the Security Organization

The business should specify the security program mission and define the program's lines of authority and decision rights in a security charter document. The security charter document contains the business's definition of security and of the security program. It must also identify how the security organization coordinates with the business and how it relates to audit, compliance, risk management, and other functions.

The charter should be a short, plain language document intended for broad consumption. It should be signed by the organization's CEO or equivalent position to give it the gravitas to serve as the business mandate and the foundation component of the security program. It should define security for the business by describing the security

program's mission, operating principles, governance, and reporting structure. For example, the security program's mission statement could describe security objectives including confidentiality, integrity, availability, safety, and privacy in terms of the business's specific high-level goals and requirements. The charter should also reference core governance principles; the following is a short sample

- The Board of Directors (BOD) and CEO (or BODs/CEOs in a legal entity with subsidiaries) are accountable to the public for risk.
- Business leaders are ultimately accountable to the CEO(s) for risk in their LOB or administrative function. Executive leadership sets the risk appetite and thresholds for the organization.
- Business leaders delegate security operations and incident response to security leaders and rely on security leaders to advise them on cybersecurity risk.
- Compliance to all applicable regulations must be the logical consequence of an effective risk management framework and program of internal controls.
- Operations, assurance, and audit functions are organized to provide three lines of defense (see Chapter 6, section "Use Two or Three Lines of Defense Model for Control Assurance").

Security is everybody's business according to their role. While avoiding specific job titles, the charter and subordinate policy documents should spell out the accountabilities and responsibilities for cybersecurity for general business roles such as

- Executives and business risk owners
- Risk, compliance, and audit functions
- Security program executive sponsor
- Security management and staff
- Asset or data owners and data stewards
- All staff

The charter should call for establishing a cross-functional coordinating committee (aka security steering committee) as a security governance forum for business, IT, and security leaders to authorize and oversee major security projects, budgets, and changes.

The charter should also define the security policy hierarchy. Few or no details are required in the charter itself other than basic scoping of the committee's basic makeup and purpose.

The charter explicitly defines the security governance model. It can specify whether the organization shall have a security leader with the CISO title. It can also specify where the CISO or security leader reports and the scope of responsibilities. The following guidance is intended especially for businesses that have formally appointed a CISO in a corporate officer position.

3.4.3 Specify CISO Reporting

Per Chapter 2's section on the "Head of Security or CISO," the "CISO" title sets an expectation that the security leader can represent the security program to the Board of Directors, external regulators, and other stakeholders as well as sit in on top business and IT leader meetings as a peer. Where a security leader, or CISO, reports in the business hierarchy is also an indicator of whether he or she is empowered to drive a cybersecurity program for the business.

In my experience, most CISOs – at least half – report to the CIO. Strong arguments can be made that this is a good thing, for if the CISO is responsible for IT security, shouldn't the position associate closely with IT? However, many security experts argue against putting the CISO too low in the organization chart or against creating a potential conflict of interest between security and a CIO whose performance objectives, such as application time to market, may run counter to security. Experts with this view advocate having the CISO report to a senior executive outside of IT – such as the CRO or CEO (aka CXO).

For the purposes of Rational Cybersecurity, there isn't one right answer. Suppose the Board considers this question: "What's more important for our Cybersecurity? Operational effectiveness and Security-to-IT alignment, or strengthening security by making it an independent function?" Directors of highly regulated organizations tend to have separation of duty requirements and prefer CXO reporting, whereas organizations under less security pressure are more likely to choose CIO reporting. Depending on the business's cybersecurity maturity level, management style, and executive personalities, either reporting structure can work, with caveats.

CIO reporting structure caveats: In most organizations where the CISO is directly responsible for conducting or overseeing IT security operations, one of our CISO contributors observed: "As the CISO, it is critical to be no more than one level removed from the Board (or CEO) and to have my name on the security section of the Corporate

Board Reports." Without that visibility, and the opportunity to present important security initiatives and budgets to executives, the CISO position might be too weak to conform to the expectations created internally and externally by using the "CISO" title.

3-2

Once businesses reach a certain size or level of security pressure, they should give their top security leader the "CISO" title. Leaders with the "CISO" title should have access and visibility to executive management and the Board.

Also, note that empowering an independent internal audit function, whether or not it is required by regulations, may provide an adequate check and balance on the CIO even though the CISO reports to IT.

CXO reporting structure caveat: If a business places the CISO function outside IT, bear in mind that IT staff may consequently be responsible for more of the security operations. A dotted line reporting arrangement could be set up between these staff and the CISO provided the maturity in governance and awareness exists to enable such matrixed functions to work well. More than one security or business leader I spoke to in more than 60 interviews while writing the book agreed that this could be the right arrangement but requires maturity.

Change is the only constant: More than one CISO I interviewed noted: Not only does the optimal reporting structure depend on hard-to-quantify management style factors, these factors change frequently.

"Organization design and placement of the CISO (or CSO) function needs to be dynamic, depending on who has which strengths and who doesn't. The Tuckman model (forming-storming-norming-performing)[3] applies as executive teams or IT teams change."

David Cross, Senior Vice President, Chief Security Officer at Oracle SaaS Cloud

[3]"Tuckman's Stages of Group Development," Bruce Tuckman, Wikipedia, 1965, accessed at https://en.wikipedia.org/wiki/Tuckman%27s_stages_of_group_development

There's clearly much more to say on the subject, and if you're interested all three authors of the "CISO Desk Reference Guide" opine on the role and reporting considerations right in their first Chapter - "The CISO".[3]

3.5 Institute Cross-Functional Coordination Mechanisms

Even for smaller businesses that don't think of themselves as needing matrixed governance, many security projects tend to be cross-functional and face the same challenges as in larger organizations. *Harvard Business Review* research found: "Projects that had strong governance support – either by a higher-level cross-functional [executive team] or by a single high-level executive champion – had a 76% success rate, according to our research. Those with moderate governance support had a 19% success rate."

Businesses should have a formal executive coordinating function responsible for cybersecurity. In addition, consider chartering an executive-level risk management committee (such as the Board Audit Committee or others) to act as the risk management forum for information risk. Finally, processes should exist for security governance to oversee IT or security projects and processes.

3.5.1 Cross-Functional Security Coordination Function or Steering Committee

A large enterprise can establish a dedicated steering committee for security-related operations, projects, and business decisions. However, mid-size organization may reasonably combine the function into a general IT leadership committee as one of its recurring work topics. We'll refer to the coordinating function generically as a "steering committee." The level of security pressure is another factor determining whether to have a dedicated committee: In 2017 and 2018, I consulted for a US-based systemically important financial market utility (SIFMU) with just a few hundred staff but a regulatory requirement to focus heavily on security at the highest levels of the business.

[4]"CISO Desk Reference Guide," Bill Bonney, Gary Hayslip, Matt Stamper, CISO DRG Joint Venture, 2019

The steering committee authorizes and at a high level can direct security projects, oversee security policy, and control the security organization structure. The heavy hitters among the leadership – those holding CISO, CIO, Chief Risk/Privacy/Compliance offices, legal, HR, and third-party management positions (or roles, in a smaller business) – should be represented on the committee. So should key LOB leaders such as manufacturing, sales, distribution, and operations. The business and security executives themselves can attend or appoint leaders with signoff authority delegated on their behalf. (In larger businesses, major LOBs may have their own business information security officers (BISOs) as well as finance and legal representatives on the steering committee.)

The steering committee should meet approximately monthly. The sponsor and/or chairperson should have administrative support to maintain a formal agenda, track issues, manage any subcommittees or activities that require attention between meetings, and publish minutes and reports. Typical activities are

- Authorize and oversee major projects necessary to create the security program or achieve important goals
- Approve organizational changes, budgets, and resources for cross-functional security projects
- Direct and oversee cross-functional projects that impact multiple business units or address strategic risks being tracked by the Board
- Monitor regulatory and audit findings and the timely response to the findings
- Mediate any conflicts arising out of projects or other security-related incidents and activities

3-3

Ensure LOB and corporate administration business leaders are engaged with the steering committee by reflecting their concerns on the agenda, giving them important roles on the committee (possibly through a rotating chairperson function) and involving them in meaningful planning, decision-making, and approval activities.

3.5.2 Risk Management Forums

What I'll refer to generically as the "risk management forum" could be chartered as a committee dedicated to information risk. The CISO or a Risk Manager on the CISO's staff can chair this type of forum.

However, the forum may instead be part of an enterprise risk management (ERM) program. ERM covers financial, operational, market, competitive, and other risks as well as information risk which rolls up into it. An ERM forum doesn't fall under information security governance, but the CISO (or a delegate) should be a member or participant.

Financial services businesses (depending on size and jurisdictions) tend to require ERM programs. Many other kinds of businesses – whether larger or small – have corporate social responsibility, ethics, and/or compliance committees to monitor enterprise risks at the highest level. Any of these executive committees (or a new group) could become the risk management forum. The forum:

- Helps executive management and the Board determine accountability and responsibility for specifc risks, define risk appetites and create guidance on preferred risk treatment strategies
- Translates executive risk guidance into policies and procedures for monitoring and controlling the top risks to the business
- Maintains a list of top risks, often using tools such as a "risk register" or "risk map"
- Tracks the risk exposure from each top risk, how it is being managed, and the status of projects related to it
- Oversees risk reporting to the Board and to external stakeholders such as investors, auditors, and regulators

3-4

Empower the risk management forum to support executives in taking accountability or responsibility for, and review their performance on, managing information risks.

Chapter 5 contains additional guidance on the activities of the risk management forum.

3.5.3 Interaction with IT Projects and Other Security Processes

Standing governance forums such as the security steering committee and the risk management forum are necessary and important. As the security program matures, especially in a larger enterprise with matrixed security governance, more and more issues can require regular agenda time.

Security leaders may be tempted to establish multiple standing subcommittees of the main steering committee or risk management forum but should be careful not to overdo it. Digital business demands more agility from businesses. Keeping standing security forums lean helps ensure that security doesn't get in the way of reasonable business initiatives through overly bureaucratic processes. Rather, the business can use existing security, IT, or corporate governance processes to promote collaboration between security business leaders and oversee security projects. These can include

- **Security architecture reviews:** Security architecture reviews occur as part of a project management "gate," through which projects move on their path to completion. Disciplined Agile processes can operate more iteratively with security being addressed in the "Sprint 0" and later sprints for quality assurance.
- **DevSecOps:** A fully or partially automated "pipeline" can produce test reports and documentation through which new functionality from development is promoted to production. See Chapter 7 for more details on DevSecOps and Disciplined Agile.
- **Third-party assessments:** Assessments of suppliers, vendors, contractors, cloud service providers (CSPs), and so on are required as part of procurement and change management.

3-5

Avoid making standing governance too heavyweight. Instead, work with IT, development, and corporate administration groups to help them understand and build enough security into their own processes.

3.6 Manage Security Policy Libraries, Lifecycles, and Adoption

When managed with tight alignment to the business, a core set of security policy documents can evolve into a collaboratively developed and formally agreed "Constitution" providing the structure for a positive security culture. Develop policies in a vacuum and they're at risk of gathering dust on the shelf.

3-6

Ensure business unit representatives provide input to security policies that will affect them. Take pains to obtain cross-functional buy-in from all affected parts of the organization.

Businesses should manage security policy documents in a hierarchical structure and develop a policy management process. The governing security policy should

- Be owned by the security organization and the chartered steering committee but endorsed by the CEO and the Board.
- Define a process for changes, documentation formats, review and expiration, approval procedures, and enforcement. It can be reviewed on an as-needed basis or approximately once every three years.
- Require that all policies specify the roles of the security or business functions that own, approve, and are covered by policies. In general, avoid explicitly referencing individuals or groups that are too low in the organization and likely to be frequently moved or reorganized.
- Establish the principle that directives or guidance should link to risk as it is understood in the enterprise and IT risk management framework in a manner flexible enough to accommodate multiple risk levels as well as changing risks and risk appetites. For example, the tiered third-party risk management process discussed in Chapter 7 could initially be established through a policy.

3.6.1 Types of Policy Documents

The term "policy" in security often conflates four or five types of control documents: a top-level security "policy" and standards, guidelines, processes, and procedure documents. Figure 3-7 displays the relationship and hierarchy among those types of documents.

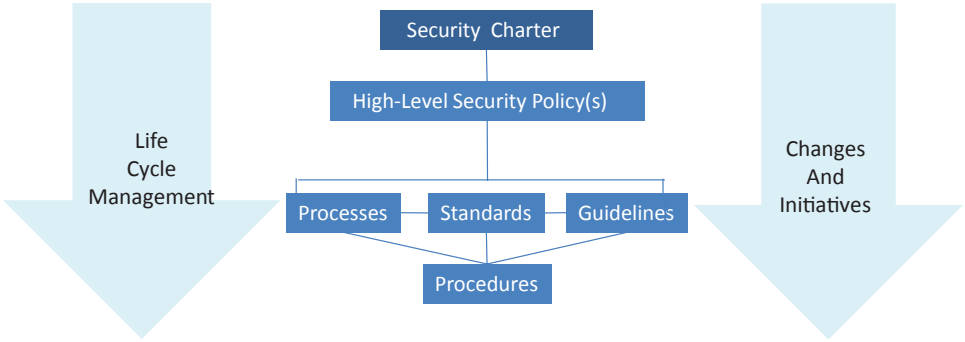

Figure 3-7. *Policy Document Hierarchy*

Each control document or type of "policy" at a lower level of the hierarchy must operate within the permitted scope of any related higher-level documents. For example, the organization's highest-level security policy may operate under the security charter. More detailed policy or standard documents set requirements for topics such as acceptable use, access, network security, encryption, and so on. Guideline documents and processes provide instructions. In general, the higher-level documents specify the required business security outcomes (the "what") and subordinate documents specify the ways and means (the "how").

Businesses should also articulate guiding principles, scope, and purpose in the top-level policies (the "why") to help management and staff understand the policies' intent in all situations. Although top-level policies should not contain promises of future improvements or plans, guiding principles expressed in the policies can indicate future direction in a general manner where appropriate. Table 3-1 identifies (in general) which kinds of security and business leaders own, are affected by, and must be aligned with each type of policy document.

Table 3-1. *Types of Policy Documents*

Document Type	Purpose	Ownership	Audience	Lifespan
High-level security policy	Formal statement of high-level control objectives (creates implicit compliance obligation)	Executive responsible for the applicable C-level function, i.e., CEO, CRO, CISO, VP compliance	Organization's management, staff, regulators and auditors	3–5 years
Standards	Detailed, mandatory control requirements for technologies, processes, or procedures	Senior manager reporting to the executive responsible for the higher-level, governing policy	Organization's management, some staff, regulators, and auditors	2–4 years
Processes	Describe the interactions and flows of multiple roles, multiple procedures, and multiple systems	Senior manager reporting to the executive responsible for the higher-level, governing policy	Organization's management, some staff, regulators, and auditors	1–3 years
Procedures	Prescribe specific steps or checklists required to accomplish specific (and in many cases, technology-specific) activities	Manager reporting to the department responsible for carrying out the procedure or a departmental manager	Narrow management and staff audience. Operate in compliance with policies, standards, and processes	6 months–3 years
Guidelines	Describe discretionary activities for technologies, processes, or procedures. May be combined with standards	Manager reporting to the executive responsible for the higher-level, governing policy or standard	Intended to be helpful to management and technical audiences	1–3 years

3.7 Budget in Alignment with Risk and the Governance Model

Multiple budgets for security activities often exist across different organizational units in the business. Along with the security governance model, budgeting and resource allocation must be rationalized.

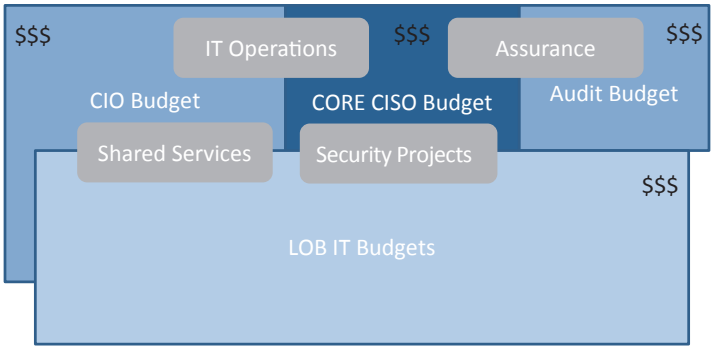

Figure 3-8. *Security Spending in the Business*

Figure 3-8 maps out where budgets for security-related activities tend to exist in the business. The security organization typically has a core budget for the activities it controls directly, but many other security budget items fall into gray areas of the IT, shared services, and even LOB's budgets. With the expansion of cloud computing and digital business initiatives, LOBs have many options for sourcing IT. In some cases, over half of IT spend is now controlled by business units. Many LOB development projects must include activities such as application security testing.

The fact that security gets funded from multiple sources is yet another reason why it is important to be mindful of selecting, or maturing toward, the right security governance model. Table 3-2 offers some observations on budgeting in the different governance models.

Table 3-2. *Budget Considerations in the Governance Models*

Centralized Governance and Multiple Budgets	Decentralized Governance and Multiple Budgets	Matrixed Governance and Multiple Budgets
Regardless of who is paying for the security activities, the security team carries out security activities. This can result in good coordination. But be careful to ensure the security organization doesn't become an unnecessary bottleneck; today's LOBs expect agility.	There's likely to be little or no coordination of security activities ongoing in different groups under different budgets. However, a security leader with "Group CISO" responsibility should perform an assessment to identify, and then fix, any significant risk exposure or unnecessary costs that could result.	Matrixed security governance can coordinate multiple groups and their budgets. However, it's important to gain maturity in risk management and governance before adding governance complexity. Otherwise, time and money could be lost to cumbersome processes. Resources could go the most politically connected groups rather than the optimum risk treatments.

Through the security steering committee and risk management forum, the business can endeavor to take a holistic, risk-based approach to prioritizing funding and resources for security regardless of which budgetary pot it comes out of. Security leaders must help the business understand current risks as well as the risk mitigation options and required funding. Security deficiencies can be linked to risks, business impacts, and the accountable executives. The following are good practices for budgeting:

- **Let risk analysis inform budgeting:** Some organizations build checklists of controls meant to satisfy perceived compliance requirements and fund those controls without analyzing their cost-effectiveness at reducing risk. Instead, security teams should use risk analysis to determine the top risk scenarios, control priorities, and budgets. In quantitative risk analyses, such as Factor Analysis of Information Risk (FAIR, see Chapter 5), the most serious losses due to

noncompliance show up as "secondary loss events" that materialize only after a primary loss event (e.g., a breach) occurs. Avoiding the primary loss event in the first place may be the best path to reducing potential costs of noncompliance. This is just one example of how risk analysis can identify the most cost-effective controls to fund.

- **Be creative about looking for low-cost risk treatments:** In some cases, the business can achieve a required security or compliance outcome through business or security process changes rather than costlier technology deployments. For example, changes in how the organization uses consumers' personal information, or obtains consent in advance from consumers, can reduce the need for many protective or responsive controls later on in the event of cyberattacks, breaches, and data subject requests.
- **Find a way to represent technical debt in security cost accounting and use it to reduce costs in the security product portfolio:** If the security organization has staff with accounting skills working on the security budget, it may be helpful to work cost of ownership into business cases in a way that represents the corrosive effects of technical debt, and promotes strategies to reduce technical debt in the IT security portfolio.
- **Review budgets quarterly or bi-annually and build in contingency plans:** Be prepared to reallocate funding if a high-priority project is having difficulties, especially if other projects on the road map depend on it. Contingency plans must also prepare the security organization to deal with budget cuts that can occur due to changes in the business's fortunes or the economic cycle.

3-7 *Link budget and resource requests to a business plan which demonstrates quantified risk reduction and other benefits to the business. Don't rely on fear, uncertainty, and doubt (FUD) to drive funding approval.*

3.8 Call to Action

The core recommendation for security leaders from this chapter is for them to define (or reset) cybersecurity and risk governance by

- Creating a security charter to define security's mission and designate lines of authority or decision rights
- Establishing an executive security steering committee and a risk management forum (or other cross-functional coordination function scaled to the size and type of business)
- Ensuring LOB and corporate administration leaders are engaged with the security steering committee function and empower the risk management forum function to hold business leaders accountable for information risks
- Avoiding heavyweight security governance processes in favor of embedding just enough security-related activities into business-as-usual processes or projects that come and go
- Developing a security policy lifecycle management function and ensuring business leaders provide meaningful input on the policies that affect them
- Aligning and risk-informing security funding and activities that come from multiple budgets

Action – Make a quick assessment of the state of the organization's security governance

Ask yourself the following short set of questions and score the answers in the Success Plan Worksheet's[4] Section 3, Table 3. Base your score on whether you would answer most of the questions with a strong "no" (1), a strong "yes" (5), or something in between.

[5] "Rational Cybersecurity Success Plan Worksheet," Dan Blum, Security Architects LLC, May 2020, accessed at https://security-architect.com/SuccessPlanWorksheet

1. Does the security governance structure align well with the way IT and the business are organized?
2. Is the business's definition of security (mission, governance, reporting structure, and operating principles) captured in the security charter, and is it reflective of the way the business really works?
3. Does a security steering committee meet regularly; do security, IT, corporate administration, and LOB representatives with signing authority regularly attend it; and is it effective at addressing cross-functional security issues and moving security projects forward?
4. Does a risk management forum exist, and does it hold business risk owners accountable for risks and serve as a useful venue for reviewing top risk analyses and treatment recommendations?
5. Are security policies, standards, processes, and procedures generally up to date, and do day-to-day practices in the business generally follow them?
6. Is the security budget centralized, or are multiple security budgets rationalized in the sense that relatively little overlap exists?

Action – Define 1–3 improvement objectives for security governance

Note improvement objectives in Section 4, Table 5a, of the worksheet. The following are examples of security governance–related improvement objectives:

- Create or revisit the security charter and work on getting business buy-in for a definition of security that is fully aligned with the business needs.
- Review Chapter 2's Table 2-2 listing security-related business roles to find any that seem appropriate for a business like yours but aren't being fulfilled. Communicate with stakeholders and find out the reason.
- Plan for a security policy refresh and identify business stakeholders affected by the current policy documents and potential new ones.

- Review the minutes or records from the last 6–12 months of security steering committee (or other coordinating group) meetings, assess the committee's strengths and weaknesses, and propose improvements.
- Work with the business finance office to collect information on all security budgets, sources of funding, and funded project charters. Call out any obvious gaps or overlaps.

Don't limit yourself to these examples. Also consider other improvement objectives that fit the gaps and priorities you've identified for your business.

CHAPTER 4

Strengthen Security Culture Through Communications and Awareness Programs

Human error or misconduct of one kind or another must be either the direct cause or a contributing factor to almost every security breach or outage. Whether it is the user clicking a phishing link, an operator accidentally deleting the corporate directory, a manager approving excessive privileges, a receptionist letting a thief or spy into the building, or an incident responder hitting the snooze button on the wrong malware alarm, the examples are legion.

Security leaders should strive to improve security-related behavior through user awareness and training programs. Sometimes these programs succeed in bettering security-related behaviors, sometimes they don't. Wouldn't it be nice to know why? It turns out that people's behavior is related to a larger issue of security culture, which is itself a part of organizational culture.

Formally adopted security policies, well-defined security governance, and clear security-related roles in the business are prerequisites for a successful security program. But in the background behind the visible security governance and security program machinery is the organization's security culture. A security culture is the part of an organization's self-sustaining patterns of behavior and perception that determine how (or if) the organization pursues security. A positive security culture can provide your best opportunity to secure the business; a negative one can be your greatest vulnerability.

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8_4

> "Culture eats strategy for breakfast, lunch, and dinner."
>
> **Peter Drucker, Management Guru**

Modern organizational thinking – and marquee schools such as Wharton or Harvard Business School – sees organizational culture as paramount for business outcomes. Hard to define, as likely to change the executive as to be changed, and usually neither all good nor all bad – culture is pervasive in the business.

Security leaders can use communications and awareness programs to gradually enhance security culture throughout the organization as well as improve specific user behaviors such as resisting and reporting phishing messages and becoming good stewards of customer information. Over a period of time, security teams can cultivate a network of influencers throughout the business to create a healthier security culture.

The chapter provides guidance for security leaders on how to

- Address common challenges
- Understand security culture and awareness concepts
- Make enhancing communication a top security team priority
- Use awareness programs to improve behaviors and security culture
- Commit to improving security culture
- Measure and improve

4.1 Address Common Challenges

According to ISACA/CMMI's 2018 "The Cybersecurity Culture Gap," 95 percent of global survey respondents identify a gap between their current and desired organizational culture of cybersecurity. Today, organizations face multiple challenges with engaging business units and executives at the strategic level and shifting the business towards a healthier security culture. Ineffective security communication styles can exacerbate these challenges.[1]

[1] "The Cybersecurity Culture Gap: An ISACA and CMMI Institute Study," ISACA/CMMI, 2018, accessed at: https://www.isaca.org/-/media/info/cybersecurity-culture-report/index.html

4.1.1 Business Executives Not Engaged at the Strategic Level

The average executive has probably been briefed on, or read about, security threats often but tends to be personally less knowledgeable than the general public about cybersecurity practices and self-assesses his or her business as not being well prepared. Moreover, we previously cited evidence that business executives tend to not consider cybersecurity strategic (see Chapter 2's section "Cybersecurity Not Considered Strategic").

According to a KPMG "U.S. CEO Outlook" study,[2] executive awareness of cybersecurity threats is high, but that doesn't translate to being ready.

- 33% of Chief Executive Officers (CEOs) identified cybersecurity as their top threat to growth.
- 92% can identify new cyber threats (i.e., from the news).
- 89% consider protecting customers' personal data "hugely important."
- But only 41% consider their company well prepared to deal with threats.

At the same time, business executives overall have relatively low detailed awareness of basic computer protection, privacy, and physical security according a MediaPro survey:

- 41% of executives' personal security and privacy survey scores put them in the "at risk" category compared to only 29% of the general population.[3]

4.1.2 Business Units at Odds with IT and Security

As discussed in Chapter 2's section "Working at Cross-Purposes," business leaders may be at odds with IT (and security) for all sorts of reasons – personal, organizational, and political reasons. Disruptive changes to IT and immaturity of security governance or

[2] "US CEO Report," Lynne Doughtie, KPMG, May 2018, accessed at https://assets.kpmg/content/dam/kpmg/us/pdf/2018/05/kpmg-ceo-outlook-2018.pdf

[3] "State of Executive Cybersecurity Awareness," David Self, MediaPro, July 2018, accessed at www.mediapro.com/blog/infographic-executive-cybersecurity/

risk management models contribute to the disconnect. Chapter 7's section "Address Common Challenges" identifies additional structural difficulties for IT. Namely, digital business strategies often lead to decentralization or fragmentation of IT control as trends such as cloud computing, bring your own device (BYOD), and a new generation of power users devolve application and infrastructure management to business units and/or cloud service providers (CSPs).

In some cases, IT (and security teams) are on board with the growing momentum toward cloud-first strategies and acting as brokers/providers. In others, they are facing a diminishing role as providers of premise-based services with shrinking business unit buy-in. If the business and IT managers or staff perceive any of the following, it can have a corrosive effect on the security culture:

- Central IT hasn't been effective at providing timely solutions or services (e.g., many days or weeks to fulfill a request for new virtual machines, storage capacity, or application access), lacks an effective cloud strategy, and/or resists the LOBs' own IT or cloud initiatives.
- Security leaders have acted like the "Department of NO," failed to offer helpful alternatives and solutions when they identify a problem, or not tried to understand the LOB's drivers or pain points.
- In large multinational organizations with different geographies, languages, and cultures, some LOBs are not engaged with IT or security programs from the headquarters or some of the meaning of these programs is lost in translation.

If cybersecurity isn't considered strategic or business units are disengaged, business leaders are less likely to support sustained efforts to improve security culture. This chapter and the book as a whole proposes multiple recommendations to build better bridges to the business and improve the security culture. But first security leaders must look inward, at their organization, themselves, and their communication styles.

4.1.3 Hard to Change Culture

One definition of business culture is "The self-sustaining pattern of behavior that determines how things are done," and it is further characterized as "An elusively complex entity that survives and evolves mostly through gradual shifts in leadership, strategy,

and other circumstances." The same authors argue that cultures are hard to change: "Cultures are constantly self-renewing and slowly evolving: What people feel, think, and believe is reflected and shaped by the way they go about their business. Formal efforts to change a culture (to replace it with something entirely new and different) seldom manage to get to the heart of what motivates people, what makes them tick. Strongly worded memos from on high are deleted within hours. You can plaster the walls with large banners proclaiming new values, but people will go about their days, right beneath those signs, continuing with the habits that are familiar and comfortable."[4]

In my experience, security culture inherits many attributes of the business culture. The good news is that security culture is a smaller problem space, and many security behaviors can be improved through targeted awareness campaigns, process changes, and even user experience (UX) changes to technologies – without changing the core business culture.

4.1.4 Ineffective Security Communication Styles

Every security organization has a culture of its own and the opportunity to influence the security culture across the entire organization it serves. An unhealthy business security culture can emerge, however, when the security organization's subculture is out of line with the broader business culture.

Both the CISO and the security team create the security organization's subculture. Although a larger security organization will have multiple teams, one or just a few predominant personality archetypes (e.g., the "cop," "ex-military," "auditor," "techie," or "business school" type) will tend to dominate the security organization and its communication style. If this style is out of line with the business culture (e.g., highly authoritarian in a consensus-oriented culture or vice versa), the security organization is unlikely to be well regarded.

Even without cultural dissonance between the security organization and the business, security leaders tend to find communicating with executives or peer business leaders challenging. Security leaders, even CISOs, serve a nonrevenue-generating function that's often positioned too low in the organization chart or informal executive pecking orders. They are often the bearers of bad news about incidents, vulnerabilities,

[4] "Ten Principles of Organizational Culture," Strategy+Business, February 15, 2016, accessed at www.strategy-business.com/feature/10-Principles-of-Organizational-Culture

deficiencies, and unwelcome regulatory requirements. To top it off, they may lack strong communication skills. An effort to overcompensate and overplay the fear, uncertainty, and doubt (FUD) card can get attention in the short run but lead to a loss of credibility when feared consequences don't soon materialize.

4.1.5 Measuring Culture Is a Soft Science

Security culture is more than awareness, and as a social phenomenon, it is an outlier to both the business financial metrics and the security technical metrics domains. Measuring whether efforts to improve security culture are effective (or that any single awareness and training campaign has succeeded) is important for our ability to understand what works. However, taking such measurements is challenging.

Organizations and practitioners who are unaware of methods to measure security culture may turn to measuring proxies, such as number of attendees and completion rates of awareness training courses. These metrics are not very useful because they only measure (at best) one or two points along a continuum of security behaviors and ignore other cultural attributes.

If the purpose of security awareness training is to improve the overall culture and not just a single behavior (such as reporting phishing messages), then a set of metrics must be devised to measure a broad set of security culture attributes. Unfortunately, there is no ISO or NIST standard for how to do this nor much research to provide empirical evidence that conventional awareness programs are effective. Such efforts that have been made to measure awareness effectiveness typically use only counts or trends of security-related events and incidents.

Measuring incidents in isolation just creates confusion. If more incidents are reported, does that mean security is getting worse or just that incidents are – at last – being reported? Incident metrics alone won't resolve uncertainty.

MEASURING SECURITY CULTURE – A PRACTITIONER'S STORY

Kai Roer, who developed the Security Culture Framework process[5] and has made a career out of security culture projects, explained: "Our process included a measurement phase. But no standard metrics existed. Although we did measure changes, we did not know if they were improvements or not. When we did security culture work as consultants, we also had to consider political factors. Initially there was lot of bias in the measurement."

In 2015, Roer teamed up with socio-informatics expert Dr Gregor Petritc to create a Norwegian company called CLTRe (pronounced "culture"). CLTRe is a software-as-a-service (SaaS)-based measurement application loaded with the best security culture metrics the two of them could devise. Roer and Petritch also began producing an annual security culture report with industry metrics. In 2019, CLTRe was acquired by the US-based awareness firm KnowBe4, Inc.

In the "Measure and Improve" section, we'll discuss Kai Roer's approach to measuring security culture as well as additional strategies.

4.2 Understand Security Culture and Awareness Concepts

A *security culture* is the part of a *business culture's* self-sustaining patterns of behavior and perception that determine how (or if) the organization pursues security. It is an amalgamation of perceptions about and behavior toward the business's own IT and security systems, security policies, and operational security practices or projects. Security culture is not fixed, it is constantly evolving based on people's experiences and social interactions.

Security culture can impact an organization's risk levels, compliance posture, and costs or benefits in both positive and negative ways. Business and security leaders ignore it at their own risk, or they can leverage it to get better outcomes.

A *security culture strategy* is a conscious effort by security and business leaders to transform their de facto security culture into one that's more conducive to information protection and risk management. The strategy also seeks to sustain security culture at the desired state as the business changes over time.

[5]"The Security Culture Framework" website, CLTRe, accessed at https://securityculture framework.net

The way that the security organization communicates and aligns with the business along with user awareness and training programs is a primary tool for improving the security culture. In a healthy security culture, the security team's communications and the awareness programs have a higher chance of success. Even in a more negative setting, the right communications and awareness messaging carried out over time can help improve the security culture. A stronger security culture will then ease many other cybersecurity challenges.

4.2.1 Your Greatest Vulnerability?

Thought leader Edgar Schein once said about business culture in general: "If you do not manage culture, it manages you, and you may not even be aware of the extent to which this is happening." Likewise, security culture can make or break a security program.

In fact, the root cause of many security breaches is not technology, but a "people" vulnerability such as an employee being tricked by a phishing message or other social engineering exploits into giving away credentials or installing malware. In other cases, a failure to follow a process, such as change control, is the culprit. Often, multiple things go wrong. A breach rarely is, and in fact should not be, caused by just one vulnerability.

Consider your own organization's security culture, and ask yourself what would happen in the following "day in the life of a security program" examples:

- When budgeting comes around and the CISO presents a reasonable plan, but the CFO criticizes "unnecessary expenses"
- When the development manager waives the security design review because the project is behind schedule
- When the Agency Director demands immediate firewall rule changes that could expose taxpayer databases to the Internet
- When a potential breach is discovered for the business's French customers' data, there's no detailed response plan, and the CISO goes to the Chief Counsel with a warning about 72-hour General Data Protection Regulation (GDPR) breach notification requirements
- When a mutating zero-day virus has been reported at three sites, and the CISO recommends shutting down the network to affected regions with critical business applications

- When the VP of Sales receives a demand from the company's largest account in Dubai for contact information on all attendees at a recent business conference, even though sharing this personal data was not in the conference agreement and could violate compliance regulations

When faced with an apparent no-win choice between business and security values, what will the management team do? Will it reason through the issues to find the least-bad choice or brainstorm a third way out, learn from the experience, and update company policies to clarify similar circumstances in the future?

Or will a series of unproductive meetings end with escalation to the CEO, bad choices, acrimony, and blaming? How did the organization get to this point?

FINANCIAL SERVICES COMPANY HEAD OF INTERNAL AUDIT'S STORY

"Since more than 80% of the company's applications were custom developed, the global Chief Technology Officer (CTO) played a critical role. In conversation, it was clear to me that, the CTO understood the need for secure application development and the underlying risks. However, he felt that development organizations did not have additional budget to incorporate these practices and capabilities.

I recall attending a meeting with the CTO and senior engineering and development executives to get them aligned on the urgent need for secure development and operating practices for their transaction processing systems. Surprisingly, the development executives were vigorously resistant: '*Why can't engineering take care of security? We are development and we need to focus on building product quickly – our focus is on writing code that is fast, optimizes the user experience, and enables us to get features to market quickly*.'

To help the CTO further understand the risk, I asked a question: '*So across the infrastructure, is traffic encrypted?*' No one seemed to have a definite answer and after substantial discussion, the conclusion, was: '*No*.' I continued: '*Then where is the data security coming from if confidential transaction data travels are over public spaces and physical pipes*?' Much to my surprise, the application development and infrastructure security teams started pointing fingers at each other instead of taking ownership and working the problem together. At this point I could see the CTO was losing interest in this topic. There were more important things to do.

> My next stop was to brief the CEO. At the end of a long and very interactive discussion with the CEO, which included the CTO who sat quietly appearing non-committal, I summarized '*We are not secure. And the central issue is that each technology team is saying that security is not a priority requirement for them and needs to be provided at another layer or by another team*.' The CEO's response was lukewarm. The CEO felt that the CTO was doing enough. The recurring subtext seemed to be: '*Yeah, we know we are highly regulated and while certain processes may not appear to be great, nothing bad has happened – ever! We're going to be ok*.'
>
> Eventually, the company experienced a serious data breach, where vulnerable applications were exploited early in the kill chain.
>
> The unfortunate event was not surprising. I have seen this storyline play out so many times across a variety of companies and industries. Complacency results from diffused accountability and a decision culture that discourages responsibility for risk taking across teams and the management layers of a company. It becomes difficult to encourage informed decisions and a calibrated sense of urgency in a culture that is sclerotic, overconfident, and focused on constraints rather than solutions."
>
> **Anonymous**

The preceding story illustrates multiple problems. Security-related roles, responsibilities, and accountabilities were unclear, and the CEO placed a low priority on security. Thus, IT, development, and executive management failed to support deploying even such a basic control as data-in-transit encryption. The last paragraph of the story explains in the head of internal audit's own words why the company's woes with security stemmed from a cultural problem.

4.2.2 Or Your Best Opportunity?

When security issues loom, the business's fate may hinge on a ripple of knee-jerk reactions preprogrammed into the security culture. We've highlighted the possibility of failures – the things you want to avoid. Let's also consider how a healthy security culture can help an organization avert security failures in most cases and respond well or recover quickly even from serious incidents. Is your organization ready? Do the leaders and staff really value security? Do they realize that it requires teamwork between security

and business functions and what role they are to play? Do they buy into the policies they're expected to observe and know what principles to consider when pressed to make a difficult decision?

Maybe not all that – yet. There probably is no perfect security culture out there. But there are plenty of good models that leading organizations can aspire to:

- **Active executive oversight:** Executives aren't just going through the motions to review a quarterly report and react only when findings or incidents are too serious to ignore. Instead, at least a chosen few are actively meeting and discussing cybersecurity with security leaders from time to time and helping the rest of the executive team and the Board exercise oversight. The CEO or another top executive works with the security leadership to understand and prioritize the business impact of security risks and projects.
- **Coordinated management:** A cross-functional cybersecurity coordination group (such as a security steering committee at larger businesses) is in place. It is sponsored from the executive level, and the committee chair dedicates quality time to it. Although not every security issue bubbles up to the group, those that do to get resolved through principles-based deliberation, as much as possible to the benefit of both business and security.
- **Engaged stakeholders:** Business and security leaders or staff perform their security and risk management roles – such as data owner, data steward, risk owner – with the right mix of empowerment and control. A network of informal partnerships between security and business functions complements the official organizational structures and processes.
- **Supportive workforce:** End users are aware of the awareness program and often apply its advice or training to their work and personal computing activities. They tend to understand that security rules and policies are there to protect the business and themselves. They appreciate the security department's efforts to "make the secure way the easy way" through tools such as password managers and mobile device management. They often report suspicious emails or other indicators of compromise to the security team.

- **Secure IT users:** Business and security staff are aware of cybersecurity risks impacting their job function, make few errors, and practice secure behaviors they have been trained for, such as configuring strong passwords, locking workstations when away from the desk, and shutting down or disconnecting workstations immediately if suspecting malware.
- **Stable and motivated security organization:** The security leaders and team(s) are with the business for the long haul. They share the business's general goals and values and cultivate partnerships with counterparts at the business level. They work closely with IT and developers to build in security solutions that are often unobtrusive and generally complementary to other business goals. They act like coaches rather than cops.

Bottom line: Businesses can create a security culture that is hospitable to positive models and outcomes like these by establishing and aligning effective security governance, user awareness and training programs, and a process to continuously measure and improve the security culture itself.

4.2.3 Attributes of Security Culture

Earlier, we defined security culture as an organization or group's amalgamation of perceptions about and behavior toward its own IT and security systems, security policies, and operational or social security practices and projects.

Figure 4-1 illustrates the interrelationship of perceptions and behavior with other security culture components as described in the report "Security Culture 2018: Measure to Improve."[6] Observe that in a security culture, attitudes, norms, cognition, and communication shape perception and behavior. Group perceptions and behavior create better or worse security outcomes. Each component of culture can be measured and has complex interactions with the other components.

[6]"Security Culture 2018: Measure to Improve," CLTRe AS, Kai Roer, 2018, accessed at https://get.clt.re/report

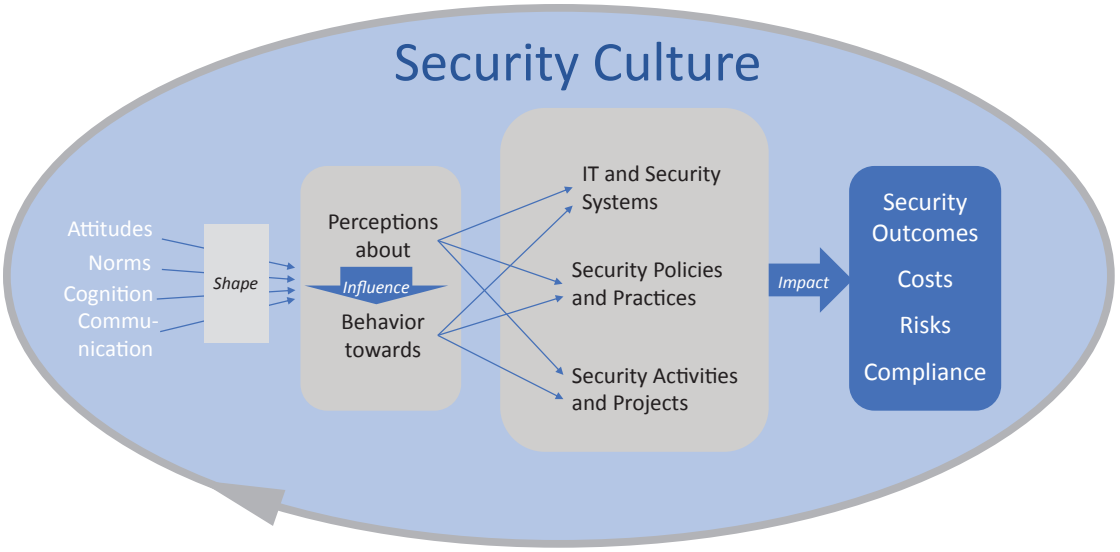

Figure 4-1. *Attributes and Outcomes of Security Culture*

Observe how the inputs and impacts (or outputs) of security culture form a feedback loop in Figure 4-1. The book "CISO Soft Skills" (discussed in Chapter 2) analyzes the security program and security culture using system theory. In the authors' model and this one, negative inputs degrade the system, producing negative outputs and a vicious circle that degrades the culture. Positive inputs and outputs do the opposite. All security cultures have a mix of positive and negative attributes and flows.

4.2.4 Security Culture Styles

Security culture in an organization is part of the larger business culture and needs to align with it. Figure 4-2 depicts various organizational culture concepts which are helpful for security leaders to understand.

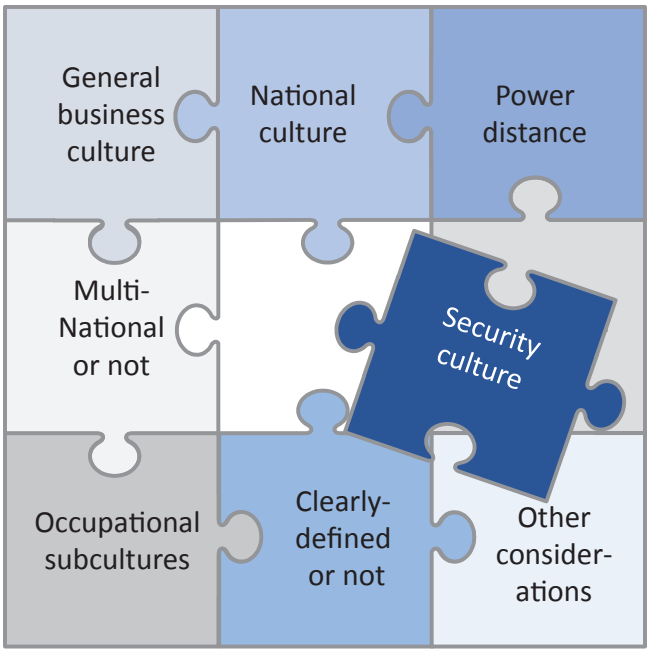

Figure 4-2. *Security and Business Cultural Factors*

General business culture can, according to the Harvard Business Review's "The Culture Factor's" research,[7] be understood in terms of eight distinct cultural styles that fall along two dimensions: how people interact and how they respond to change. In another model, Hofstede Insights analyzes organizational cultures along six dimensions,[8] including whether they are means oriented or goal oriented, internally or externally driven, easygoing or strict in work discipline, local vs. professional, open vs. closed, and employee oriented or work oriented. Hofstede also provides tools organizations can use to measure their cultures.

National cultures can be compared in many ways and must be considered as well as the general business culture in determining which security culture strategies and governance models (e.g., centralized, decentralized, and matrixed) will be effective. For example, organizations in a country typified by a high power distance[9] are likely to have

[7] "The Culture Factor," Harvard Business Review, January–February 2018 Issue, accessed at https://hbr.org/2018/01/the-culture-factor

[8] "Organizational Culture," Hofstede Insights, accessed at https://hofstede-insights.com/models/organisational-culture/

[9] "How Power Distance Influences Leadership," Florida Tech Online Blog, accessed at www.floridatechonline.com/blog/psychology/how-power-distance-influences-leadership/

better results with a centralized, prescriptive leadership approach, while organizations in a country with a low power distance may align better with a decentralized or matrixed organization's consensus- and collaboration-based processes.

In addition to national cultures, distinct **occupational subcultures** for executives/managers, office/administrative staff, developers, and other groups exist in almost all but the smallest organizations. Technology and IT services companies have many "white-collar" knowledge workers and developers. Health care has doctors and nurses; educational institutions have professors and teachers. Organizations in retail, manufacturing, utilities, and transportation have large numbers of "blue-collar" workers staffing factories, facilities, stores, or field operations. Government, financial services, and business services industry organizations have their own unique mixes of blue-collar and white-collar functions. The desired security cultural traits and the awareness methods to instill them may vary between these occupational subcultures, and the differences should be considered in deciding where a more prescriptive and where a more flexible and collaborative security culture strategy, governance, and communications approach would be optimal.

Some businesses – such as Chevron, Google, and Southwest Airlines[10] – have a business culture that is **clearly defined** and intentionally cultivated in a consistent manner, some do not. One can look at an organization's vision statement, or mission, to see if it calls out or implies a business culture style. If not, security leaders should look for other clues as to which of the cultural styles the organization seeks to follow.

Multinational businesses sometimes attempt to superimpose a global business culture vision over operating units in different countries; this scenario may dovetail with matrixed business, IT, and security governance (see Chapter 3). Or, local subsidiaries may be encouraged to operate with distinct national or local organizational cultures.

Other considerations: Organizational culture research doesn't identify a perfect culture, since the efficacy of culture is relative to the goals of the organization. However, much is written about the (numerous) dysfunctional organizational cultures including one short piece from the Hofstede Insights.[11] Business leaders often identify and discuss culture issues on their own and may be in the middle of a culture change project.

[10]"10 Examples of Companies With Fantastic Cultures," Sujan Patel, *Entrepreneur*, August 2015, accessed at www.entrepreneur.com/article/249174

[11]"Ask an Expert: 6 Signs That Your Organisational Culture Is Not Working?," Hofstede Insights, accessed at https://news.hofstede-insights.com/news/2018/06/15/ask-an-expert-when-an-organisational-culture-is-not-working

4-1

Security leaders should align their definition of security, the security program, and security awareness messages with the business culture. When multinational cultures are in play, the security organization must be flexible and creative on how it aligns to them.

4.3 Make Enhancing Communication a Top Security Team Priority

Security culture and awareness campaign outcomes are shaped by the whole message that businesspeople get from the security organization. Security leaders can address the challenge described in the section "Ineffective Security Communication Styles" by understanding how businesspeople perceive both the security organization's occupational subculture and the messages they're receiving and by improving communications in the following ways:

- Cultivate a collaborative and supportive communication climate with business leaders, managers, and staff to encourage open interaction. Communicate with the expectation that stakeholders will be the supportive colleagues you need them to be.
- Be mindful of the audience and tailor messages appropriately. Don't use highly technical language that might lose businesspeople. Use examples businesspeople can understand. Keep presentations as brief and actionable as possible while providing supporting material.
- Couch negative messages as an opportunity for improvement rather than criticizing or casting blame.
- Discover positive points and include them in the message; there will almost always be something stakeholders are already doing well, some area where they have improved, or positive intentions they have expressed. Give stakeholders public credit for any help they provide, even in small things.

- Also accentuate the positive by communicating with a sense of efficacy, as advised in Chapter 2's section "Earn Trust and Cooperation from Users." Stakeholders will respond well if offered an easy or achievable way to improve or reduce risk.
- Be respectful of stakeholder's time. Prepare for meetings with stakeholders in advance to minimize the amount of information gathering required during meetings. Take note of the information learned from stakeholders and make it available to security team colleagues to avoid repetitive requests.

The following generalized example proposes a good way to frame briefings of security issues or calls to action for stakeholders. Note the focus on teamwork done in advance of the briefing to show the security organization's collaborative approach.

COMMUNICATION TIP FOR CISO EXECUTIVE BRIEFING

- **Begin with a realistic take:** We may have some bad incidents, audit findings, or negative third-party assessments. There's a lot of red (risk) on this chart.
- **Map to business impact:** Here's how our risk scenarios relate to your core business functions. Here's what happened to some of our peers.
- **Emphasize teamwork that's gone into finding a solution:** Here are some ways we can (or already have) work with business teams to come up with a new approach (e.g., strategy, policy, technology upgrades, budget).
- **Focus on business outcomes:** This is how the new approach could protect or recover your core business functions or performance metrics. Here's how the required work would affect you.
- **Set realistic expectations:** Even with the new approach, there are still some risks we must live with. However, by working together we can greatly reduce our risk and have a defensible strategy. Any and all questions welcome!

All communications involve three components: the content, the relationship between the parties, and the organizational structure that frames the relationship and content. As we discussed in Chapter 2's section "Clarify Security-Related Business Roles," having a clear definition of roles and responsibilities can help many aspects of the security culture. Better security governance structures and security communication efforts are mutually supportive.

As noted in section "Security Culture Styles," security leaders must be mindful of the business culture as they seek to communicate with stakeholders. Communicating effectively across multinational business cultures in large organizations requires a sustained team effort as suggested in the following CISO stories.

COMMUNICATION TIP FOR MULTINATIONAL IT AND SECURITY TEAMS

CISO Stories of Building a Multinational Security Culture

"You have to travel and get in front of the international business units. Face to face meetings, continual reiteration that you are building the security program for them and with them, not 'just because.' Understand and work with different culture's communication styles. I found that in India they don't want to say no, you have to get to the reasons why something would not make sense and work with those issues. Sometimes this means learning more about the customers of your customers.

Once the relationships existed, I was able to cross-fertilize know how on international weekly calls among security staff – e.g. Australia is having audit findings, here's how Sao Paolo's team handled that issue. If they've done something and been rewarded for it, they will value it."

Michael Everall, CISO

"We realized we needed to tell people what we were doing as a team (everything from the network architecture on up); we made a list of 50 initiatives and prioritized 10 with champions assigned to develop presentations. When they travelled, they had to present one of that 10 to the local site. I told staff that I wouldn't sign their expense reports unless they made a presentation, and I would personally add an extra ½ day to my trips for the presentation and open house Q&A. This was really appreciated, and we learned a lot."

Paul Simmonds, CISO

Recognition of the need for security leaders and CISOs to improve soft skills has been growing for some time. The average CISO in 2020 is almost certainly a better communicator than his or her counterpart in 2010. But it hasn't been enough – yet – to improve cybersecurity-business alignment and cybersecurity outcomes against the rising bar of threats, regulations, and business needs. CISOs can take the following steps to improve the security organization's business communications:

- Make improving security-related communications a top priority.
- Provide communication training, measure communication skills, and hire effective communicators within the security organization.
- Recruit security champions within the business's sales and marketing teams to provide additional coaching or training on communication skills for key security managers and staff.
- Obtain commercial communications training, coaching, and tools. Offer these enablers both to members of the security organization and to members of security-related functions such as compliance.
- Use the communication tips provided here for executive briefings and international teams. Collect a library of such tips for other situations.

4.4 Use Awareness Programs to Improve Behaviors and Security Culture

Awareness programs can be targeted to improve specific security-related behaviors for defined audiences. They can also be used in a strategic effort to improve security culture. Figure 4-3 diagrams three dimensions of an optimal user awareness and training program.

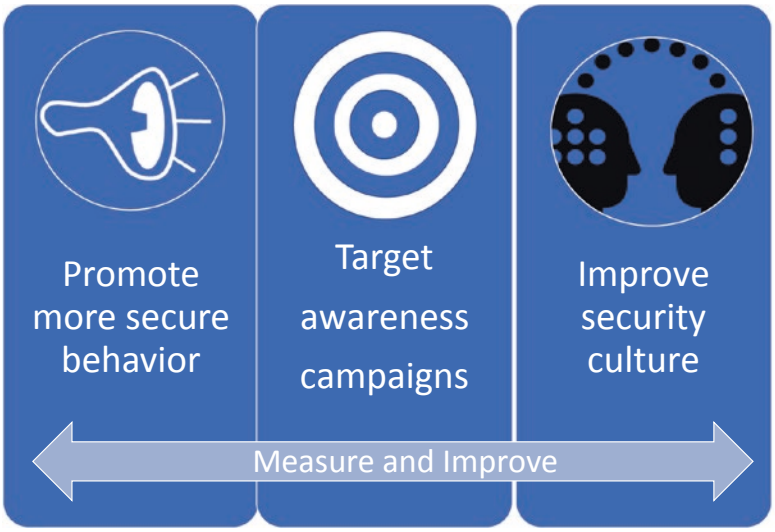

Figure 4-3. *Dimensions of User Awareness and Training Programs*

NOTE I could have written a whole book on user awareness and training programs. Instead, I've limited discussion to the programs' goals and strategies that support security culture and business alignment. Fortunately, there's another book that's highly complementary to the notion of driving a healthy security culture through the awareness program. Perry Carpenter's "Transformational Security Awareness"[12] gets much deeper into tactics and I'll refer to it herein.

4.4.1 Promote More Secure Behavior

Today's users work online in a minefield of malware, ransomware, social engineering, and insecure devices, applications, and networks. Some primary purposes for awareness programs are to improve users' understanding of cyber threats to themselves and the business as well as teach them to practice basic security hygiene against those threats. Role-based awareness and training can also be deployed to IT, development, and other business areas to reduce human or technical vulnerabilities and/or promote regulatory compliance.

[12]"Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors," Perry Carpenter, John Wiley and Sons, Inc., 2019.

Some of users' most common insecure practices are

- Failing to be vigilant enough to ignore or report potential phishing messages
- Falling for other social engineering tricks
- Selecting weak passwords or not changing default passwords
- Sharing accounts with colleagues, friends, and family members
- Telecommuting unsafely (using insecure Wi-Fi, leaving devices unlocked or unattended)
- Disabling security controls on a device
- Installing or using unauthorized applications
- Using obsolete software or unpatched software
- Revealing potentially sensitive information in personal interactions or on social networks
- Falling afoul of industry-specific compliance issues such as protecting customers' personal information

Security leaders (with the support of the business) should use the full array of security program instruments to promote more secure behavior including policy, processes, awareness programs, and tools that either prevent insecure behavior or discourage it. An even better approach is to make secure behavior the path of least resistance; for example, multifactor authentication obviates the need to create highly complex passwords and change them frequently.

4.4.2 Target Awareness Campaigns and Training Initiatives

Awareness program leaders can identify which kinds of insecure practices are most prevalent or serious for the business by

- Running vulnerability scans for top areas of user-related vulnerabilities, such as weak passwords
- Interviewing the organization's most knowledgeable user-facing staff in incident responder, help desk support, and HR roles to identify security topics on which users need help

- Reviewing relevant audit findings (such as privileged administrators sharing passwords to service accounts in an unauthorized or ad hoc manner)
- Surveying users or supervisors in the target populations

For further prioritization, the types of insecure practices can be correlated and prioritized for different audiences. Work environment factors to consider are the users' business roles, hardware and software, IT-related roles, relevant risk scenarios, and defensive controls already in place. Find out whether different populations of users can

- Telecommute and use BYOD solutions
- Browse the Web relatively freely and connect to personal web-based mail from their work device
- Have local administrative privileges on their work device
- Get access to personal or sensitive information
- Administer IT systems or applications

Awareness program leaders can then identify a small number of audience types and tailor awareness messaging and training. For example, at a retail company, one might target all employees and full-time contractors for phishing training and phishing simulation testing. However, only office workers with devices would be trained on device security hygiene. Only administrative staff and store managers would be trained on consumer privacy regulatory compliance during an initial awareness campaign.

Having selected the target behaviors and populations, identify specific awareness/training objectives, audiences, messages, and medium(s). Note that IT staff and developers might merit awareness and training on some of the same issues as end users, but the messages and training content could vary. For example, both end users and IT staff could be cautioned against sharing accounts. IT staff could also be advised of acceptable organization-standard account sharing workarounds such as password vaults for break glass access[13] but cautioned to adhere to policies against granting excessive privileges to colleagues or end users.

[13]"How to Design a PAM Break Glass Process," Dan Blum, Security Architects LLC, January 2020, accessed at https://security-architect.com/how-to-balance-assurance-and-availability-in-pam-systems/

Larger organizations under medium or high security pressure should have a group dedicated to awareness training and a communications organization providing content preparation and delivery. In smaller organizations, or organizations lacking staff dedicated to awareness and communication, the security leader responsible for the program should consult with internal marketing staff and/or supervisors to learn which mediums (e.g., videos, email newsletters, lunch and learn sessions, posters, etc.) would be most effective for each audience.

"We try to follow the good practice of sending a positive message in awareness programs. Our awareness program leader believes that if you teach people how to be secure in their personal lives, that translates to business benefit because the basic literacy applies to everybody. Also, teaching awareness this way raises attendance at events."

David Sherry, CISO Princeton University

In "Transformational Security Awareness," Carpenter repeatedly emphasizes the need to work with human nature, not against it. People tend to resist doing things that are difficult, awkward, or require change. We tend to quickly forget about 90% of our training unless it is reinforced through use. Carpenter writes that instilling knowledge and awareness is like "an exercise in cutting through the noise and slipping past the brain's defenses" to motivate users, give them the ability, and continually prompt them do the right thing. Facing this challenge, it is generally best to automate the desired task or behavior whenever possible.

Awareness professionals must adjust content and tactics to the following user behavior groupings: Those motivated and able to perform a duty, those motivated but not able, those able but not motivated, and those with neither motivation or ability. That's how deep security user awareness and training can get into behavioral science, multimedia content development, and attention management. Carpenter notes: "Being a security expert doesn't naturally transfer to communicating security-related information to people outside the field." Therefore, in my experience, successful awareness programs rely heavily on non-technical people with a background in marketing, education, or communications to work with technical experts.

4.4.2.1 Special Considerations for Work at Home, or Bring Your Own Device (BYOD) Programs

In 2020, COVID-19 forced many organizations to greatly expand teleworking and BYOD programs. As part of expanded remote access, employees in many cases require more latitude to browse the web free of restrictions or protections from proxies or firewalls. Hackers have moved to exploit newly vulnerable users and their organizations leading to increases in fraud and abuse.

Although its generally preferable to limit users' vulnerability through automated technical controls, such as blocking ports on a device, it isn't always possible to do that in a BYOD environment where controls require more user discretion, or user cooperation, to operate.

As organizations seek to stabilize home office security and (in many cases) to continue supporting remote work over the long haul – users' security awareness becomes even more strategic to business success. Security leaders can take the opportunity to partner with business and IT functions concerned with improving staff's digital literacy and proficiency, which are also a cybersecurity concern.

4.4.3 Coordinate Awareness Messaging with Managers and Key Influencers in Target Audiences

Business people are more likely to be influenced by awareness and training if their managers and executives support the program.

4-2

To maximize the chance of success, security leaders need to gain buy-in for awareness, training, or security culture improvement programs, in advance from the managers or executives of the target groups.

Security leaders responsible for the awareness program should establish relationships with business or LOB executives, gain their trust, and seek their buy-in and support for the strategic use of awareness programs.

"The attitude, behavior and messaging related to security from the CEO (and other executives) is critical. Just having the CEO wear a badge whenever appearing on an all-employee video sends a message."

Christopher Carlson, Information Security Writer and Adviser

Once management is supportive, role- or audience-specific awareness and training doesn't necessarily require an over-sized budget. The awareness program can reach out to influencers in the organization as well as security team members and IT staff to get some assistance. Consider using customizable curricula with a "train the trainer" approach. Engage experienced staff to introduce, explain, or add context to generic or third-party training content for their colleagues.

4-3

Coordinate security communications to the business with IT computer support and applicable corporate administration functions (HR, legal) or LOBs. Align instructions on how to perform basic or role-specific security duties with corresponding security processes.

Involving IT or business-level staff in customizing role-specific training or awareness content not only builds the library of training materials but is also more engaging and memorable to the staff themselves. Role-specific training can be tied to corresponding security processes, such as how should

- An executive sign off on a risk acceptance memorandum
- A data steward evaluate a Sales Department request for releasing customer information to a partner
- A system administrator request access for a third-party vendor to troubleshoot a critical system

See Chapter 6's Table 6-3 to identify which control domains engage which business functions. Consider training needs for managers and staff in the roles needed to implement each control domain according to the organization's security or business processes. As the awareness program builds a network of key influencers throughout the organization, its ability to create a healthy security culture grows.

4.5 Commit to Improving Security Culture

Business and security leaders in organizations with a healthy security culture tend to accept and approve of requirements for awareness programs and security governance. They seek to move the organization from being one that performs tactical awareness and training projects to one that intentionally defines and measures security culture targets as a way to achieve its security vision, drive its security strategy, and meet its security objectives.

A long-term commitment to improve security culture could operate on a few different points of the continuum between purely tactical compliance–driven awareness programs and strategic, full-on security culture transformation programs. Note that strategic commitment could take the following forms:

- Establish formal security culture teams, projects, and process methodologies. ENISA's "Cyber Security Culture in Organizations" report[14] proposes a "do it yourself" model for such a program.
- Engage a management consultant specializing in driving business change and who has experience working with IT and security programs.

I'm guessing that the majority of those reading this, however, don't have the mandate for a full-on transformation program or funding for the additional project team that would be required. The good news is that what I propose in the sections "Make Enhancing Communication a Top Security Team Priority" and "Use Awareness Programs to Improve Behaviors and Security Culture" are about midway along the continuum between a tactical and strategic approach. Although they require and deserve some additional funding and management priority, they shouldn't require additional teams of resources in the typical organization.

Awareness and training efforts to strategically improve security culture can be built in an iterative manner and therefore be accessible to almost any security organization in almost any business. The main prerequisite is to enrich the awareness and training program to be a bit more strategic, enhance security-related communications, and measure aspects of the security culture along with the results

[14]"Cyber Security Culture in Organisations," European Union Agency for Network and Information Security (ENISA), November 2017, accessed at www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

of these efforts. As described in section "Measure and Improve," the awareness and communications programs can periodically measure and assess the as-is culture and security posture, select departments or audiences for awareness projects, and perform them. Then measure the results and adjust or sustain those activities, practices, or communications that are successful. At a later stage as awareness and communications programs mature, the business could choose to begin a full-on security culture improvement initiative.

4.6 Measure and Improve

Because security culture is multifaceted and full of subtleties, businesses can benefit by developing, choosing, and monitoring culture metrics. Due to staff turnover and continual changes in security policies, technologies, regulations, and the business, security culture and user awareness program effectiveness should be measured at least once every two years. Security leaders can pursue any (or all) of three suggested approaches to measure security culture–related information over time:

- Measure security-related communications effectiveness.
- Measure security awareness program effectiveness.
- Measure culture comprehensively to determine whether a security culture program is effective.

4.6.1 Measure Your Ability to Improve Security-Related Communications

What if some of security culture's woes are self-inflicted (see the "Ineffective Security Communication Styles" section)? Why then it would be useful to measure the progress and effect of efforts to apply the guidance in the "Make Enhancing Communication a Top Security Team Priority" section. CISOs can

- Make a list of recent security communications to stakeholders via briefings, meetings, email announcements, newsletters, posts, and important informal contacts. Have an objective party or audience member rate each on a scale of 1–5 for clarity, fitness for audience (i.e., business or IT), positivity, efficacy, and other desirable attributes. Track these ratings over time.

- Self-assess and ask key team members to self-assess communication skills.
- Get feedback from stakeholders after briefings.

Set targets for improvement based on the data and measure again after a period of time.

4.6.2 Measure the Effectiveness of Security Awareness Programs

We can often measure the effectiveness of programs to promote more secure behavior by analyzing IT artifacts before and after awareness or training campaigns. Examples include events in logs, device or account security configuration settings or passwords, and test results such as the output from phishing simulations. In some cases, one must get creative about identifying IT artifacts that are outcomes of the behavior, such as the number of files flagged for containing sensitive data outside authorized repositories. Still other behaviors don't produce IT artifacts but must be measured by human observation.

For other attributes of the security culture (see Figure 4-1) we can measure norms and attitudes through user surveys, and cognition or compliance through testing and observation.

4.6.3 Measure Security Culture Comprehensively

Some of the industry insights provided in this chapter might not have been realized were it not for *The Security Culture Report 2018*.[15] The results from the report demonstrate the value of being able to measure security culture. Repeating measurements at the organization level enables businesses to understand how their security culture improves or worsens over time and fine-tune awareness, training, and other programs to correct course as needed. Improvements in culture can also be cited in audit or compliance reports as evidence that "people and process" controls are operating effectively.

The CLTRe toolkit[16] measures the attributes of security culture listed in Figure 4-1: attitudes, cognition, communication, compliance, norms, and behavior.

[15]"Security Culture 2018: Measure to Improve," CLTRe AS, Kai Roer, 2018, accessed at https://get.clt.re/report

[16]CLTRe website, CLTRe (a KnowBe4 subsidiary), accessed at https://get.clt.re/the-cltre-toolkit/

4.7 Call to Action

The core recommendation for security leaders from this chapter is to improve security culture through awareness and communications programs as follows:

- Seek executive support for making security culture improvement a strategic objective.
- Devise ways to promote, prioritize, and target awareness programs to improve security culture as well as problematic security behaviors.
- Coordinate awareness messaging and other communications with the executives or managers of the target audiences.
- Focus on role-specific training as well as basic user-related awareness issues such as the vulnerability to phishing messages.
- Target security communications as needed to applicable audiences or groups.
- Obtain support from influencers in target audience, especially for role-specific programs.
- Evaluate how the security organization communicates with businesspeople, and measure how well the communication is received.
- Measure the success of awareness programs and other efforts to improve security culture.
- Measure improvements in security-related communications.

Action – Make a quick assessment of the state of the organization's security culture, communications, and awareness programs.

Ask yourself the following short set of questions and score the answers in the Success Plan Worksheet's[17] Section 3, Table 3. Base your score on whether you would answer most of the questions with a strong "no" (1), a strong "yes" (5), or something in between.

1. Do business executives prioritize and support cybersecurity (i.e., consider it strategic)?

[17] "Rational Cybersecurity Success Plan Worksheet," Dan Blum, Security Architects LLC, May 2020, accessed at https://security-architect.com/SuccessPlanWorksheet.

2. Do business, IT, and development managers provide resources to security projects and help enforce security policies?
3. Do security team members have positive relationships and communications with business stakeholders?
4. Does the security organization treat communicating with IT and business leaders as being a top priority?
5. Are security leaders incentivized to
    a. Maintain regular communication with IT and business leaders in their functional area?
    b. Improve their communication skills and those of their team members?
6. Does the security organization have a user awareness function sized to the business?
7. Does the user awareness and training function
    a. Communicate in an efficacious manner ("we can do this," "here's how others have been [safe, successful]")?
    b. Target awareness programs to specific audiences?
    c. Coordinate programs with the audiences' leadership?
    d. Provide role-specific training?
    e. Recruit champions among the target audiences and "train the trainers"?
    f. Provide information or free tools that will help staff and their families improve cybersecurity at home?
    g. Coordinate with the marketing organization's internal communications program?
    h. Use innovative and entertaining communications mediums, products, or services?

8. Does the security leadership or awareness program itself measure whether awareness and training programs are improving
    a. Security-related behavior?
    b. Attitudes and perceptions about the security program?
    c. Understanding of policies, tools, and procedures (cognition and compliance)?
    d. Compliance audit results?

Action – Define 1–3 improvement objectives for security culture
Note improvement objectives in Section 4, Table 5b, of the worksheet.
The following are examples of security culture–related improvement objectives:

- Continuously maintain the stakeholder engagement table as part of an ongoing personal or team project (especially in larger organizations).
- Assess your communication style or habits and improve at least one practice.
- Get the security team to assess group communication styles or habits and improve at least one practice.
- Create and manage at least one practice for user awareness and training improvement (e.g., task key team members to collect feedback from 1–3 business or IT stakeholders on security-related communications).
- Prepare an informal briefing on security culture (using this chapter as a resource) and present or discuss it with at least one of your business or IT executive sponsors.

Don't limit yourself to these examples. Look for improvement objectives that fit the gaps and priorities you've identified for your business.

CHAPTER 5

Manage Risk in the Language of Business

For too long, information risk management has been lost in translation. Technical risk analyses were unintelligible to the business and even security practitioners lacked common terms, definitions, or analysis models. Without a working risk management framework, security and business leadership have found it hard to agree on priorities, policies, or budgets. Even security teams struggle prioritizing which controls to implement.

But this need no longer be the case. In this Chapter, we'll learn how businesses can use the standard ISO 31000 Risk Management framework, and Open Factor Analysis of Information Risk (FAIR) models as the basis for a comprehensive set of well-aligned processes. Using quantitative criteria such as the monetary value of loss events and the probable frequency of occurrence makes it easier to roll information risks up into the enterprise risk map and report them in the language of business, i.e., dollars, pounds, euros, rupees, etc. We will also discuss ways to assess risk efficiently across a broad class of issues and assets throughout the organization.

Using these recommendations, businesses can

- Understand and employ risk management framework standards
- Establish the context for the risk program (and gain stakeholder buy-in)
- Implement a tiered risk assessment process (and weave it into IT and the business)
- Perform enterprise risk assessments to identify top risk scenarios

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8_5

- Treat risks holistically
- Monitor issues and risks continuously
- Communicate risks to stakeholders effectively

5.1 Address Common Challenges

Despite the availability of standards, the industry still struggles with risk management. And yet risk *is* the reason we have cybersecurity programs. Challenges include

- Lack of consistent information risk terminology and alignment with other enterprise risk domains
- Unrealistic expectations and ineffective risk analysis methods
- Myopic focus on control assessment while ignoring other risk treatment options
- Analysis paralysis and uncertainty about where to start

5.1.1 Lack of Consistent Information Risk Terminology and Alignment with Other Enterprise Risk Domains

Definitions for key risk terminology – particularly "risk," "threat," "vulnerability," and "impacts" – are found in various security standards, guidelines, and other writings. However, these definitions vary widely. Without consistent terminology, business and security teams cannot be certain they are even communicating about risks – let alone develop effective risk treatment programs.

Worse, in some organizations, security staff seem to be running around with the proverbial "hair on fire" syndrome. They treat every single risk-related issue (e.g., vulnerability, threat or pen test report, compliance gap, etc.) as if it were a clear and present danger before even analyzing the business risk scenarios.

Information risk encompasses both true cybersecurity risks from cyberattackers acting on vulnerabilities and IT operational risks from operator error or IT component breakage. Due to its complexity, businesses need security and risk professionals to perform the analyses. However, as discussed in Chapter 1's section "Taking Accountability for Risk," business leaders need to understand information risk in

business terms. Information risk must also be quantified, like financial risk, to roll up from the security organization to the business level.

Fortunately as we'll discuss in section "Understand and Employ Risk Management Framework Standards," the industry has solutions that businesses can adopt for a consistent risk management vocabulary.

5.1.2 Unrealistic Expectations and Ineffective Analysis Methods

Many people who don't understand cybersecurity believe businesses should try to avoid or prevent *all* information risks. Such thinking is valid for life-or-death safety objectives, but many other security objectives should be balanced against the costs or other business impacts of the required effort. It's critical to have an objective framework for such analysis.

Businesses often employ ineffective qualitative methods for risk analysis, and it is still somewhat unusual to find a business using a quantified risk appetite agreed between stakeholders to identify what types and levels of risk are acceptable. Qualitative risk analyses assign ratings such as "low," "medium," and "high" or numerical risk scores. The analyses may rely entirely on subjective criteria, and even expert analysts may have cognitive biases. When business and security leaders can't agree on a transparent and objective method for evaluating risk, communication is difficult.

When expectations are unrealistic and risk analysis processes poorly defined or lacking objectivity, it should be no surprise that the results can be difficult to defend. Business executives will often ask security leaders to present on risk and then challenge the output: "What's in that yellow dot on the heat map anyway?"

As Jack Jones, Chairman of the FAIR Institute, likes to say, "*For most companies, security spend is like the advertising budget. You know you're wasting half of it; you just don't know which half.*"

5.1.3 Myopic Focus on Control Assessment While Ignoring Other Risk Treatment Options

Often cyber-risk teams focus on risk mitigation using controls for reducing risk to the exclusion of other risk treatment options such as avoiding, accepting, disaggregating, or transferring risks. Risk assessment becomes little more than control assessment in which the lack of a control, such as data-at-rest encryption, is automatically assumed

to be a risk. Although that isn't always untrue, it can cause businesses to misjudge both the amount of resources required for cybersecurity and how to allocate those resources. Fortunately, the risk program can incorporate tiered risk assessment methods to triage out unimportant issues, and a holistic risk treatment program can consider all the options to help the business conserve and prioritize resources.

5.1.4 Analysis Paralysis and Uncertainty About Where to Start

In a FAIR Institute risk management maturity survey,[1] only 17% of respondents report having strong risk analysis or assessment practices. Reviewing this survey, the criteria required to be "strong" are somewhat daunting to all but the best-funded and most effective security organizations. For example:

- Putting senior business executives' performance incentives to manage information risk on a par with product, schedule, and financial incentives or other key performance indicators
- Hiring specialists in quantitative risk analysis and threat intelligence and applying a formal quantitative risk analysis model (which may require premium tools and data sources)
- Performing rigorous root cause analysis of all noncompliant conditions
- Conducting regular independent review of risk-based decision-making processes

For a security leader struggling to get business buy-in (another challenge with risk management just like all else security), those tough criteria may seem out of reach. Fortunately for the typical business, a risk program only needs to be "strong enough" in the right areas. The security team would not need to score 100% on the FAIR Institute maturity survey to become effective, and even getting to 60 or 70% could move the needle significantly toward improved cybersecurity program outcomes.

[1] "The Road to Cyber Risk Maturity 2018 Risk Management Maturity Benchmark Survey," FAIR Institute, January 2019

For example, section "Implement Tiered Risk Assessment" explains how some risk analysis processes can be implemented quickly from the bottom up by a small team and distributed to other groups in the organization.

5.2 Understand and Employ Risk Management Framework Standards

If the business has taken steps to establish control baselines, simplify and rationalize IT, and promote the right security culture and governance model, risk management can fit right in as the keystone to these efforts. Businesses just need an organizing framework for it. So, if we could get our organization to implement a risk management framework that was objective and crossed silos, what would it look like? Although multiple framework standards exist (including one from NIST), I recommend these two: ISO 31000:2018[2] for the overall framework and Open FAIR for the quantitative risk analysis model.[3]

5.2.1 ISO 31000 Risk Management

In the ISO model, security and business leadership first set the context for risk. Staff perform risk assessments and risk treatments and monitor risks for changes. Business leadership communicates risk appetite, preferences, and decisions to security leaders. Security leadership communicates new risks, status of known risks, and programs for remediation to all stakeholders. Risk practitioners from IT teams, the CISO, and the Chief Risk Officer (CRO) monitor IT operational risks, cybersecurity risks, and enterprise risks, respectively.

5.2.2 Open Factor Analysis of Information Risk (FAIR)

We recommend using the Open FAIR definition for any kind of risk. FAIR defines risks as "The probable frequency and the probable magnitude of future loss," and, in fact, one can substitute the words "loss exposure" for risk at any time per this definition. Loss exposure, or risk, in FAIR concerns itself with assets that have value which can be lost,

[2]ISO 31000 Risk Management, International Organization for Standardization (ISO), 2018

[3]"Open Group Standard: Risk Analysis (O-RA) (C13G)," The Open Group, 2013. Accessed at https://publications.opengroup.org/c13g (free registration and login required)

stolen, or affected in negative ways. FAIR also describes an ontology of risk component definitions, starting with frequency and magnitude of loss. Once trained on these definitions, business and security people can talk about risk in the language of business.

Many in the industry are aligning on the Open FAIR risk model (shown in Figure 5-1). It provides a comprehensive set of risk terminology definitions and a quantitative method for estimating loss expectancy (i.e., a range of annualized loss).

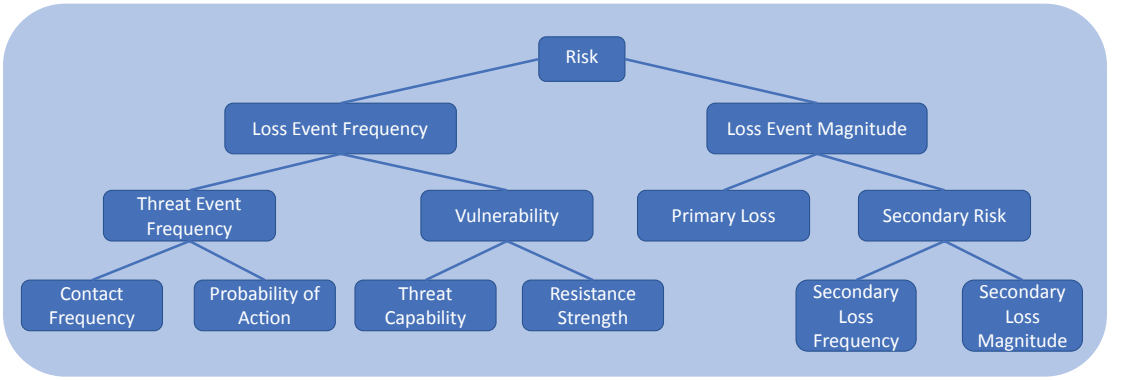

Figure 5-1. *Open FAIR Model*

"RISK" AND OTHER RELEVANT DEFINITIONS

Risk (per FAIR): The probable frequency and magnitude of future loss

Information risk scenario: A threat acting on a vulnerability against an IT or business information asset to produce a loss event

Risk-related issue: Any reported event, circumstance, or concern that could affect one of the FAIR model components (boxes)

FAIR offers a consistent way of describing information risk and performing quantitative risk assessments. FAIR also provides ways to quantify the level of risk assessors' confidence and addresses the multivariate nature of information risk using Monte Carlo simulations. The assessors must have a clear understanding and shared assumptions about the scenario under analysis. Using FAIR-based tools efficiently across a broad range of scenarios requires risk assessors to have considerable real-world experience with the tools and a good storehouse of risk data that is specific to

the business. Performing large numbers of full quantitative analyses requires a level of maturity and some risk analysis tools from the business.

5.2.3 Tiered Risk Assessment Process

I recommend that security teams adopt the FAIR methodology for risk analysis and train security risk professionals and the core security team in FAIR concepts so that they can speak about risk consistently. However, FAIR does not yet include a lightweight method of triaging risk scenarios that can be rolled out to business and IT staff without requiring many hours of training. I'll address this challenge in section "Use a Lightweight Method to Triage Risk Scenarios."

Businesses can come up to speed on FAIR in the spirit of "crawl, walk, run." Initially, train the core security and risk management teams on the model. Develop the capability to use it for in-depth risk assessments. Lightly train business risk owners and IT or security operations leaders to understand FAIR analyses using examples of risk scenarios pertinent to the business. Deepen FAIR adoption over time until it becomes possible, if desired, to replace qualitative shortcuts used for lightweight risk assessments or other needs.

Figure 5-2 illustrates a conceptual risk management framework combining the ISO 31000 and Open FAIR standards. The remaining sections of this chapter cover each major process in the framework.

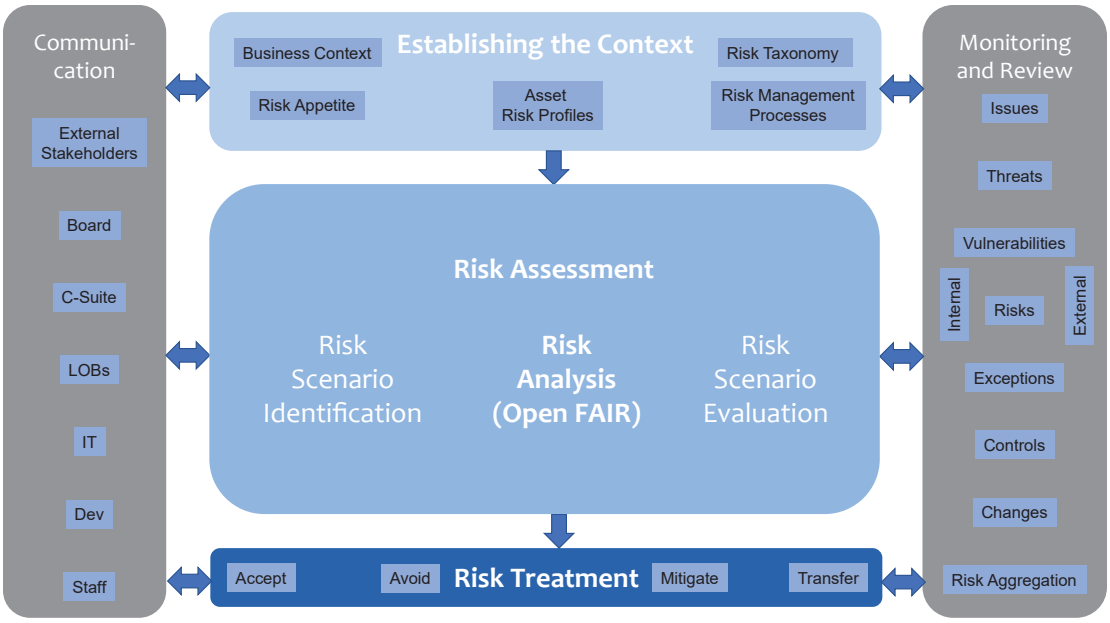

Figure 5-2. *Conceptual Diagram for the Major ISO 31000 Risk Management Framework*

5.3 Establish the Context for the Risk Program

Businesses should define the scope of information risk programs based on the types of assets, regional or organizational boundaries, risk scenarios, or compliance issues to be covered. The following key to cybersecurity-business alignment summarizes a work program to establish the risk context. It also outlines the contents of this section.

5-1

Prepare analysis of business risk scenarios and propose an information risk framework. Socialize the proposed risk framework to obtain broad stakeholder buy-in. Seek top-level sponsorship for the risk management program and formalize risk management accountabilities.

5.3.1 Prepare Analysis of Business Risk Context

Ideally, security leaders have top-level sponsorship up front for investments of time and resources in the risk program. Since that's not always the case, confident security leaders can prepare a business case for the program that includes an analysis of the business risk context and an outline of a proposed risk framework. Consider this required "homework" to gain top-level support and build the actual risk program later.

Consider using PESTLE analysis[4] to understand and document the risk program's business context for risk leaders:

- **Political:** Who are the business and security stakeholders and what is the governance framework?
- **Economic:** How does the business make money? What are the core processes (i.e., sales, marketing, research, value delivery, value development, finance) that could be at risk?
- **Social:** Who are the users, managers, and executives that will be impacted by the risk program, what training will be required, and how to get buy-in?
- **Technological:** In which existing management processes and tools (e.g., IT governance, risk, and compliance (GRC), asset management, IT service management (ITSM), vulnerability management, third-party management, etc.) will risk management capabilities be embedded? What new tools may be required?
- **Legal/regulatory:** What regulatory requirements influence risk management for the business? Do they specify how risk management must be done?
- **Environmental:** Who are the secondary stakeholders (i.e., customers, investors, regulators, society as a whole) that would be impacted by IT outages, data breaches, or other losses?

[4] "What is PESTLE Analysis? A Tool for Business Analysis," accessed at https://pestleanalysis.com/what-is-pestle-analysis/

5.3.2 Outline a Proposed Risk Framework

As described earlier, I recommend using the ISO 31000 risk management framework and Open FAIR for risk analysis. In this chapter, I'll provide additional information on risk assessment, risk monitoring, risk treatment, and risk communication processes for the framework.

Business and IT leaders generally require some education on information risk terminology and a briefing on how the program would work. Develop a briefing describing how ISO 31000 and Open FAIR concepts can be used in a risk management program for the business. Prepare a briefing on the need for a consistent language to identify, describe, and assess threats, vulnerabilities, impacts, and risks as well as an outline of the risk processes required.

5.3.3 Obtain Top-Level Sponsorship

Top-level sponsorship from a CEO, CFO, President, General, Provost, and other top business leaders is fundamental to a risk program. If required, build a business case from the analysis of risk context and, in presenting it, consider the guidance in the "Board Communication" section of this chapter.

However, security leaders need more than the sponsor's signature. They need a formal assignment by the executive of business risk accountability to business leaders and some mechanism for holding business leaders accountable. Businesses can do this in different ways.

STORIES OF BUSINESS LEADER ACCOUNTABILITY FROM THE FIELD

"At the Bank, we had the view that technology doesn't have risk, businesses do. Our role is to help make them aware of the risk and advise them on the alternatives. Our risk acceptance process was based on a simple memorandum. The form explained the risk and if we felt it was egregious ended with a single line that read: ***'Moving forward with this is against the recommendation of the CISO.'*** *The number of these that a business leader filed would have been counted, but we never had one signed off. In the Bank's culture, it was better for the business leader to remediate the issue than to explain why it was necessary to overrule the CISO."*

Steve Katz, CISO

"Business and IT leaders would come before the Corporate Ethics and Compliance Oversight Committee at least once every 2 years to present a self-assessment of the entirety of risk to their business unit. I sat on that Committee along with officers for audit, HR, legal, financial, and other functions. Completing the assessment was a rigorous 6-month process to which each of us would assign a support person to help the business unit understand what was required. The assessment process drove accountability to the business and issues flowed up to the enterprise risk map."

Malcolm Harkins, CISO

Businesses have different ways of holding business leaders accountable for risk, and multiple models can work provided that the idea of managing risk tightly has top-level support. The key is to get security and business leaders collaborating through an established risk management forum (see Chapter 3, section "Risk Management Forums") and to create a risk acceptance process with enough granularity and coverage to take in all issues critical or important to the business.

Locate and work as closely as possible with executive stakeholders responsible for financial risk, operational risk, and other forms of business risk; they may be found chairing or preparing reports for Audit Committees, corporate social responsibility committees, or other compliance-related functions.

5.3.4 Socialize Risk Framework for Broad Stakeholder Buy-in

Stakeholder buy-in for the risk program is required to successfully operationalize it. Security leaders must convince stakeholders of the "why" of, or reason for, the information risk program by explaining the business risk context, outlining the framework, and telling stakeholders how they would be impacted. Often, it is helpful to work through one of the business's top risk scenarios using FAIR analysis with the stakeholders and present the results to top executives as a way of showcasing the proposed methodology.

As noted earlier, a risk management framework could start with information risk (requiring only CISO and/or CIO sponsorship), or it could be integrated into an ERM program with CXO sponsorship. Present the briefing with a proposed risk taxonomy, framework, and processes to the appropriate business, IT, developers, and other stakeholder audiences. The presentation can be tweaked for different audiences and adjusted based on audience feedback.

5.3.5 Define Accountabilities, Risk Appetites, and Risk Processes

After completing the work discussed previously as well as gaining the necessary sponsorship and stakeholder buy-in, security leaders can continue to define and operationalize the risk program as follows:

- **Identify accountability:** Senior business, IT, or security leaders of the company should be identified as strategic risk owners via policy documents or formal memos from the top-level sponsor. Formally define and announce the accountability mechanisms such as signoff memos, self-assessments or performance evaluations, incentive structures, and other measures.
- **Determine risk appetites:** The thresholds for acceptable, unacceptable, and catastrophic impact from information risk often aren't well defined. It can take some analysis and deliberation to tease risk appetites out of the "executive subconscious" into explicit definition. Security leaders can ask questions like: *How long could the electronic order taking system be down before the company takes a material loss?* Then extrapolate the risk appetites for downtime or financial loss based on the answers to such questions. Often, the risk appetite information emerges dynamically whenever staff present risk analyses to executives.
- **Weave risk management into cybersecurity governance:** Governance must encompass core cybersecurity accountabilities and cross-functional coordination functions for risks, operations, and other program functions (see section "Institute Cross-Functional Coordination Mechanisms" in Chapter 3).
- **Plan risk management processes:** Organization-wide processes for developing IT asset risk profiles, performing risk analysis and risk treatment, monitoring, and communication can be formally developed at this point and become part of the risk management context.

5.4 Implement Tiered Risk Assessment

Risk assessment – which in the ISO model includes risk identification, risk analysis, and risk evaluation – is the core of risk management. It exists in a feedback loop with risk treatment and risk monitoring. However, as we discussed in section "Analysis Paralysis and Uncertainty About Where to Start," most businesses haven't yet begun to assess information risks comprehensively in a consistent and objective manner.

The good news is that security organizations can work with IT and the business to triage issues from the bottom up and sort out risk scenarios for quick treatment or further, detailed analysis.

5.4.1 Use a Tiered Risk Assessment Process

Figure 5-3 depicts a tiered risk assessment model that I recommend for clients.

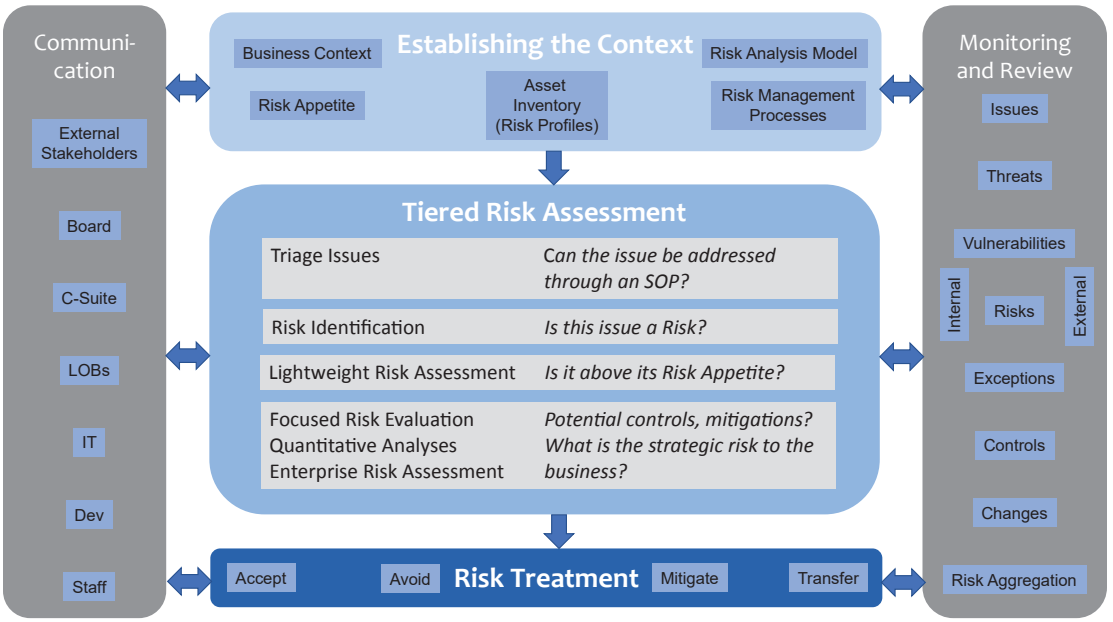

Figure 5-3. *Tiered Risk Assessment Model in the Risk Management Framework*

The tiered risk assessment process is designed to

- Eliminate > 90% of the issues that can be resolved through standard operating procedure (SOP) before they become a significant IT operational risk or a cyber-risk
- Engage business and IT staff in the issue triage and early risk identification processes
- Remediate or gain routine exceptions for > 90% of IT operational and cyber-risks at the business or IT team level
- Focus the resources of the information risk team professionals primarily on the top risks that represent the highest loss exposure to the business

Security Architects Partners, a consulting company I work with, has developed a form of tiered risk assessment called the Agile Risk Management (ARM) Framework[5] and implemented it for several clients. Some examples in the sections that follow come from this framework, and readers can get more detail at the link.

The idea with tiered risk assessment is that staff should first identify which issues in an IT environment are in fact risks and which can and should be resolved through business-as-usual processes. Most issues aren't risks until they exceed defined thresholds derived from business or information risk appetites. Therefore, issue triage should be done as the first step in a tiered assessment process.

5.4.2 Implement Asset Risk Profiling

Often the importance of an issue (such as a vulnerability) is relative to the asset(s) it affects. A tiered risk assessment process needs an easy asset risk profiling method that can be done on the fly whenever potential risk to the asset is identified. The method can also be added to asset inventory processes. An asset risk profile should contain asset risk metadata and an overall asset risk score that represents a quick summary of how the asset could contribute to risk. During triage, staff need only evaluate the asset risk score, but during risk assessment, trained risk advisors should consider more detailed risk metadata collected during the profiling process.

[5]"Agile Risk Management Framework," Dan Blum, Security Architects LLC, January 2020, accessed at https://security-architect.com/RiskManagementResources

IT, development, and LOB staff can easily be trained to use a tool to generate asset risk profiles. It's possible to create asset risk profiles for a single asset, such as a server, or an application or system that aggregates many atomic assets.

5-2

Engage business or IT teams responsible for asset management on creating a flexible asset risk profiling mechanism that can be activated just in time, integrated with ITSM or configuration management database (CMDB) tools, and updated through the change management processes.

The ARM methodology provides a taxonomy for asset risk metadata, a way to capture it on the fly, and the ability to calculate risk scores for first time use on an asset. On-the-fly asset risk profiling can be accomplished in minutes by the asset owner and can populate an existing asset inventory for future reference. Readers can learn more about ARM[5] or devise a similar method.

5.4.3 Identify Issues That Could Bubble Up to Risk Scenarios

Risk-related issues can come from any circumstance or report that factors into one of the risk model components from Figure 5-1. Risk issues include vulnerabilities, software defects, third-party deficiencies, threat or penetration test reports, compliance gaps, audit findings, new business models, and more. But unless an issue can combine with other risk model components (e.g., a threat finds a vulnerability and causes a loss event), there's no risk scenario. Many risk scenarios are highly unlikely to occur. Others can be easily treated.

To triage issues with the ARM framework, staff members can use the *severity rating* of the issue and the *risk metadata* of the asset to look up an issue remediation time window. The easiest way to explain this is to consider a simplified vulnerability prioritization example from a procedure we worked up for a client:

1. Describe the vulnerability issue, such as a new OpenSSL vulnerability affecting 60 web servers. Look up or quickly calculate the assets' risk metadata and match it against the vulnerability severity using the critical, high, medium, or low (CHML) scale provided by most vulnerability management vendors.

2. Look up a remediation time window from a table that matches the affected asset's risk score and the issue severity.
3. Estimate how long would be required following standard operating procedures to close vulnerability issues.
4. Escalate vulnerability issues that cannot be remediated within the remediation time window.
5. Record all issues, issue-to-risk triage outcomes, and issue remediation outcomes in an issue management system, such as Jira.
6. Monitor the issue until it is resolved, and repeat issue-to-risk triage anytime there is a material change to the issue's severity, assets affected, or remediation schedule.

Organizations can use this procedure to triage any type of issue that relates to a specific asset (such as an application). Some issues, such as penetration test reports and audit findings, aren't necessarily specific to a single asset but can affect entire systems, applications, or aggregated assets. No matter. Organizations can tweak remediation time windows, severity values, and other parameters within the procedure.

For issue identification and triage, staff need not be knowledgeable about how vulnerabilities or other issues could affect the assets. They only need to know how to use the triage methodology and to specify how long it takes to resolve the issue. Thus, asset risk profiles and severity scores provide all the context required. Generally, the more important the asset, the shorter the remediation time window.

5.4.4 Use a Lightweight Method to Triage Risk Scenarios

When an issue can't be resolved in time or according to standard operating procedures, it should be escalated for a quick or lightweight risk assessment. Because digital businesses tend to generate many information risk scenarios, risk assessors (in an ideal world) should be able to quickly identify risk scenarios that

- Have already been analyzed and should be treated the same way as a previous scenario
- Exceed risk appetite for the affected information assets and must be escalated for in-depth analysis and reviewed by senior security or business leaders

- Do not exceed risk appetite and can be treated immediately according to the recommendations of the asset owner or risk advisor

This model of lightweight risk assessment could be accomplished by a centralized risk team whose members are trained in the FAIR model, have access to an organized database of previously assessed risk scenarios, and have identified risk appetites (i.e., tolerable amounts of loss exposure) for many types of information assets and business risk owners.

In my experience, even if they like the idea of FAIR, most organizations have only a few resources dedicated to risk assessments. This is true for all but the largest organizations that are most committed to risk management. Yet the typical digital business is either identifying or (often) ignoring many more risk scenarios than a few full-time or fractional resources can deal with.

The need for a lightweight method that nonexperts can use is even more important for businesses committed to a decentralized or agile management approach and a lean centralized security organization.

LARGE TECHNOLOGY COMPANY'S AGILE RISK MANAGEMENT STORY

Early on in working with agile risk management (ARM), a very large client threw us an interesting curve ball: This company is all agile. Not only software development projects, but all projects, use the agile methodology complete with standup meetings, nine-person "squads," and so on. To fit the company culture, our client wanted risk advisors to be part of the agile squad or at least the surrounding "tribe."

My first reaction was: Are you crazy? You can't train that many risk advisors! Over time, however, the idea of engaging large numbers of IT and development staff in the early tiers of risk assessments grew on me. Isn't this what the meme "security is everybody's business" is all about? We developed an online form consisting of questions staff should know the answer to plus some artifacts for lightweight risk assessment customized to the client's needs.

How could a business scale risk management to cover many issues across large populations of users and assets? ARM proposes a Lightweight Risk Assessment (LRA) process based on FAIR that can be used by lightly trained nonexpert staff to prioritize risks by estimating the probable frequency as well as the probable financial, operational, liability, or strategic loss magnitude of a risk scenario. Parameters for estimation are

provided in a lookup table for the staff to use as they go through the LRA by answering a short set of about five questions. Based on these answers, the ARM tool calculates a risk score. If the score is below a certain number, the assessor can select the risk treatment and sign off on the scenario. If the score is too high, the risk scenario must be escalated for in-depth analysis or a higher level of signoff. Either way, the results of the analysis go into an operational risk database for review by the business risk owners and the risk management team.

The Binary Risk Assessment[6] provides another lightweight method. It includes an open source application that asks staff ten questions covering threats, vulnerabilities, protection strength, assets, and impacts. It outputs a low, medium, or high risk rating after staff answer the ten questions. As with ARM, nonexpert asset owners or risk advisors could be trained to answer the questions based on consistent parameters; they could decide on risk treatment for low and medium risks, but more senior leaders or risk management professionals would decide on high risks. The results of all risks that aren't escalated for a higher level of signoff should be documented and periodically reviewed by risk management professionals.

5-3

Use tiered risk assessment processes to engage business, IT, development, and other staff in risk management. Provide automated tools that make it easy for asset owners or risk assessors to triage risks by asking staff role-appropriate questions they should already know the answer to.

5.4.5 Develop Risk Scenario Evaluation Processes

The final phase in risk assessment is the in-depth risk scenario evaluation (or just risk evaluation, per ISO). Detailed risk scenario evaluations should provide a more detailed analysis of how a risk would materialize and a method for ranking potential risk treatments or controls. Such evaluations can include full quantitative FAIR analyses of loss exposure before treatment (aka inherent risk) and after treatment (residual risk). As the core information risk team performs in-depth risk assessments and reviews the

[6]"Binary Risk Analysis," Ben Shapiro, 2011, Whitepaper, accessed at https://binary.protect.io/

results of lightweight assessments and issue triage, it can feed higher risks up into an enterprise risk assessment process.

A tiered risk assessment method could triage 90% of the issues before they became risks and handle 90% of the lower risks in a routine manner. The information risk team for a retail firm with 5000 employees might identify 100 higher risks in a year. Some of the most serious ones could materialize from multiple scenarios and merit more than one assessment. On the other hand, risks dealing with similar issues – such as vulnerabilities, software deficiencies, or audit findings on weak internal controls – might be grouped into a handful of assessments. Having a well-defined process to organize and analyze risk scenarios is important.

Focused risk assessments can be done for any of the following reasons:

- Scenario-based analysis of a specific risk(s)
- Business case development
- Security program planning and control prioritization
- Reporting to regulators, stakeholders, or investors

Scenario-based analysis: Focuses on a single risk scenario or groups multiple related scenarios into one. For example, financially motivated cybercriminals might be able to compromise a web-based ecommerce application at a retail company via any one of multiple vulnerabilities and implant ransomware of different types to cause multiple loss events. Once analysts have developed calibrated estimates for the threat, controls, and impact factors in the scenario, they can perform a quantitative analysis using the Open FAIR risk tool[7] or a commercial system such as the RiskLens product. By following an objective quantitative discipline, the leadership can perform data-driven analysis informed by multiple stakeholder experts (e.g., legal on liability, marketing on reputational, sales on competitive, and IT on remediation cost impacts).

Overall risk input for a business case: The security or risk organization can perform one-off risk assessments for a business case, for example, to get approval for funding mitigation of application vulnerabilities. Risk analysts could calculate the estimated costs to fix the vulnerabilities or to apply other controls for the ransomware scenario and recalculate the Open FAIR analysis with the controls in place. The before and after results

[7]"Introducing the Open Group Open Fair Risk Analysis Tool," The Open Group, March 2018, accessed at https://blog.opengroup.org/2018/03/29/introducing-the-open-group-open-fair-risk-analysis-tool/

yield a return on security investment. For example, one might determine that by using an offsite backup system, incident response upgrades, and multifactor authentication at a total cost of $750,000, the retail company could reduce the ransomware risk (as an annualized loss expectancy) by $5 million.

Report risks to stakeholders, regulators, or investors: In some countries, companies are required to report risks to investors and/or regulatory authorities. In the case of the USA, public companies listed on the stock exchanges must disclose material risks to investors. Recent guidelines by the Securities and Exchange Commission (SEC) establish an expectation that corporations quantify risks being reported.

5.4.6 Perform Enterprise Risk Assessments to Identify Top Risk Scenarios

Sometimes, security leaders are tasked to quantify the aggregate information risk to the business, and CROs may need to do the same for all enterprise risks. More often, security leaders must simply identify the top information risks (aka strategic risks). Data for the enterprise risk assessment can be collected in the following ways:

- **Bottom up:** Collect information from any documented risk assessments. Estimate costs of documented incidents or breaches to the business or similar organizations during recent years. Identify any gaps in the range of issues covered by the assessments; unless there's a healthy mix of assessments from vulnerability- or software defect–related issues, red team and threat-focused issues, and audit findings, consider expanding the set.
- **Business impact assessment (BIA) information:** Obtain any available lists of critical assets identified by the business continuity and disaster recovery (BC/DR) team. Cross-reference known risk scenarios against the assets. Use and improve the BC/DR team's interdependency analysis for critical assets to find the most critical areas of IT and security infrastructure for systemic risk analysis.

- **Enterprise risk map:** Consult the ERM risk map or any list of (noncyber) risks created for the Board or a Board Committee such as the Audit Committee. Attempt to identify information risks that could directly or indirectly factor into the top enterprise risk scenarios that business leaders are most concerned with.
- **Systemic risk analysis:** You may have read about systemic cybersecurity risk to the economy, or financial systems, but what about the risk to your own business? Looking for the top information risk scenarios to "Tier 1" assets from the BIA or the top enterprise risks is a great start, but what might you have missed? Answer: You need to do a BIA for any parts of the security infrastructure, or security program, that the BIA didn't cover. What if your directory, authentication, or key management services go down? What if two or three senior security engineers or responders become unavailable?
- **Infrequent but high impact scenario analysis:** As I wrote in "Waking Up to Cybersecurity's New COVID-19 Reality,"[8] many security professionals treated the early 2020 pandemic outbreak as a theoretical concern and probably missed early opportunities to prepare for a surge in remote access, supply chain risk, and business continuity needs. In hindsight, security leaders should maintain access to data on what the impacts of an infrequent but devastating (outlier) risk scenario like a pandemic could be. Also through risk management processes, prompt risk teams to watch for early warnings of outliers materializing. Although it isn't normally reasonable to overprepare for them, significant outliers should be addressed as a cyber-resilience issue (see Chapter 9's section "Develop Contingency Plans and Cybersecurity Strategy for Resilience").

After all major risk concerns have been collected, normalize them using the FAIR model. Group closely related risk scenarios together. Rank using a rapid or exhaustive quantitative estimation methodology. Determine a risk appetite or maximum tolerable

[8]"Waking up to Cybersecurity's New COVID-19 Reality," Dan Blum, March 2020, accessed at: https://security-architect.com/waking-up-to-the-new-covid-19-cybersecurity-reality/

loss. Present the risks on the list that exceed the risk appetite as the "top risks." Maintain the list of top risk scenarios as events warrant between major refreshes of the enterprise risk assessment.

GLOBAL HIGH TECHNOLOGY MANUFACTURER CISO'S ERM STORY

"Prior to being the head of security at the company, I'd worked in various business units, including the controller's department. At our Corporate Ethics and Compliance Oversight Committee, I found the enterprise risk map. I brainstormed with the executives whose teams had analyzed these risks to learn how cybersecurity issues might contribute to them.

As of the early 2000s, the risk map had 9 items including sole source factory failure, competitive core products, and antitrust actions. I was able to weave direct or indirect cyber-risk causal scenarios into 2 of the top enterprise risks. During a similar exercise in 2015, I found an enterprise risk map with 25 items and wove 18 cyber-risks into them. I believe this shift has occurred for almost every company. Today, for example, ransomware could be a major risk driver to sole source factory controllers and logistics systems."

Malcolm Harkins, CISO

5-4

Work with the executive responsible for preparing the enterprise risk map for the Board. Weave direct and indirect information risks into the risk map. This exercise will increase the relevance of cybersecurity and educate security leaders on senior executives' perception of business drivers, business risks, and risk appetites.

5.5 Treat Risks Holistically

Risk treatment can take four forms: accept, avoid, transfer, or mitigate the risk. And yet, many security leaders put practically their entire focus on mitigation through applying controls such as those in the control baseline from Chapter 6.

> "To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."
>
> **Sun Tzu, *The Art of War***

5.5.1 Formalize Risk Acceptance and Risk Exception Processes

When a risk owner decides not to treat a risk, the risk should be formally accepted. Otherwise, the business is open to accusations of not having a competent risk management program or, worse, of covering up risks that it could reasonably be expected to recognize. Once accepted, risks should be periodically reviewed.

A risk exception process is subtly different from risk acceptance. Risk acceptance is explicitly acknowledging a potential loss exposure and allowing it to continue. A risk exception, on the other hand, is a temporary acknowledgment of noncompliance with policies, laws, or regulations that is also creating exposure to loss, but that the business intends to remedy.

The exception process should include signoffs, require compensating controls in some cases, and make exceptions temporary in nature. Also, as changes to the IT environment or the threat environment unfold, the information risk team should monitor accepted risks in the registry for material changes to their probability of materializing or impact worsening.

5.5.2 Educate the Business on Risks to Avoid

In some cases, business leaders choose to avoid risk. For example, a retail business might decide not to engage an out-of-country credit card processing service provider due to concerns about transferring customers' personal data across borders in violation of national privacy regulations in some jurisdictions. The time spent educating business leaders, IT leaders, developers, and staff on risk pays dividends later. Security-related processes can also proactively provide IT and business leaders with other options. For example, Chapter 7's section "Manage Cloud Risk Through the Third-Party Management

Program" describes a financial institution's third-party risk management case study. If an LOB proposes to use a vendor with a high risk score, the security team can explain the issues with the vendor and propose alternatives to stakeholders during a 30-minute meeting.

5.5.3 Share Responsibility, Outsource, or Obtain Insurance to Transfer Risk

Transferring risk to a third party isn't always possible, and often only some of the risks can be transferred. The adage "You can transfer responsibility but not liability" is usually true. Because risk transfer isn't a perfect solution and requires much nontechnical input into the how-to, security professionals often tend to overlook or neglect it. However, businesses should take advantage of the following risk transfer opportunities:

- **Implement a framework for determining third-party shared responsibilities, service-level agreements (SLAs), and contracts:** Contracts with third parties can often induce them to reduce risk more efficiently than the business could through its own efforts. SLAs provide a way to measure third-party efforts and assess any third-party deficiencies. (For more information, see Chapter 6's section "Apply a Shared Responsibility Model to the Control Baseline.")
- **Consider whether cyber-insurance is right for the business:** Cyber-insurance is a type of general insurance that covers information risks. First-party cyber-insurance covers direct losses to the business from breaches, outages, or other incidents. Third-party coverage addresses secondary losses from claims and legal actions against the business as a result of information risks. Cyber-insurance can make a lot of sense as part of the cyber-resilience strategy, especially when a business knows it cannot afford to cover high impact losses but does not see a good return on security investment from trying to mitigate them because they occur too infrequently. Also, cyber-insurance may be required for credit agreements or other contracts. In such cases, cyber-insurance could keep a small company out of bankruptcy and preserve even a larger, financially strong organization from credit downgrades or steep stakeholder losses. Also, carrier-provided

breach response and other services can be helpful. See Chapter 9's section "Develop Business Continuity and Disaster Recovery Plans" for more information.

5-5

Think outside the box of risk mitigation controls to develop a robust set of risk transfer practices. Consult the legal team on contracts and cyber-insurance, the finance team on cyber-insurance, and the vendor management team on contracts and shared responsibility frameworks.

5.5.4 Evaluate Business Changes and Controls for Risk Mitigation

Security leaders often focus almost all their attention on creating new controls or bringing an existing control to bear on a new risk because that is, well, what they can control. However, risks can also be mitigated by business changes to process, partners, facilities, or activities as well as controls. Perhaps being able to help business or IT leaders and staff find more secure options for getting their work done without having to implement additional controls *is* the "acme of skill" from the Sun Tzu quote at the beginning of this section. For example, an LOB could consider modifying privacy-related business practices (such as collecting or reselling personal information without consent) that might violate regulations.

All this being said, at least some of Sun Tzu's "one hundred victories" must come from "battles" or the use of actual security controls. In Chapter 6's section "Develop Architectural Models and Plans for Control Implementation," we recommend developing an initial control baseline and security architecture road map for building the controls. For the ARM project, we developed a Control Library that helps clients track which of the NIST Cybersecurity Framework controls and/or customer-defined controls are required, how they are implemented, and in which IT environments. Similar artifacts are available in some IT governance, risk, and compliance (GRC) systems.

During focused risk assessments, analysts can determine "what if" risk treatment options, assessing and evaluating the effectiveness of potential controls and other mitigation or transfer options. Using metadata about the controls (such as strength or type), they can select the right ones to apply to each risk scenario.

After selecting one or more controls for treating a risk scenario, analysts can update the IT GRC system or Control Library with the control information. In this way, the security team keeps the control baseline continuously risk informed.

5.6 Monitor Issues and Risks Continuously

The risk management framework must monitor known, new, and changing risks. It must track them in issue management systems and operational risk registries. Not all risks can be treated up front, and risks change over time. Monitoring risks is often as important as analyzing them in the first place.

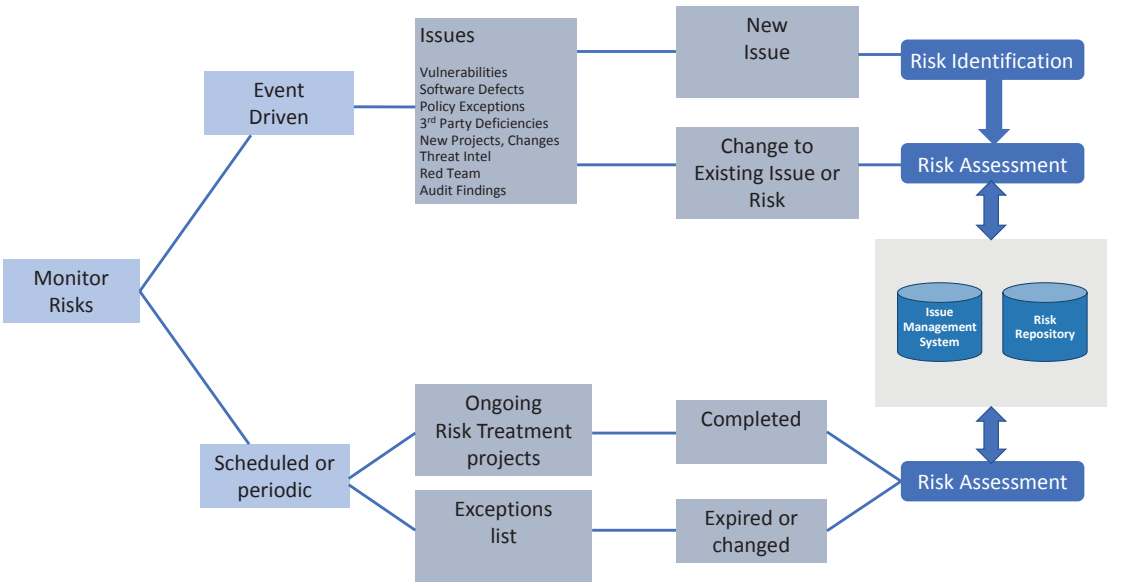

Figure 5-4. *Monitoring Risks and the Risk Management Program*

As shown in Figure 5-4, risks should be monitored on an event-driven basis as well as through scheduled or periodic review.

- **Issues:** Risk scenarios can develop from the types of issues shown in Figure 5-4. Some – such as threat intelligence that cyberattacks exploiting a known third-party deficiency are increasing against an LOB – may recur over and over. They may need to be reanalyzed

from time to time and may prove to have higher or lower ratings than before. If so, security business leaders should reevaluate existing treatments or exceptions for these risks.

- **Risk treatment projects:** Review risk assessments whenever a risk treatment project or activity completes; for example, a new technical control mitigating access risk is ready to move into production, or a cyber-insurance policy expires and is offered again at similar terms. For the top risks in the business, reviews may also be required when treatment milestones are missed and/or at arbitrary time intervals. If residual risk remains and is higher than required thresholds, escalate the risk for new exception signoffs and/or new risk assessments.
- **Exception lists:** Review the risk assessment for a risk whenever an exception expires. If the risk is still higher than the risk appetite, escalate the risk for new exception signoffs and/or risk assessments.

5.7 Communicate Risk to Stakeholders Effectively

Risk should be the common language for communication between security and the business. The risk framework provides the feedback loop to collect information for risk analysis and treatment and to communicate risks to stakeholders. In alignment with the CRO and the ERM program, CISOs can communicate effectively at multiple levels with

- Business staff and associates
- Business risk owners
- Board of Directors and Executives

5.7.1 Business Staff and Associates

Employees of the business, long-term contractors, and even third parties are – to a greater or lesser extent – part of the risk program. For one of our clients using ARM, multiple business and IT staff will take on risk advisor roles. Still more staff in that company and others like it will perform the issue-to-risk triage process. The risk program can make staff more conscious of the risk dimension to their day-to-day duties and well versed in the use of issue and risk management tools and processes.

To engage the business staff and associates, organizations of all sizes should

- Provide information on basic security issues all organizations face and generic risk scenarios through security awareness programs

Larger organizations, especially ones under high security pressure should

- Create awareness, training, and communications channels for risk-related roles such as business risk owners, risk advisors, asset owners, and data stewards.
- Identify potential risk management champions among the staff being trained or prepped for risk management roles. Assign individuals on the information risk team to recruit or mentor champions, and work with them to provide informal meetings and other communications to the business and IT.
- Work with HR and/or LOB managers to ensure appropriate performance goals and incentives for those in the champion roles.

5.7.2 Explaining Risk to Business Risk Owners

Business risk owners include CXOs and – in larger organizations – also LOB, IT, or development leaders. They are accountable for effective risk management and vested with the authority to accept known risks and/or allocate resources to treat the risks. As we discussed in the section "Establish the Context for the Risk Program," businesses should make such accountability explicit and tangible through a visible business process. Security and risk leaders can provide role-specific training and communication channels for the business risk owner role.

Security and risk leaders should

- Advocate for explicit accountability to business owners for working with the risk management program to define risk appetites, risk treatment, and formal risk acceptance
- Seek and maintain informal relationships with business risk owners and any business information security officers (BISOs) outside of the enterprise security department in a large organization

- Bring training and awareness efforts to life by helping business leaders recognize risk scenarios that can materialize from information risk
- Advocate for business leader participation in security steering committees or forums

5.7.3 Board Communication

The Board of Directors is accountable for oversight to ensure the business accomplishes its mission, such as delivering investment returns to owners, providing services, or meeting other key objectives. Most Boards for larger organizations maintain committees, such as an Audit Committee. Risk management often lies within the Audit Committee purview, but some financial services and other highly regulated companies maintain a separate Risk Committee or another compliance-related forum. Some Boards in the defense industry or critical infrastructure industries maintain a Cybersecurity Committee due to the strategic upside as well as downside importance of safely aligning operational technology (OT) with information technology (IT).

WHAT'S THE STORY ON BOARD-LEVEL ENGAGEMENT?

In general, many Boards still struggle to address information risk oversight. Engagement remains low in critical areas; for example, a recent Shared Assessments group survey[9] found only 32% of respondents stating that their Boards have a "high engagement and level of understanding" on the important topic of "cybersecurity risks relating to vendors."

According to knowledgeable sources I interviewed such as Professor James Tompkins (Kennesaw State University) who researches corporate governance and Board-level risk oversight, there currently is no standard format for the risk documents or presentations (i.e., risk registers or risk maps) that Boards receive. However, Boards always want to know what the top risks to the company are and to understand or

[9] "Vendor Risk Management Benchmark Study: Running Hard to Stay In Place," Shared Assessments Program and Protiviti, April 2019, accessed at www.prnewswire.com/news-releases/2019-protiviti-and-shared-assessments-survey-finds-board-involvement-a-key-indicator-of-vendor-risk-management-maturity-most-organizations-will-drop-vendors-to-de-risk-300827875.html

quantify them in business terms such as lost revenue, delayed product delivery, breach recovery costs, opportunity costs, competitive impairment, and so on.

To ensure they can oversee information risk effectively, security leaders can advocate that as an industry best practice, Boards should

- Include at least one member who is knowledgeable about cybersecurity. Though technically literate, this individual(s) need not be highly technical; it is more important that they have a deep background of business experience with cybersecurity from previous roles.
- Maintain a committee structure well suited to the oversight of risk management.
- Have direct contact with the security leadership and ensure their alignment with the business and their support from the business and that they obtain the resources required to run a cybersecurity program.

In leading companies, the CISO presents to the Board Audit (or other) Committee meetings regularly. For many businesses, there is a cybersecurity, or risk, agenda item for the CISO to present to full Board meetings at least once a year. The CISO may also present on significant security incidents (such as the breach of the business or one of its competitors) on request.

5-6

Advocate for more Board engagement on information risk, but don't assume Board members have time to acquire much technical knowledge. Always communicate risks in terms of business impacts. Keep presentations concise and actionable.

Security leaders should

- Advocate for effective Board information risk oversight through personal contacts with existing Board members and top executives, providing copies of National Association of Corporate Directors (NACD) information risk–related guidance and offering to invite Board-level security experts from other organizations to visit or speak.

- Advocate for the CISO's ability to regularly brief the Board and Board Committees on information risk programs. Regardless of where the CISO reports in the organizational hierarchy, this engagement will help the CISO understand the top-level business requirements better and be more effective in the role.
- Maintain informal relationships with individual Board members, especially those chairing key committees covering risk and/or technology-savvy Board members.
- Coordinate information risk reporting with the CRO or whichever function in the organization handles ERM.

When presenting to the Board (or making executive presentations in general), keep the content simple, short, and to the point with backup information available at need. Avoid getting into technical detail but do focus on the organization's cybersecurity situation, on the top risks, the program for managing those risks, and any executive actions or support requested. For more tips, see Chapter 4's section "Make Enhancing Communication a Top Security Team Priority."

Content typically presented in board presentations is generally unsatisfactory according to Catherine Allen, CEO of Santa Fe Consulting and a Corporate Board member. "The worst of it is PowerPoint presentations, death by PowerPoint. Pictures are good but don't contain enough detail. Bulleted lists are better but either tend toward verbosity or leave out details." Allen provides a piece of advice to CISOs presenting to Boards: "The best option for me has been to see infographics."

Even if the Board holds the CISO in high regard, it may demand independent third-party assessments of the security program itself. The security leadership should support such assessments. Additionally, CISOs should help the Board get benchmark data when requested on what other organizations in their industry are doing for cybersecurity. This information is available from trade press articles, Information Sharing and Analysis Centers (ISACs), and the CISO's own network as well as independent research companies.

5.8 Call to Action

The core recommendation for security leaders from this chapter is to manage risk in the language of business as follows:

- Establish the context by adopting a consistent framework – I recommend the combination of ISO 31000, Open FAIR, and a tiered risk assessment process.
- Obtain top-level sponsorship and establish clear business risk owner accountability.
- Work with the IT and business teams responsible for asset management on creating a lightweight asset risk profiling mechanism.
- Create a tiered risk assessment process.
- Develop a focused risk assessment or risk evaluation method to select controls and other risk treatment approaches, including risk acceptance and risk transfer processes.
- Work with the executive responsible for preparing the enterprise risk map for the Board and weave direct or indirect information risks into the list.
- Monitor issues, risks, top risks, risk treatments, risk acceptances, and risk exceptions.
- Create risk communications programs tailored to staff, managers and stakeholders, and the Board.

Action – Make a quick assessment of the state of the organization's information risk management program.

Ask yourself the following short set of questions and score the answers in the Success Plan Worksheet's[10] Section 3, Table 3. Base your score on whether you would answer most of the questions with a strong "no" (1), a strong "yes" (5), or something in between.

[10]"Rational Cybersecurity Success Plan Worksheet," Dan Blum, Security Architects LLC, May 2020, accessed at https://security-architect.com/SuccessPlanWorksheet

1. Are business owners held accountable for information risk?
2. Are business, IT, and security teams using consistent terminology for discussing risk and consistent criteria for assessing risk?
3. Are stakeholders coming to security for guidance or advice before taking important decisions that could create risk?
4. Are risk assessments used to prioritize security projects, manage third parties, or make other decisions?
5. Is a quantitative risk analysis methodology in use?
6. Are issues, risks, exceptions/acceptances, and top risks monitored in an issue management system; IT governance, risk, and compliance (IT GRC) tool; and/or risk register?
7. Are top information risks being regularly communicated to executives and the Board, and is the dialogue constructive?

Action – Define 1–3 improvement objectives for risk management

Note improvement objectives in Section 4, Table 6, of the worksheet. The following are some guidelines and examples.

If the business doesn't yet have a formal information risk management program, look for improvement objectives in the section "Establish the Context for the Risk Program." For example:

- Perform a PESTLE analysis[4] to understand and document the risk program's business context and discuss it with at least one business or IT executive sponsor.
- Task security and risk team members unfamiliar with FAIR to read section "Open Factor Analysis of Information Risk (FAIR)" and the Open Group Standard: Risk Analysis (O-RA)[7] and other FAIR resources.[11]

[11] "FAIR Resources," Dan Blum, Security Architects LLC, January 2020, accessed at https://security-architect.com/RiskManagementResources

To improve a risk management program that's up and running, consider the following sample improvement objective:

- Review the organization's asset inventory program and identify an IT champion willing to work with the risk management function on devising a method to capture asset risk scores and risk metadata as described in section "Implement Asset Risk Profiling."

To improve the identification of top information risk at the executive level, consider the following sample improvement objective:

- Meet with executive stakeholder(s) responsible for reporting risk to an Audit Committee (or other risk management forums). Identify or discuss
  - Who are, or could be, accountable risk owners for categories of information risks?
  - Potential overlaps between information risks and top enterprise risk scenarios

Don't limit yourself to these examples. Look for improvement objectives that fit the gaps and priorities you've identified for your business.

CHAPTER 6

Establish a Control Baseline

All security programs depend on having some basic controls, called a control baseline, in place. After all, one would not deem a house or an office "secure" without locks on the doors to control entry.

There are many technical and nontechnical controls that a business *could* implement, but few businesses have the time, money, or inclination to implement them *all*. Some guidance is needed to determine which controls are most needed, and to that end the industry provides various standard control frameworks.

Some control frameworks – such as the International Organization for Standardization (ISO) International Standard 27001 and the National Institute of Standards and Technology (NIST) Special Publication 800-53 – contain many granular controls. Others such as the Center for Internet Security's Top 20 Critical Security Controls provide a more minimalistic list.

This chapter provides a Rational Cybersecurity take on the minimum viable control baseline by identifying core control domains and guidance for choosing granular controls based on the business's unique needs. It also focuses on specific requirements for alignment with IT or business groups to implement or operate each type of control effectively.

Security leaders can use the information in this chapter to establish a control baseline by

- Selecting a list of controls scaled for a business of their type and size
- Developing an architectural model and road map for implementing the controls across the business or prioritized environments
- Prioritizing deployment phasing across various IT environments using risk management

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8_6

- Sharing responsibility for control operation with third parties, such as cloud service providers (CSPs)
- Aligning control operation with appropriate IT, development, corporate administration, and line of business (LOB) groups

6.1 Understand Control Baselines and Control Frameworks

Businesses require a written policy that states how they will address security. Organizations have a legal obligation to adhere to their own policies, and in some jurisdictions or industries, policies are required to address specific security objectives such as safety or privacy. A complete security policy encompasses multiple documents, including formal definitions of the controls the business will implement.

Security leaders understand controls. Still, the terms "control framework" and "control baseline" – which are different terms for a "list of controls" – get tossed around and used in different ways.

What Is a Control Framework?

A control framework is a list of *control objectives*, or security requirements, such as "Physical devices and systems within the organizations must be inventoried." Notice this example says *what* the organization is supposed to do, but not *how*. Usually, subordinate policy or procedure documents detail control activities.

The security industry is replete with helpful standards for security control frameworks. Some of the most important ones are

- NIST SP 800-53 rev 4[1] (controls for US Federal information systems and organizations)
- ISO 27001[2] (management system and reference controls) and 27002[3] (code of practice and implementation guidance)

[1] "NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations," NIST, April 16, 2018. Accessed at https://doi.org/10.6028/NIST.SP.800-53r4, April 2013

[2] International Standard ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements (second edition), ISO/IEC, 2013

[3] International Standard ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls, ISO/IEC, 2013

- ISACA COBIT[4] framework for enterprise IT governance and management
- Cloud Security Alliance (CSA) Cloud Controls Matrix,[5] which provides a useful cross-reference to many of the other frameworks

Some compliance regulations define their own control frameworks, others reference one or more general-purpose control framework standards. For example, US Federal Government regulations such as National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171[6] reference both NIST and International Organization for Standardization (ISO) control frameworks, but map more specifically to NIST's own control frameworks. A control baseline for a contractor covered by NIST 800-171 would need to reference the NIST control frameworks.

6-1

Work with the legal team(s) and lines of business to list compliance regulations that apply to the business. Use this list to determine which standard control frameworks the control baseline should reference and which objectives or activities it should comply with.

When compliance requires a specific control, such as data-at-rest encryption, it may be necessary to implement it. Beware, however, of falling for the following myth. Always look beyond compliance to assess the top risks to the business and the controls they imply.

6

Compliance to a regulation or a checklist of controls equals (or guarantees) security.

[4] *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*, ISACA, 2012. Accessed at www.isaca.org/cobit/Pages/CobitFramework.aspx

[5] CSA Cloud Controls Matrix v3.0.1, March 2019. Accessed at https://cloudsecurityalliance.org/research/cloud-controls-matrix/

[6] "NIST Special Publication 800-171 Revision 1: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," NIST, December 2016, accessed at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

What Is a Control Baseline?

The work of security is never done. Nonetheless, the security leadership should be focused on a "minimum viable product" for the outcomes it delivers. What we mean by a "control baseline" is the minimum set of security controls specified for a business IT environment and applicability guidelines to where they apply. For example, some controls might apply to systems with confidential data but not to systems with public data. Other controls might only be implemented for newer versions of applications or operating systems that the organization considers "strategic" and not for capabilities that are being phased out.

What Do We Mean by Establishing a Control Baseline?

Establishing the control baseline is the process of implementing it for actual IT systems. The organization must not only specify a minimum viable set, it must prioritize which business units, regions, or systems implement which controls. Once implemented, it must verify the controls are operating correctly and sustain them.

6.2 Address Common Challenges

The industry is mature in understanding what security controls could be implemented, but immature about prioritizing them in a risk-informed way, organizing them in a coherent architecture, and engaging business stakeholders in the work of implementing controls. The following issues continue to challenge businesses:

- Too many controls? Seeing the forest through the trees
- Difficulty risk informing controls
- Controls without a unifying architecture
- Lack of structure for sharing responsibility with third parties
- Controls out of line with business culture

6.2.1 Too Many Controls?

The standard control frameworks each contain hundreds of control objectives and many additional guidelines or requirements for control activities. We are inundated with an abundance of information, often conflicting terminology, oversight requirements, and

products which can be overwhelming for smaller organizations and anyone just getting started. Even larger organizations and experts struggle to see the forest for the trees. Recognizing this challenge:

- **The Center for Internet Security (CIS) maintains a list of the "top 20" security controls**[7] curated through a community of IT experts. Its stated goal is to help practitioners see through the "fog of more" and identify a set of prioritized actions based on best practices for defense in depth.
- **NIST publishes a Cybersecurity Framework**[8] as a higher-level, more business-accessible list of controls that also provides pointers to the granular NIST 800-53, ISO 27001, COBIT, and the CIS top 20 controls.

Despite the NIST and CIS efforts, I'm not convinced they have produced a minimal viable control baseline. Although NIST CSF provides a very useful way of looking at controls, there are over 100 of them. Enumerating all the subcontrols that detail the CIS makes its baseline much more numerous than 20. And although the CIS 20 covers cybersecurity technology well, it doesn't cover the people and process behind it with the same rigor. The idea of an industry control baseline is something of a myth.

There exists one control baseline that is suitable for every business.

7

Readers might be wondering, if that's the way I feel about control baselines, why this chapter? My answer is that although no one control baseline can fit every business or IT environment perfectly, businesses should still develop an overarching control baseline as part of the high-level security policy and use it as a yardstick in selecting controls for each of its IT environments.

To help that effort, I've identified 20 control domains (or groups of controls) later in this chapter and provided guidelines for selecting granular controls within them.

[7] "CIS Controls V7," Center for Internet Security, March 19, 2018. Accessed at www.cisecurity.org/controls/

[8] "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1," National Institute of Standards and Technology, April 16, 2018. Accessed at www.nist.gov/cyberframework

6.2.2 Difficulty Risk Informing Controls

Many think risk management is something you do *after* the security program becomes sufficiently mature rather than a vital component that helps get the program off the ground and guide the program *while* it matures. Another challenge is the industry's relatively low level of risk management maturity. Practitioners still struggle because

- Selecting controls based on risk scenarios is currently more of an art than a science.
- Operationalizing risk management throughout the enterprise also requires mature, risk-informed asset and vulnerability management, third-party management, and other processes.
- It is sometimes difficult to determine which controls are reducing risk less than others and should be decommissioned during a budget cut or reallocation process

6.2.3 Controls Without a Unifying Architecture

Today's digital businesses must implement controls in a hybrid multicloud environment and address a burgeoning crop of regulatory requirements across the international market landscape. Larger enterprises face additional complexity from multiple generations of IT infrastructure and applications.

One can make all the right moves by identifying the greatest risks and the controls to treat them, but without architectural alignment, controls may not be effective. Many organizations have acquired a lot of security tools needed to implement controls. But because they haven't planned how to integrate those tools with other tools and processes, they get little value.

How should businesses develop the control architecture? Like the NIST CSF, I recommend starting with a basic cybersecurity and risk assessment. In the section "Develop an Architectural Model and Plans for Control Implementation," we cover this critical step to align the control baseline with the operational security environment.

6.2.4 Lack of Structure for Sharing Responsibility with Third Parties

When a business relies on a third party to operate its systems, some of the controls may be operated by the third party and some by the business, and they must coordinate their efforts. To be effective, the business control baseline must be aligned with the third-party controls through shared responsibility models.

Shared responsibility has proven difficult for the industry to address through existing control frameworks. To solve shared responsibility, we need to focus on what the business is doing with a system provided with the aid of a third party (the "use case"), what controls it can operate for itself, and what controls the third party operates. The section "Apply a Shared Responsibility Model to the Control Baseline" provides guidance on how to analyze and define shared responsibilities.

6.2.5 Controls Out of Line with Business Culture

Risk and regulatory considerations incline security departments toward implementing restrictive controls on users, but one must be careful not to get in the way of business growth and agility. Digital business requires exploiting technology in innovative ways. It's all too easy for security teams and business staff to work at cross-purposes, as in

- Security policy writers create control standards and requirements without engaging the business to learn whether the requirements are practical or provide guidance on how the business can best meet the requirements.
- IT or LOB executives turn a blind eye to some security policies and don't tell security teams in advance about all their digital innovation or procurement plans.
- Developers use "port agility" to get traffic through the firewall even as the network security team tries to block it.
- IT administrators kill the security team's privileged access management (PAM) initiative with passive-aggressive or uncooperative behavior.

Control objectives, or principles, such as least privilege (i.e., designing systems and processes to minimize privilege grants to users or administrators) are well enough in theory but often difficult in practice. Overly restrictive controls at the user level can create negative staff perceptions about security, potentially leading staff to withhold cooperation and make the controls less effective. Impeding business efforts to innovate in pursuit of business objectives can reduce business leader buy-in for the security program and tends to prove futile as the business wins many – if not most – arguments with security.

Security leaders should discover and confirm how controls can align with the business as a check on the initial control baseline and for implementation guidance. See section "Align Control Deployment and Business Functions" further on in this chapter.

6.3 Select a Control Baseline from the Essential Control Domains

Creating a control baseline is a useful exercise for security professionals regardless of whether you're starting with a blank slate in a new position or trying to validate an existing control baseline. Take the control domains in Table 6-1 coupled with the guidance in this section as a starting point for creating a control baseline that fits your business.

Table 6-1. *Rational Cybersecurity Control Domains*

Control Domain	Summary Description
Security governance	Govern security roles, responsibilities, decisions, and strategy.
Risk management	Create a taxonomy framework and processes to identify, assess, treat, monitor, and communicate risks.
Security policies and awareness	Document security requirements for people and systems. Publicize them and motivate or empower users to follow them through user awareness training.
Asset inventory	Discover IT assets, profile their risk, and identify all critical assets as well as asset owners.

(*continued*)

Table 6-1. (*continued*)

Control Domain	Summary Description
Third-party management	Discover third parties, profile their risks, and manage shared responsibilities for security.
Network security and zoning	Protect network security, arrange IT assets in physical network segments or logical compartments (i.e., "zones"), and provide perimeter protections to the zones.
Authentication, user account management	Manage employee, contractor, and other users' accounts; authenticate access to those accounts.
Access management and authorization	Enable asset owners to ensure that authenticated users can only access resources as prescribed by business policies.
Security configuration and change management	Configure IT systems and applications in a secure manner and control changes to policies, configurations, documents, and code.
Data protection	Classify and discover sensitive information. Apply encryption, tokenization, or data leakage protection (DLP) on data in motion, at rest, and in use.
Secure software development and application security	Follow secure software development lifecycle (SDLC) and/or DevSecOps standards and practices in development projects.
Vulnerability management	Scan IT systems and applications for software, hardware, or configuration vulnerabilities; prioritize and remediate vulnerabilities.
Physical security	Monitor and protect the business's physical facilities to safeguard the users and assets within the facilities as well as the facilities themselves.
Secure HR practices	Perform background checks and ensure that people-related security practices (e.g., background checks) comply with laws and good practices.
Real-time threat detection	Detect hacking, malware, and abuse against IT systems and devices; generate alerts to security monitoring systems; and triage alerts for effective response.

(*continued*)

Table 6-1. (*continued*)

Control Domain	Summary Description
Logging and log review	Generate and collect event logs of security-relevant information in keeping with security standards; review logs to detect threats or compromises of IT systems.
User account monitoring	Monitor both standard user accounts and privileged user accounts for unauthorized, unusual, or suspicious activity.
Incident response	Identify and investigate all types of incidents, contain threats, eradicate malware or damaged configuration, recover, and learn from incidents.
Backup and data recovery	Back up data, configuration, and code of IT assets in a secure manner and test the ability to perform data recovery.
Business continuity	Identify critical assets, create procedures and facilities to recover their functionality within a specified time in the event of outage, and test recovery.

The remainder of this section aligns the Rational Cybersecurity control domains with the NIST CSF and provides guidance for readers to use in selecting at least a minimal set of controls from most or all domains to form their business's control baseline. For each control domain, the text identifies

- **Definition:** Brief definition of the control domain.
- **Description:** Describes requirements for the control domain broadly aimed at attaining the Level 3, or "Defined" maturity level. Recall from Chapter 1's section "Maturity," Figure 1-6, that attaining the Defined maturity level requires that security roles, responsibilities, and policies be defined and established in at least some areas, but only requires manual means of verification.
- **Business dependencies:** Identify the business functions that tend to be involved with the control domain deployment, for example, IT and development managers for security configuration and change management and HR for secure HR practices. Table 6-3 in section "Align Control Deployment and Business Functions" summarizes a master table of control domains and business interdependencies.

6.3.1 Serve Up a Balanced Diet of Controls

As shown in Figure 6-1, the NIST CSF structures controls into the five primary defensive security categories.

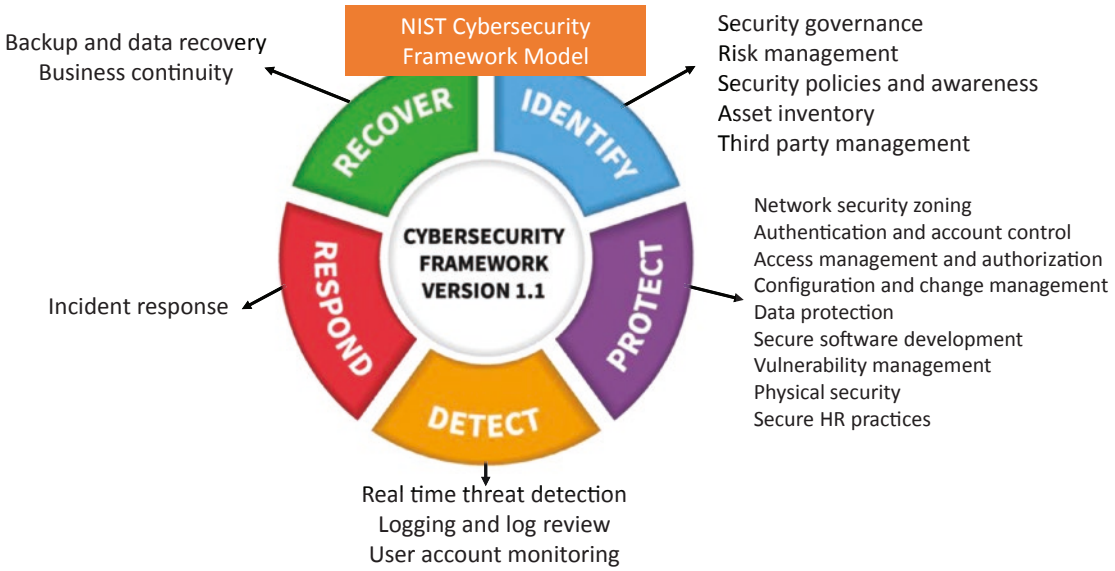

Figure 6-1. *Control Domains in Terms of NIST CSF*

I've noted where each Rational Cybersecurity control domain falls around the NIST CSF "wheel." It's not an exact mapping; some control domains like network security zones and physical security have both "protect" and "detect" properties. But it should give readers an idea of how the control domains complement each other to complete the security posture.

Although NIST CSF isn't the only way we could categorize controls, it provides value in understanding and promoting a holistic security posture:

- **Identify (ID):** Know what you have and what you need to protect.
- **Protect (PR):** Endeavor to prevent harm to your IT assets or security objectives.
- **Detect (DE):** When protection fails – and it will eventually – at least detect the problem.

- **Respond (RS):** Upon detecting an attack, incident, or serious vulnerability, act to stop or contain it.
- **Recover (RC):** Once the breach has been closed, fix the damage.

All five types of controls are required for a balanced security posture in today's target-rich digital environment. Even if an organization does a great job in the Identify and Protect areas, threats will sometimes prevail. Attacks or incidents must be detected and mitigated quickly, and the damage repaired, if only to report a near miss to the regulators, save the business from fines, and preserve its good reputation.

Although some control domains may be more important than others depending on the type of business, basic security hygiene usually requires at least some effort into each of them. Later sections on how to risk-inform and how to scale the control baseline provide guidance on when Level 3 "Defined" maturity would be too much or not enough.

Select the NIST CSF controls cited by the references in the following tables that are applicable for your IT environment and risk profile. Each table contains my description of the control domain and its Level 3 maturity criteria, business functions or roles it depends on for deployment, and the NIST CSF controls related to the control domain. Readers can also use the NIST CSF's mappings from CSF's own relatively high-level controls to the more granular NIST 800-53, COBIT, and ISO 27001 controls when more specific direction is required.

6.3.2 Identify All Aspects of Situational Awareness

More than one of security leaders I interviewed for the book described asset discovery and inventory as the most critical control that's often overlooked. But "identify" should be seen in a much broader context; we need to identify accountabilities, strategic risks, and more.

"If you know the enemy and know yourself you need not fear the result of a hundred battles."

Sun Tzu, *The Art of War*

Security Governance Control Domain

Definition: Governs security roles, responsibilities, decisions, and strategies through a set of processes and capabilities operated jointly by business and security leaders

Description: Puts a CISO or other top security leaders in place. Defines the lines of authority, accountability, and responsibility for cybersecurity. Aligns cybersecurity risk, security policy, and resource allocation with business strategies. Reports security and risk status and progress to executives and stakeholders in business terms.

Business dependencies: Executive stakeholders, LOB, and IT management.

References: Chapters 2, 3
NIST CSF references:
ID.GV: All four controls

Risk Management Control Domain

Definition: Creates a taxonomy and process to identify, assess, treat, monitor, and communicate risk.

Description: Discovers and communicates business leaders' risk appetite and desired risk treatment strategies, that is, accept, avoid, mitigate, or transfer different kinds of risks. Puts a standard control framework in place and determines control selection and prioritization. Maintains and communicates risk register to management. Aligns with regulatory requirements, compliance, and audit functions.

Business dependencies: Enterprise risk management, executive stakeholders, LOB executives, and compliance teams for basic program. Potentially any other business stakeholders depending upon the content of specific risk assessments.

References: Chapter 5
NIST CSF references:
ID.BE: Business environment
ID.RA: Risk assessment
ID.RM: Risk management
ID.SC: Supply chain risk

Security Policies and Awareness Control Domain

Definition: Documents security requirements for people and systems in the business and publicizes them through user awareness training.

Description: Establishes a lifecycle management process for high-level policy and subordinate standard, guideline, and procedure document hierarchies. Seeks to promote secure behavior and a healthy security culture. Covers security governance, risk management, acceptable use of IT and information assets, data classification, access management, incident response, and other policies. Puts an awareness and training program in place. Refer to Chapter 3 for guidance on policy management and Chapter 4 for advancing awareness and the supporting security culture.

Business dependencies: Executive stakeholders, LOB, IT, development leadership, and project management office (PMO) as well as awareness team and/or internal marketing team.

References: Chapters 3, 4
NIST CSF references:
ID.GV-1: Organizational policy
PR.AT: All five controls

Asset Inventory Control Domain

Definition: Discovers IT assets, profiles their risks, and identifies all critical assets as well as asset owners.

Description: Maintains asset inventory databases, directory services, and other registries with information on the assets. Using asset risk profiles, identifies the organization's most valuable, critical, or high-risk assets (aka "crown jewels"). Refer to Chapter 7 for consideration of "knowing what you have" as part of rationalizing IT and to Chapter 5 for more information on asset risk profiling.

Business dependencies: Asset inventory functions are generally led by IT, development, and LOB managers.

References: Chapters 5, 7
NIST CSF:
ID.AM: All six controls
ID.RA-1: Identify asset vulnerabilities
PR.DS-3: Assets managed

A STORY OF UNIDENTIFIED ASSET RISK

"When I was the CISO of a global corporation, we had a comprehensive global outsourcing contract. Worryingly, when asked, they couldn't tell us how many devices we had on the network. I need visibility! The outsourcer eventually estimated we had 88,000 devices, but I knew that was too low because my rule of thumb was 1.5 devices per person. When we implemented Qualys [asset discovery and vulnerability scanning] it found 138,000 devices. That in turn gave us the visibility to understand which devices the outsourcer should manage and hold their feet to the fire requiring: 'Fix all critical vulnerabilities on a device in a timely manner.'"

Paul Simmonds, CISO

Third-Party Management Control Domain

Definition: Manages vendors, suppliers, and other third parties, profiles their risks, and manages shared responsibilities for security.

Description: Provides security input on business decisions to use new third parties or make major changes to existing use cases. Sets standards for security controls or conduct by third parties. Conducts audits of third parties in the highest risk tiers.

Business dependencies: Third-party management generally led by procurement or vendor management. IT management, LOB leadership, and other stakeholders initiate third-party relationships.

References: Chapter 5
NIST CSF references:
ID.SC: Supply chain risk

6.3.3 Protect Information Systems and Assets

Businesses should apply a defense-in-depth strategy using network boundaries, hardening and securely configuring systems, managing digital identity and logical access control, encrypting or obfuscating data in transit or storage to prevent unauthorized access, and providing physical security and personnel controls. Some of these controls can be implemented using commercial off-the-shelf (COTS) products, cloud-based or cloud-native security services, or even open source tools. When the organization develops its own applications, it also needs to ensure the software is written securely.

Network Security and Zoning Control Domain

Definition: Arranges IT assets in logical compartments or physical network segments (i.e., "zones") and provides perimeter protections to the zones. Uses network firewalls, microsegmentation in data centers, virtual LANs (VLANs), and other solutions to enforce communications policies. Controls remote access to protected or restricted via virtual private networks (VPNs), jump hosts, or reverse proxies.

Description: Protects network routing and control devices. Separates assets of different levels of criticality, or with different compliance or communications needs, using zones. Provides zone perimeter enforcement using network firewalls, host-based firewalls, virtual machine firewalls, or identity-based access controls to form physical or logical boundaries.

Business dependencies: EA, IT, and development leaders and architects as well as compliance and audit, networking, network management, and endpoint security teams.

References:
NIST CSF references:
PR.AC-3: Remote access
PR.AC-5: Network segregation
PR.AC-7: Device authentication
PR-PT-4: Protect control networks

Security zoning has been a consistently difficult topic since at least the 1990s when private business networks began connecting to the Internet. Hackers began to ply their trade, security teams put up firewalls, and end users and developers found ways to get traffic around or through the firewalls. By the late 1990s and early 2000s, the concept of a "virtual enterprise" doing business with customers, suppliers, partners, and telecommuting employees was in vogue, and security architects began to speak

of deperimeterization. In the early 2020s, COVID-19 dramatically increased the need for telecommuting, remote access, and zero trust architectures[9] that require strong authentication or other security measures for all access, regardless of originating location.

Businesses continue struggling with how much security zoning is necessary and how to implement it. Too little, and the business's IT resources may be overly exposed to cyberattackers. Too much, and the IT architecture may become inflexible and impede business agility.

Authentication and User Account Management Control Domain

Definition: Manages employee, contractor, and other users' accounts; authenticates access to those accounts.

Description: Manages user accounts in directory services and other authentication systems for all employees and third-party contractors or partners and authenticates access to resources by people, machines, or services on the network. Depending on the criticality of the accounts, supports passwords, biometric sign-on, or stronger authentication capabilities such as one-time password (OTP) token generators and contextual authentication services. Protects secret authentication credentials such as passwords from disclosure. For consumer accounts in some jurisdictions, includes core privacy features such as consent management. Uses special techniques, such as password vaulting, for privileged user accounts.

Business dependencies: IT and development managers. Compliance and audit.

References: Chapter 8
NIST CSF references:
PR.AC-1: Manage IDs, credentials
PR.AC-6: Identity proofing
PR.AC-7: User authentication

---

[9]"Zero Trust Networks," Doug Barth, Evan Gilman, O'Reilly Media, Inc., July 2017, accessed at www.oreilly.com/library/view/zero-trust-networks/9781491962183/

Access Management and Authorization Control Domain

Definition: Enables asset owners to ensure that authenticated users can only access resources as prescribed by business policies.

Description: Enforces access control at multiple layers, such as network perimeters, access proxies, systems, databases or repositories, and applications. Controls fine-grained access permissions at the application level using security groups, roles, or attributes. Provides access management processes and workflows to request or review access. Provides access provisioning (and deprovisioning).

Business dependencies: EA, IT managers, development managers, and any other stakeholder relying on shared IAM services or controlling a system affected by shared access control policies. Compliance and audit.

References: Chapter 8
NIST CSF references:
PR.AC-2: Physical access control
PR.AC-3: Remote access
PR.AC-4: Authorization
PR.AC-5: Network access
PR.PT-3: Least functionality

Security Configuration and Change Management Control Domain

Definition: Configures IT systems, network devices, and applications in a secure manner and controls changes to policies, configurations, documents, and code.

Description: Securely configures systems to reduce attack surface by applying least privilege and least functionality principles. Applies vendor or service provider secure configuration baselines. Supports change management to minimize "drift" from the baselines and uses automated tools to check operating system instances, workloads, and deployed application configuration settings against baselines for managed assets.

Business dependencies: IT managers, development managers, and any other stakeholder controlling a system affected by shared security configuration and change control policies. Compliance and audit.

Security Configuration and Change Management Control Domain

References:
NIST CSF
PR.IP-1: Secure baseline configuration
PR.IP-3: Change control

Data Protection

Definition: Classifies and discovers sensitive information and applies core data security and privacy controls such as encryption or data leakage protection (DLP) on data in motion, at rest, and in use.

Description: Encrypts data on the wire using Transport Layer Security (TLS) and similar protocols and encrypts data at rest on mobile devices. Databases and other critical repositories where large amounts of structured or unstructured sensitive data are stored may leverage secure configuration, access control, restrictive security zoning, and database audit and protection tools rather than encryption to avoid degrading functionality. Defines data classification policies and data owners and discovers or keeps an inventory of sensitive data in the IT environment. Chapter 8 discusses data governance which affects data protection as well as access control.

Business dependencies: EA, IT managers, development managers, and any other stakeholder holding confidential or restricted data (especially when using shared data protection services). Compliance and audit.

References: Chapter 8
NIST CSF
ID.AM-5: Resource classification
PR.DS-1: Data-at-rest protected
PR.DS-2: Data in transit protected
PR.DS-4: Adequate capacity
PR.DS-5: Data leak protection

Secure Software Development and Application Security Control Domain

Definition: Follows secure software development lifecycle (SDLC) and/or DevSecOps standards and practices in development projects.

Description: Sets standards, training, practices, and tools enabling developers to create more secure systems and applications. Performs threat modeling and security reviews during the design phase or at intervals during agile development processes. Provides tools for static and dynamic software testing as well as vulnerability assessment to add assurance during the quality control process, at least for critical applications. Provides basic web application firewall (WAF) functionality.

Business dependencies: Chief Technology Officer (CTO) and development leaders

References: Chapter 7 (DevSecOps)
NIST CSF references:
PR.AC-4: Access control (for applications)
PR.AT-1, 2: User awareness, training
PR.DS-7: Separate development from production
PR.IP-2: Implement secure SDLC
PR.IP-12: Vulnerability management plan

Vulnerability Management Control Domain

Definition: Scans IT systems and applications for software, hardware, or configuration vulnerabilities; prioritizes and remediates vulnerabilities.

Description: Provides processes and tools for periodic automated vulnerability scanning and vulnerability remediation through patching or applying compensating controls. Patching processes take software updates from multiple vendors and/or a third-party vulnerability management tool. Prioritizes vulnerability remediation. For critical assets, tests patches before applying them to reduce chance of impact on users or disruption to production systems.

Business dependencies: IT and development leaders, compliance and audit

Vulnerability Management Control Domain

References: Chapter 5 (triage, prioritization)
NIST CSF references:
PR.IP-12: Vulnerability management plan
PR.IP-1: Secure baseline configuration
DE.CM-8: Vulnerability scans
RS.MI-3: Vulnerability mitigation
PR.MA-2: Remote maintenance
PR.PT-3: Least functionality
PR.DS-6: Integrity checking

Physical Security

Definition: Monitors and protects the business's physical facilities to safeguard the users and assets within the facilities as well as the facilities themselves.

Description: Protects business facilities, such as office buildings, data centers, and servers. Provides physical access control systems, such as locks, alarms, and physical identity badge readers. Uses cameras and motion sensors to monitor facilities. Protects against natural threats such as earthquakes, fires, and floods.

Business dependencies: Facilities management (physical security, executive protection, badging), IAM teams.

References:
NIST CSF references:
PR.AC-2: Physical access control
PR.IP-5: Physical security policy compliance
DE.CM-2: Monitoring systems (a detect control)

Secure HR Practice Control Domain

Definition: Performs background checks and ensures that people-related security practices (e.g., awareness training, policy enforcement) comply with laws and good practices.

Description: Maintains and follows HR and/or security policies and procedures for background checks, hiring, contracting, awareness programs, terminations, incident investigations, and disciplinary actions as they relate to security. Provides input on any policy or procedure, such as monitoring staff emails and communications for leakage, or controls on personally owned mobile devices.

Business dependencies: HR, security operations and monitoring, IAM, and international legal teams.

References:
NIST CSF:
PR.IP-11: Cybersecurity included in HR practices

6.3.4 Win the Race to Detect

In recent years, this saying emerged: "There are only two kinds of organizations: Those that have discovered a breach, and those that have been breached and don't know it." Cyberattackers can penetrate a business quickly; the 2019 Crowdstrike Global Threat Report[10] found the progression from initial compromise to acting on the cyberattacker's target often unfolds in minutes or hours. Against that, as we'll describe in Chapter 9, the average time businesses take to detect intrusion may be measured in months.

One slip, and the business could experience a ransomware infestation during which attackers encrypt their data and throw away the key. Or, compromised end user devices and credentials could be used to steal sensitive data. Rapid detection of threats in the IT environment is critical.

[10]"2019 Crowdstrike Global Threat Report: Adversary Tradecraft and the Importance of Speed," Crowdstrike, March 2019, accessed at www.crowdstrike.com/resources/crowdcasts/2019-global-threat-report-crowdcast/

Real-Time Threat Detection Control Domain

Definition: Detects hacking, malware, and abuse against IT systems, generates alerts to security monitoring systems, and triages alerts to enable effective response.

Description: Provides multiple layers of defense to detect and prevent hacking and malware threats to the IT environment. Deploys intrusion detection systems as well as endpoint and server-level malware scanning and removal. Combines technical, procedural, and educational controls against phishing, which is the most common malware delivery method for targeted cyberattacks. Interfaces to incident response capabilities to quarantine, contain, or block any malware found on endpoints. Provides enough skilled staff to configure and tune the products, perform investigations, and orchestrate responses, such as cleaning infected systems or temporarily quarantining compromised network segments. Operates security information and event management (SIEM) capabilities, or makes use of cloud-enabled ones, to correlate security events and apply machine learning (ML) to detect anomalies.

Business dependencies: IT teams, legal.

References: Chapter 9
NIST CSF references:
DE.CM-1, 4, 5, 7: Detect malware, unauthorized mobile code, suspicious network activity
DE.AE-4,5: Understand, process alerts
DE.DP: Detection processes (all controls)
DE.CM-6: Monitor external services

Logging and Log Review Control Domain

Definition: Generates and collects event logs of security-relevant information in keeping with security standards; reviews logs to detect threats or compromises of IT systems.

Description: Operates on endpoints, servers, applications, infrastructure systems, network devices, and security services themselves. Creates processes and acquires tools to monitor and review the log information. Provides skilled technical security staff to analyze logs using basic log management and collection tools to identify indicators of compromise from the mass of normal activity. May begin to operate a SIEM or other advanced tools to supplement real-time threat detection with log-based detection as well as to produce security reports for audit or trend analysis.

Business dependencies: IT and development teams, HR, legal, compliance.

Logging and Log Review Control Domain

References: Chapter 9
NIST CSF
PR.PT-1: Logging and log review
DE.AE-1, 2: Analyze logs to baseline normal activity and attacks
DE.AE-3: Collect and correlate log data from multiple sources

User Account Monitoring Control Domain

Definition: Monitors both standard user accounts and privileged user accounts for unauthorized, unusual, or suspicious activity.

Description: Monitors for common types of unusual user activity, such as multiple failed authentication attempts followed by access from an unexpected location. Complies with legal protections or work rules while performing the necessary monitoring, especially for privileged accounts, by combining technical, procedural, and educational controls.

Business dependencies: IAM, HR, legal, audit, compliance teams.

References: Chapters 7, 8
NIST CSF:
PR.AC 1, 4, 6, 7: Capture user and access management events
PR.PT-1: Audit logs collected per policy
DE.AE-1: Baseline normal account activity
DE.AE-3: Collect and correlate log data
DE.CM-1, 3, 7: Monitor networks, devices, personnel activity

6.3.5 Respond Effectively and Appropriately

Businesses must have the ability to take corrective action in response to detected attacks, vulnerabilities, and incidents. Effective response capabilities are the other side of the "detect" coin; they can often mitigate most of the damage from cyberattacks.

Incident Response Control Domain

Definition: Identifies and investigates all types of incidents, contains threats, eradicates malware or damaged configuration, recovers, and learns from the incidents.

Description: Provides a program to respond to incidents before breaches or other emergencies materialize. Enacts a set of response policies, plans, and processes that define what constitutes an incident, how each type of incident will be handled, and who is responsible for which activities. Provides technical capabilities and procedures to contain, investigate, and escalate incidents to executives and report them to external stakeholders such as customers, partners, regulators, law enforcement, and the general public.

Business dependencies: Executive stakeholders, IT, development and LOB leaders, HR, legal, compliance, vendor management, public relations teams, and any other stakeholders affected by incidents.

References: Chapter 9
NIST CSF
RS.RP-1: Response planning
RS.CO (communication): All controls
RS.AN (analysis): All controls
RS.MI (mitigation): All controls
RS.IM (improvement): All controls

6.3.6 Recover from Outages or Breaches

Businesses must be able to recover from outages to IT systems caused by operational errors, physical failures, or cyberattacks. In addition, serious data breaches or ransomware incidents require long-term recovery efforts to restore reputation, market position, or operational capabilities even after a hacking or malware threat has been contained and eradicated.

Backup and Data Recovery Control Domain

Definition: Backs up data, configuration, and code of IT assets in a secure manner and tests the ability to perform data recovery.

Description: Prepares for the loss of IT systems or data by taking data backups, designating warm or cold standby systems for use in the event of an outage. Tests recovery of user data, configuration, and entire systems. May arrange relationships with outsourced providers of redundant compute, storage, and network resources.

Business dependencies: Business continuity team, IT, development and LOB leaders, vendor management, and any other stakeholders affected by outages or data loss.

References: Chapter 9
NIST CSF:
PR.IP-4: Backups
RC.RP-1: Recovery plan executed

Business Continuity Control Domain

Definition: Identifies critical assets, creates procedures and facilities to recover their functionality within a specified time in the event of outage, and tests recovery.

Description: Provides basic business continuity processes to recover critical assets identified during a Business Impact Assessment (BIA). Prepares for the loss of IT systems or data by taking data backups, designating warm or cold standby systems for use in the event of an outage. Creates contingency plans and performs failover tests or other tests. Manages recovery from regulatory, legal, and reputational damage in the event of a breach of sensitive data. May arrange cyber-insurance and relationships with outsourced providers of redundant compute, storage, and network resources.

Business dependencies: Business continuity team, IT, development and LOB leaders, legal, vendor management, compliance teams, and any other stakeholders affected by outages or breaches.

References: Chapter 9
NIST CSF:
RC.RP-1: Recovery plan executed
RC.MI-1, 2: Recovery plan improvement

6.4 Develop Architectural Models and Plans for Control Implementation

For most organizations, the control baseline is a work in progress. Security leaders rarely have the luxury of starting over. Nor is the work ever done: New types of systems and applications constantly join and leave the IT environment, and many controls must be continuously improved or changed over time.

Establishing the control baseline across all control domains requires people and process as well as technology. Businesses must put governance structures in place to ensure that the controls get implemented correctly and to verify they're operating correctly. They must also address shared responsibility models for controls operated across their own and third-party (e.g., cloud provider) environments.

6.4.1 Maintain Assessments, Target Architectures, and Implementation Road Maps

Businesses must create a road map for implementation and prioritize controls based on risk. Road maps, or implementation plans and schedules, should be guided by a target architecture.

If you don't know where you're going, any road will get you there.

Target architecture(s) can be developed for the entire control baseline, for individual control domains, or for crosscuts of the control domains. The architecture specifies the technical components and interfaces that implement control objectives. It must also identify people's roles (such as users and administrators) in providing controls and the need for any processes or procedures covering the control activities (such as log review).

To produce a target architecture, security leaders should have a current security assessment. The security assessment should provide a control gap assessment aligned to a list of top information risks. Use the risk assessment and applicable regulatory requirements to identify control gaps. Use the control gap assessment to prioritize and inform the target architecture and more detailed design or requirements documents.

Using risk-informed target architecture recommendations, develop a road map for implementation. Periodically update risk and control gap assessments and maintain target architectures and road maps as living documents.

6.4.2 Use a Two or Three Lines of Defense Model for Control Assurance

To ensure controls are effective, security organizations must concern themselves not only with the strength of the controls but also the quality of implementation and rigor of operation. To provide assurance, most financial services and many businesses in other industries use a "three lines of defense" metamodel (combining architecture and governance) to verify and confirm controls as follows:

- **First line (implementation and operations):** IT and development business process or system owners perform most day-to-day implementation and operations work. For example, business staff use on-premise SAP systems or cloud-based Salesforce services with support from IT operations and development.
- **Second line (security administration, monitoring, and assurance):** Security staff can back up IT operations staff to provide assurance by defining, validating, or checking IT's security procedures. Security staff also often operate security tools such as cloud access security brokers (CASBs) and key management services that exist solely for assurance. Security staff perform security monitoring, security design reviews, and penetration testing from the second line as well.
- **Third line (audit):** Audit can provide an independent check on the implementation, operations, and assurance processes in the first and second lines. Often a combination of internal auditors and external auditors operates according to an annual or semiannual schedule. Internal audit should report outside of IT, often directly to a Board of Directors' Audit Committee. External audit reports (such as an

American Institute of Certified Public Accountants (AICPA) Service Organization Control 2 (SOC 2)[11] report or a Payment Card Industry Data Security Standard (PCI DSS)[12] report) are also reported to compliance stakeholders.

6-2

Internal audit or compliance functions should sample security assurance (second line) as well as IT operations (first line) functions for deficiencies in meeting the business security policies. The security organization should assist internal audit in maximizing insight and efficiency in its process and partner with internal audit on executive reporting to help make audit findings actionable for stakeholders.

6.4.3 Apply a Shared Responsibility Model to the Control Baseline

As security leaders or architects select baseline controls, they must eventually bring the discussion down from the abstract control framework level to the individual services provided for different IT environments or use cases. When IT or security environments are operated by third parties, it's helpful to have a shared responsibility framework that defines security requirements and evaluation criteria for different types of third parties, or third-party use cases, to improve control assurance.

Businesses increasingly depend on cloud service providers (CSPs) and other third parties to deliver IT capabilities. For example, if a customer hosts credit card processing on servers in the cloud and requires PCI DSS certification for them, the CSP must also be certified.

In general, there's a common misconception that service providers will take care of customers' security needs by default. After all, CSPs do offer user account management, logging, and other controls. Unfortunately for the customer, however, it can only

[11] "SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy," AICPA, March 2018, accessed at www.aicpastore.com/SOC/reporting-on-controls-at-a-service-organization-re/PRDOVR~PC-0128210/PC-0128210.jsp

[12] "Payment Card Industry (PCI) Data Security Standard version 3.2.1," PCI Standards Security Council, May 2018, accessed at www.pcisecuritystandards.org/document_library

outsource *some* of the responsibility for security to a CSP and little if any of the liability or accountability for breaches.

Security leaders and staff broadly recognize the need for a shared responsibility model (e.g., the Workday SaaS tool provides logging, but the customer must configure the logs, collect them, and review them). But to develop such a model, we can't rely on control frameworks alone. We need to focus on what the business is doing with a third-party provided system (the "use case") and then ask the following questions covering four perspectives on shared responsibility:

1. What controls must the customer operate to secure the use case?
2. What controls (or capabilities) should the third-party provide to the customer?
3. How should the customer evaluate the general security posture of the third party to know whether to trust it?
4. What controls that the third party is solely responsible for should customers most rigorously evaluate?

The shared responsibility arrangements are different depending on the type of third party. Table 6-2 identifies six types of third party use cases, customer dependencies for each one, and critical criteria to evaluate.

Table 6-2. *Types of Third Parties*

Type of Third Party	Inter-dependencies and Evaluation Criteria
Generic vendor, partner, or third party	The following third party evaluation criteria flow down the table, applying to all vendors or third parties. All vendors or third parties should be viable businesses, offer or agree to acceptable contractual terms, and provide a security program with their own controls that are commensurate to the risks of the use case. In general, every third party should provide secure HR services, security policy and awareness, incident response, and other controls for itself.
Commercial off-the-shelf (COTS) product vendor	Businesses deploy software or hardware products and rely on the vendor for secure software (or system) development, vulnerability management support, and training for the product.
Full-time contractor staffing providers	Some onshore or offshore professional services companies provide contractors for staff augmentation, and some engagements last months or years. These staff may be treated similarly to the customers' own employees. As the staffing provider's customer, the organization will be depending on the provider's secure HR practices and user account management to validate staff are employees in good standing at the contractor organization. However, the customer organization must also provide user account management and authentication for the individual contractors' use within the customer's IT environments.
Software-as-a-service (SaaS) provider	SaaS CSPs provide turnkey applications on demand, such as Salesforce or Workday. Customers need the vendor to provide security for the full IT stack, but enable customer control of user account management for the customer's staff, log review, and other application security features.
Platform-as-a-service (PaaS) provider	PaaS CSPs provide an application development and application platform environment on which customers can build, host, and run COTS or custom applications. Customer PaaS requirements are similar to the SaaS ones; however, the customer needs more control over application and data security features in the service.
Infrastructure-as-a-service (IaaS) provider	IaaS CSPs provide a compute virtualization and cloud storage environment on which customers can build, host, and run compute infrastructure and applications. Customers are responsible for all host-level security features in the guest OS.

Requirements and evaluation criteria for third parties also vary with the use cases and characteristics of partners or suppliers. For example, many products or services require vendors to connect into the customer network and troubleshoot problems or perform maintenance. Customers depend on the vendor to provide secure device configuration for vendor's devices and identity and access management for the users. However, customers must provide remote access controls and perform their own real-time threat detection for the access.

Risk should also inform third-party management and the shared responsibility model. For example, a product or service designed to update real-time market prices and margin requirements for a financial services company needs more monitoring and control than a supplier of network cables and printers. Some organizations perform a quick risk assessment of the technology or service use case for a supplier and place it in a higher or lower tier with more or less controls and assurance requirements for it.

Shared responsibility means that some security controls must be operated solely by the third party and are out of the customer's hands. Where risk warrants, customers need a way to verify that the third party has the controls. In some cases, customers send staff or consultants into third-party facilities to do a complete audit of their security posture against NIST, ISO, or other control frameworks. However, many suppliers (such as CSPs) tend to be unwilling to submit to site visits or any security oversight. Fortunately, standard audits such as SOC 2 exist for service providers that can make it unnecessary for customers to audit CSPs themselves. Instead, customers can obtain evidence of the CSP's SOC 2 certification.

Although SOC 2 provides a defensible and pragmatic way to confirm a third party's basic security hygiene, customers should look deeper under the covers when sharing responsibility with a third party for protecting critical business systems. If customers can't perform third-party audits themselves, they should request and sign a nondisclosure agreement (NDA) for the detailed copy of the third party's independent audit report. It may validate some of the third party's security claims and/or provide findings where improvement or compensating controls are required.

For more information on managing third party CSP security, see the Chapter 7 Section "Manage Cloud Risk Through the Third-Party Management Program." Readers can also obtain detailed CSP control frameworks, questionnaires, and other information from the Cloud Security Alliance's Security Trust Assurance and Risk (STAR) program.[13]

[13]"Cloud Security Alliance Security Trust Assurance and Risk (STAR)," Cloud Security Alliance, Accessed At: https://cloudsecurityalliance.org/star/

6.4.4 Tune Controls to Security *and* Business Needs

The following guidance from Malcolm Harkins' *Managing Risk and Information Security*[14] is helpful in evaluating and implementing controls: "For a few years…I thought of information risk and security as a balancing act…But as my responsibilities grew…I realized that a balancing act was the wrong analogy. We could not start from a position of making trade-offs between risks and enablement, or between security and privacy. So I began using a different model…of optimizing what is really a multivariate equation of risk dynamic and business objectives in order to create solutions that are 'tuned to target.'" The variables in Harkins' control tuning model are

- Risk and compliance
- Cost and maintenance
- Productivity and user experience
- Market objectives
- Customer needs

Security leaders can tune controls using the variables in this model. Given a risk scenario, security leaders may have a choice of mitigation strategies and controls to deal with it. Once controls are selected, they can be tuned to the desired deployment style by planning who, what, and how to implement and operate them while considering the variables in the control tuning model.

6-3

Engage business and IT stakeholders who have a security-related role maintaining controls, are the business owners for assets protected by the controls, or whose operations or business objectives could be impacted by the controls. Tune control deployment style to their business needs and risks.

Finally, many controls must be changed or improved over time because neither the use case requirements nor the threats are static. For example, the growth in telecommuting and cloud computing over the years (and in 2020, with COVID-19)

[14] *Managing Risk and Information Security: Protect to Enable*, 2nd Edition, Malcolm Harkins, Apress Open, 2016

necessitated increased use of remote access. Also, more stringent privacy requirements and potential for abuse of facial recognition and other machine learning (ML)–enabled technologies have created the need for new privacy-enhancing controls and changed requirements for deploying existing controls.

In general, the massive volume of security events and the speed with which threats can compromise an IT environment put a premium on fully automated exploit blocking or ML-enabled detection controls that can keep up with the pace of threats at scale in many environments. Over time, security teams must evolve from "manual detect" to "automated protect" styles of control deployment. This will be required to keep up with adversaries while also minimizing "control friction" vis-à-vis the legitimate users of the protected technology and the controls themselves.

6.5 Scale and Align the Control Baseline

Different types of businesses need different controls scaled to the business culture and deployed at appropriate maturity levels. For any business, control implementation must be aligned to the business functions supporting security for the control.

6.5.1 Scale to Business Size, Type, and Industry

For a small business, the implementation of many controls will be less complex than for a large enterprise. There will be fewer business units, groups, roles, duplications of functions, required integrations, more simplified processes, and (in some jurisdictions) reduced regulatory requirements. However, the small business security team has fewer resources to deploy security controls and tends to require easier-to-use or deploy solutions than a larger business.

For example, small and medium-sized organizations under low security pressure could modify the control domains' maturity requirements as follows:

- **Governance:** Combine the security steering committee function with an IT steering committee or even a single executive staff meeting for all administrative decisions.
- **Security policies and awareness:** A single security policy document might suffice. However, detailed technical procedures should still be in separate documents.
- **Access management:** Smaller organizations may not require formal access request, access review, and access revocation processes.

- Only use two lines of defense (omit internal audit)
- Prefer simplified cloud-based solutions for
  - Real-time threat detection
  - Logging and log review
  - User account monitoring
  - Backup and data recovery
  - And other controls

On the other hand, a large decentralized business such as a multinational corporation with multiple subsidiaries requires added maturity in many areas and may even need more than one control baseline due to major divergences between multiple lines of business and regions. See Chapter 3's section "Matrix Models."

Also, medium or large organizations under high or very high security pressure should generally meet the maturity criteria in most or all control domains and in some cases exceed them. As mentioned in the "Address Common Challenges" section, high maturity procedural controls and/or privileged access management tools are a common requirement.

Small, medium, and large organizations with a relatively low level of complexity may be able to deploy controls universally to cover all assets. Organizations with high complexity and low maturity may need to compromise, applying many controls only to critical business assets at first.

Organizations with high levels of complexity *and* security pressure should prioritize efforts to reduce complexity. However, if the organization cannot further reduce complexity, deploying advanced automated assessment and detection solutions may be useful. Emphasize automated configuration and compliance assessment tools, third-party management services, security analytics and machine learning for real-time threat detection, and so on. Have processes that support, motivate, or require LOBs and IT teams to remedy deficiencies detected against the control baseline in their areas.

Other special vertical industry considerations apply. Application program interface (API) security is everything to high technology companies or CSPs with many exposed services. Software vendors and SaaS companies must put a higher emphasis on secure software development practices. Online retail companies with no brick-and-mortar stores could deemphasize physical security. High technology manufacturing companies, utilities, and transportation companies must improve their ability to provide security controls to IT/OT (operational technology) environments.

6.5.2 Align Control Deployment and Business Functions

Security programs, and even a minimum viable control baseline, have many points of alignment with the business. I went through the 20 control domains in the previous section and cross-referenced all the core business interdependencies to create Table 6-3. The table maps the business functions (other than those in the core security organization itself) to each control domain. Security leaders can use this information to identify which business functions they should engage with in the process of specifying control baseline requirements for each control domain.

Security leaders shouldn't be daunted by the size of the table; they will not need to implement all the controls and manage all the alignments at once. What is necessary is knowing which business leaders hold the leading roles for which business functions, to get to know those leaders and to include aligning with them in control implementation project plans as these come up for action in the security architecture road map.

6-4

Identify the leaders for the various business functions as well as business or IT owners of critical assets. Assign informal relationship managers to them. For business functions with multiple control domain alignments, establish formal coordination forums or projects as the work content merits.

Table 6-3. *Master Table for Aligning Business Functions to Control Domains*

Business Function	Control Domain Inter-Dependencies
Executive stakeholders	Security governance, risk management, security policy and awareness, incident response
LOB executives, leaders	Security governance, risk management, security policy and awareness, asset inventory, third-party management, incident response, backup and data recovery, and business continuity. Many other control domains also tend to have inter-dependencies on LOBs in organizations with decentralized security governance.
IT leaders or teams	Security governance, security policy and awareness, asset inventory, security zoning, authentication and user account management, access management and authorization, SCCM, data protection, vulnerability management, logging and log review, incident response, backup and data recovery, business continuity
CTO and/or development leaders or teams	Security governance, security policy and awareness, asset inventory, security zoning, authentication and user account management, access management and authorization, SCCM, data protection, SDLC, vulnerability management, logging and log review, incident response, backup and data recovery, business continuity
Business continuity team	Backup and data recovery, business continuity
Compliance and audit	Risk management, security zoning, authentication and user account management, access management, SCCM, data protection, vulnerability management, logging and log review, incident response, business continuity
Endpoint or mobile device management team	Security zoning, real-time threat detection
Enterprise risk management	Risk management
Facilities management	Physical security, business continuity
Human resources	Secure HR practices, user account monitoring, incident response

(*continued*)

Table 6-3. (*continued*)

Business Function	Control Domain Inter-Dependencies
Internal marketing team	Security policy and awareness
IT asset management	Asset inventory
Legal team	Secure HR practices, logging and log review, user account monitoring, incident response, business continuity
Network management team	Security zoning
Procurement and/or vendor management	Third-party management, security zoning, access management and authorization, data protection, incident response, backup and data recovery
Public relations	Incident response
UAT team	Security policy and awareness

6.6 Call to Action

The core recommendation for security leaders from this chapter is to establish the control baseline as follows:

- Select which control frameworks to reference based on your business's industry and compliance requirements.
- Put a minimum viable control baseline in place.
- Select granular controls from the 20 major control domains and the NIST CSF model control categories.
- Prioritize the granular controls based on risk.
- Build two or three lines of defense into the control architecture.
- Work with the business's third-party management organization to apply shared responsibility models or concepts to third-party relationships.
- Tune control deployment style to the business's risk, risk appetite, culture, and functional requirements for the protected assets.

- Seek to achieve a "Defined" maturity level or better in each control domain.
- Align control deployment with the leaders of the business functions involved with the controls as well as with owners of critical assets.
- Scale control deployment to the business's type, size, and compliance requirements.

Action – Make a quick assessment of the organization's control baseline

Ask yourself the following short set of questions and score the answers in the Success Plan Worksheet's[15] Section 3, Table 3. Base your score on whether you would answer most of the questions with a strong "no" (1), a strong "yes" (5), or something in between.

1. Does the business have a "control framework" and/or a "control baseline" document that lists the control objectives for IT and the business?
2. Does the security organization have published guidance mapping the control objectives to the required control activities for different levels of risk or different situations (e.g., data classifications, use of third-party services)?
3. Is the control baseline mapped to requirements documents and solution architectures for critical operational systems in IT and security environments?
4. Is the control baseline updated and followed?
5. Do IT, security, or third-party management groups have a shared responsibility framework to aid in evaluating third-party services?
6. Does an architecture document specify how the controls should be deployed?
7. Does the business have an assurance or an audit function to verify controls are operating?

[15] "Rational Cybersecurity Success Plan Worksheet," Dan Blum, Security Architects LLC, May 2020, accessed at https://security-architect.com/SuccessPlanWorksheet

Action – Define 1–3 improvement objectives for the control baseline

Note improvement objectives in Section 4, Table 7, of the worksheet. The following are guidelines and examples of control baseline improvement objectives:

- Evaluate the current control baseline document(s) to see if they can be used as is or as a draft starting point.

If the business requires a new or rewritten control baseline:

- Create an initial detailed outline for a new control baseline using a spreadsheet or a governance, risk, and compliance (GRC) tool. Populate the draft using information from the 20 security control domains.

If a current and credible security assessment is not available:

- Perform a rapid enterprise risk assessment[16] based on the methodology from Chapter 5, section "Perform Enterprise Risk Assessments to Identity Top Risk Scenarios," using available data to identify at least a rough list of top information risks.
- Perform a control gap assessment against the control baseline and the list of top information risks. Depending on the size of the business, rapid or deep security assessments[17] can be performed within a 30-, 60-, or 90-day period.

Don't limit yourself to these examples. Also consider other improvement objectives that fit the gaps and priorities you've identified for your business.

[16]"Rapid Enterprise Risk Assessment," Dan Blum, Security Architects LLC, January 2020, accessed at: https://security-architect.com/RiskManagementResources

[17]"Security Assessments," Dan Blum, Security Architects LLC, January 2020, accessed at: https://security-architect.com/SecurityAssessmentResources

CHAPTER 7

Simplify and Rationalize IT and Security

What you cannot manage, you cannot secure, and a control baseline can't be fully or efficiently implemented across a chaotic IT environment. Although CISOs, or other security leaders, don't own the IT strategy, they have an interest in making it as simple and well defined as possible.

Too many IT environments are aging and dysfunctional. Cloud computing and modern development practices promise transformation to the powerful, seamless IT systems digital businesses need, but often just disrupt, disappoint, and add to the complexity. Amid these challenges, the security leadership needs to be able to reference an up-to-date, approved IT strategy.

To support their organizations' digital transformation initiatives (aka "digital initiatives"), IT organizations must consolidate, simplify, and modernize the infrastructure hosting core business applications. They must rationalize application portfolios. To catch the cloud computing wave, IT and security must change the way they operate from "IT-as-provider" to "IT-as-broker" by excelling at third-party risk management and hybrid cloud monitoring or management. Cloud-enabling processes such as DevOps can take on characteristics of DevSecOps, and Agile of Disciplined Agile, while still enabling rapid innovation.

First the IT and digital innovation, and then the cybersecurity function, must create a strategy that optimizes business agility, operational efficiency, cost-effectiveness, and risk reduction. Although security leaders can't drive the IT or digital strategy on their own, they can request, encourage, and contribute to its development.

Where good practices are lacking, security leaders can advocate for them and implement those that they can as part of ongoing security projects or changes. Security leaders can showcase good practices such as tiered risk assessments, third-party risk

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8_7

assessments, DevSecOps, and security service catalogs. In many cases, security leaders can leverage their inherently cross-functional role to help promote an effective IT strategy.

This chapter provides guidance on how to

- Address common challenges
- Help develop a strategy to consolidate and simplify IT
- Learn from digital initiatives
- Provide security for a governed multicloud environment
- Upgrade IT operations with DevSecOps and Disciplined Agile

7.1 Address Common Challenges

IT and security organizations often share a common challenge described in Chapter 4's Section "Business Units at Odds with IT and Security." Many organizations' internal IT infrastructures are aging and dysfunctional, losing adoption to cloud-based deployments or digital innovation functions outside the IT chain of command. The drift in larger organizations is toward decentralization as the pace of change in IT accelerates and business units take advantage of cloud services. And yet all too often, digital transformation projects or cloud initiatives end up underdelivering and adding to the complexity of the overall IT environment. The security function gets caught in the middle, charged with protecting a mess not of its own making. Resistance seems futile when security lacks input to the IT or digital strategy or when no strategy is in place.

7.1.1 IT Out of Alignment with Digital Business Initiatives

Is it "IT" or is it "Digital?" Most businesses in 2020 have launched some type of digital transformation project, stood up Digital Innovation Lab(s) at the enterprise or line of business (LOB) level, or even gone so far as to appoint a Chief Digital Officer. This sort of development could be a good thing… or not. Done poorly, competing digital initiatives may cause rival fiefdoms to emerge without uplifting core IT environments.

Shadow IT is an explosion of cloud computing adoption for business use by employees and workgroups with no centralized IT organization involvement. Whereas digital innovation initiatives may be seen as strategic, shadow IT deployments tend to be

more tactical. Between shadow IT and digital initiatives not aligned with IT, it becomes hard to even talk about the IT environment, especially in large organizations. One could ask whether the "IT environment" means *all* the business's IT capabilities regardless of who runs them or just the centrally managed part of IT?

I'll use the term "overall IT environment" inclusively of all IT or digital systems whether they're run by central IT, an LOB, or a CSP. In my experience, even in larger organizations, there's usually one security function nominally responsible for defending or at least overseeing the defense of the whole IT environment. The good news is that, managed correctly, digital initiatives (including shadow IT) can sometimes accelerate the development of digital business capabilities available to all LOBs.

7.1.2 Complexity as the Enemy of Security

Too many IT environments are highly complex, riven into silos, and replete with duplicate capabilities and internal support organizations that become increasingly difficult to sustain. This can happen for the following reasons:

- We (the IT organization) inherit an IT environment that grew organically, not one built and maintained from an architectural blueprint.
- We undertook project after project from a tactical perspective. Projects were underfunded or under-resourced. Project contractors or on-staff developers and engineers failed to provide transfer of knowledge for long-term operations or maintenance. Documentation wasn't created or maintained.
- Our technical debt – or the cost of reworking systems that we still need but find increasingly unfit for purpose – is out of control.
- Different business units, or workgroups, never aligned on a common architecture and portfolio of shared services. They went out on their own to build, buy, or subscribe to YETAs (yet another application(s)) of the same type we already had.

"At the end of a decade or two, IT departments across the business have become curators of IT museums. Old, or suboptimal tools (like a custom financial loan management platform built on Microsoft SharePoint, or many disjointed SAP Enterprise Resource Planning (ERP) modules) have been woven deeply into the business process. They are hard to replace. Dozens of satellite applications, such as customer relationship management (CRM) or business analytics, have been bolted haphazardly on to the tangled mess."

Anonymous Client

Then a new IT opportunity comes along. The "revolutionary" capability or application has an exciting name or buzzword. The business launches a new project driven from a digital innovation team or even from EA. "This is going to change everything, enable the business, reduce costs and risks!" Only it doesn't. Technical debt isn't easy to repay.

Security leaders get caught in the middle, responsible for securing a tangled mess that is not of their making. The more complex an IT system or application is, and the more richly it is integrated into the fabric, the harder it is to secure it. Assurance, or being sure, that something is secure requires threat modeling all the ways it can be attacked and verifying that controls – such as error checking, malware scanning, or configuration hardening – are in place and operating to cover all important attack vectors. Logging services, software updating must be added. A limited budget for assurance and control can run dry amid endless permutations.

The good news is that the security leaders can influence the business toward reducing complexity and following good practices. But security leaders must get themselves positioned correctly in the organization to help drive a coherent IT and security strategy.

7.1.3 New DevOps or Agile Models Fielded Without Security Provisions

Digital businesses, software suppliers, and cloud service providers (CSPs) alike are driven by the market to do more with less and to do it faster. Agile project management can speed release cadences and, in some cases, make service providers more responsive to end customer needs. DevOps models can reduce the number of staff needed to run IT systems as well as streamline the release process.

DevOps is a style of IT operations in which the same team that performs development also performs operations, generally through automated processes. DevOps has become popular due to cloud computing and agile development models in which new capabilities are frequently developed in 2-week sprints, and functionality is released to production continuously. However, DevOps can create security issues if there isn't a separation of duty between development, test, and production operations roles.

"Many organizations are advancing into the DevOps culture but not addressing security in the process. IT and security managers must be prepared to deal with the cultural and technical challenges of defining DevSecOps responsibilities clearly and apportioning them to development and security staff. An additional challenge is that the security environment can be quite dynamic. How can the DevSecOps practices move fast when there's a lot of technical debt?"

David Cross, Senior Vice President, Chief Security Officer at Oracle SaaS Cloud

---

Engaging developers requires a different approach in the (modern) development environment, where agile development models have supplanted the waterfall development models that once ruled the roost. Waterfall software development models[1] – which are heavy on documentation, reviews, and approvals – are favorable for assurance. However, in the digital business environment, most development teams have moved to agile development models[2] that emphasize early delivery, continual adaptation or improvement, and rapid or flexible response to change.

Agile development has become a popular method for creating software, and some businesses even use agile principles or agile project management outside the software development area. However, in some cases agile process has become an excuse for no process at all. It is common to find development teams that don't perform or document up front systems requirements analysis. It can be difficult for security teams to engage development when there is no process to inject security into and no documentation against which to perform security reviews.

[1] "Waterfall Model," Wikipedia, accessed at https://en.wikipedia.org/wiki/Waterfall_model

[2] "Agile Software Development," Wikipedia, accessed at https://en.wikipedia.org/wiki/Agile_software_development

Fortunately, some aspects of both agile and DevOps models can be positive for security, as I'll describe in the section "Upgrade IT Operations with DevSecOps and Disciplined Agile."

7.2 Help Develop a Strategy to Consolidate and Simplify IT

The preceding challenges paint a troubled picture of "macro-complexity" (too many types and instances of systems and applications) and "micro-complexity" (systems integrated in complex or custom ways that aren't well managed or documented). What can CISOs or other security leaders who don't control the IT strategy do? As it turns out – a lot! Start with the following objectives that should be part of any IT strategy:

- Understand how to reduce macro-complexity by consolidating or rationalizing core enterprise applications.
- Understand how to consolidate core infrastructure and security platforms.
- Understand how to simplify micro-complexity by adopting consistent management practices for the IT environment.
- Discern the IT strategy and align the security road map to it.

Take opportunities to position security as a coordinating function, at least informally. Implementing many of these practices is IT's job, but the security function is heavily involved and will live or die based on the outcomes. It pays to understand typical IT strategy objectives and the good practices that can lead to accomplishing the strategy. While doing the security work they have to do within IT anyway, security leaders can align or coordinate with IT, digital, risk, or finance teams already following practices that will support an effective IT strategy.

7-1

Leverage the inherently cross-functional roles security is naturally asked to perform – as policy establisher, access gatekeeper, and security service enabler – to help improve the IT or digital architecture and strategy.

7.2.1 Understand How to Reduce Macro-Complexity by Consolidating or Rationalizing Enterprise Applications

The IT or enterprise architecture (EA) function leads and staffs application rationalization projects, not security. However, security leaders should understand the process and support it in the interests of enabling an IT strategy to help set security priorities, support security objectives, and simplify the IT security environment. So as to be able to talk intelligently on these topics during meetings that shape the IT strategy, let's consider the following brief explanation of application consolidation and rationalization.

Every business has its core operating and administration functions, such as

- Product or service development, manufacturing, or extraction
- Logistics, communications, transportation, or delivery
- Sales and marketing
- Product or service delivery, customer support, accounting, etc.

There may be more than one core application instance, for example, a retail and manufacturing conglomerate has multiple "cash cow" product lines; a national government has multiple departments.

IT organizations can identify core functions of the business and map them to core applications as follows:

- For each line of business, name the core operating functions and list the applications that support them.
- Next, identify the administration functions – such as HR, accounting, facilities, legal – that support each line of business and list the applications that support them.

You don't have to generate a complete list of *all* the applications that enhance or support the core applications; that comes later with the application portfolio exercise. Core applications are just the main applications.

Rearchitect or Rationalize Core Applications

In studying the core functions of the business, one often finds multiple core application vendors used for multiple lines of business, for example, both SAP and Oracle for general administration and Microsoft, IBM, and some open source tools

for product development in the same area. Ideally, there could be one and only one core application suite for each core function. Rationalizing applications is the process of phasing out applications that do the same thing or at least specifying which is the enterprise standard and requiring LOBs to justify using a different solution.

One may also discover an aging core application or perhaps an old version of the vendor's product. Whenever possible, core applications should be based on modern architectures using a recent version of the product or service. IT or development organizations can also refactor core applications by eliminating now-unnecessary modules, replacing ones that are easy to replace, and wrapping others with APIs. Eventually the code in the wrapped modules can be pulled out into microservices or itself replaced. Often, application-specific security modules can also be refactored to use general-purpose security products (i.e., for encryption or identity management functions).

Also, per the following cybersecurity-business alignment key, some specific security-related controls may benefit from competent application portfolio management.

7-2

Coordinate the asset inventory control and asset risk profiling implementation, timing, and data models with those of IT- or EA-led application consolidation and rationalization efforts.

7.2.2 Understand How to Consolidate Core Infrastructure and Security Platforms

IT or EA should develop an IT strategy for consolidating infrastructure platforms as well as enterprise applications. Security controls must be implemented in the infrastructure using a combination of native platform capabilities and multiplatform (or hybrid cloud) integration patterns. Simplifying infrastructure security systems (especially identity and access management (IAM) and logging) yields major benefits to security team workloads and accuracy.

Infrastructure Platform Background

A core infrastructure platform provides the set of hardware or software compute, storage, and network capabilities needed to support one or more business applications. It includes physical or virtual servers and containers, operating systems (OSes), network routers, and storage facilities.

Examples of infrastructure platforms include public cloud infrastructure-as-a-service (IaaS) solutions – such as Amazon Web Services (AWS), Google Cloud Platform, and Microsoft Azure – as well as private cloud, premise-based solutions based on VMware or virtual data center solutions. Vendors such as Cisco, Juniper, and EMC provide the network and storage capabilities for private clouds and in some cases in partnership with public cloud suppliers.

Security in the IT Strategy for Infrastructure Platforms

The IT strategy should seek to minimize the number of infrastructure platforms. Otherwise, the more platforms and the more integration patterns are required, the more complex the control baseline(s) becomes along with all other aspects of IT management and security.

Often, strategists advocate moving infrastructure to public IaaS systems so as to simplify IT. However, although IaaS offloads operations tasks such as data center and server hardware management, it still leaves the customer to manage operating systems, network zoning, performance, availability, backups, and more. Any IaaS that isn't required to support a core business application is fair game for consolidation. When rationalizing or rearchitecting core applications, businesses should consider the infrastructure consolidation too. One option is to source new versions of core applications from a software-as-a-service (SaaS) solution. SaaS completely offloads IaaS requirements from the customer. Most software vendors are shifting their strategic development priority into a cloud offering such as Microsoft Office 365, Oracle Data Cloud, and SAP HANA.

IaaS or private cloud solutions remain the only choice, however, when a business's core applications are either developed in-house or must be heavily customized beyond the limits of vendors' SaaS solution flexibility. Even then, platform-as-a-service (PaaS) or "serverless" deployment options on IaaS may be an option. Typically, an in-house private cloud infrastructure and one or at most two public cloud IaaS infrastructure platforms can satisfy most business infrastructure platform needs.

Each infrastructure platform requires a skilled team to operate and maintain it, and any security controls must be operationalized for it. For example, a compliance regulation or the business's own security policy might require encryption of sensitive data-at-rest in all platforms. Encryption key management could then be implemented using platform-native capabilities (such as Amazon Key Management Services (KMS)) or a third-party capability (such as the Thales/SafeNet virtual key management servers

running in AWS). If the business also used VMware in its private cloud, it would have to implement encryption key management there as well. Potentially, elements of the same third-party encryption key management capability can be used across the hybrid cloud of multiple infrastructure platforms.

7-3

Work with IT infrastructure platform teams to develop a menu of reusable native or hybrid cloud capable security controls. Communicate security recommendations to IT teams and application developers for using the preferred (strategic) controls and/or guidance and decision trees for control selection.

7.2.3 Understand How to Simplify Micro-Complexity by Adopting Consistent Management Practices for the IT Environment

Many core IT systems are highly configurable and complex to deploy – think Windows Active Directory domains with interforest trusts or SAP and Oracle ERP suites each integrated with 20, 50, or even more satellite applications for development, collaboration, or analytics. One such core system isn't even the whole IT environment, but if you draw out all its inputs, outputs, services, and dependencies, it can sometimes look like the proverbial tangled mess.

Fortunately, core systems setup need not be complex and obtuse. Solution engineers can simplify the micro-complexity of the larger core systems through standard architecture patterns for identity, security, network, storage, monitoring, data models, and business continuity. By tackling macro-complexity through consolidation and micro-complexity through good deployment practices, IT can reduce or avoid technical debt.

Since much of the micro-complexity comes *from* security, the security team has a natural mandate and many opportunities to help reduce it. To do so requires close engagement and collaboration with IT.

7.2.4 Discern the IT Strategy and Align the Security Road Map to It

Security leaders have a stake in simplifying and rationalizing IT. Although they can't drive the IT strategy on their own, they can request, encourage, and contribute to its development. Without an IT architecture and strategy in a business of any complexity, there can be just too many moving parts to protect.

Security leaders must look through the lens of risk first. Even if highly sensitive data is mired in a legacy system one hopes to replace, it is still a protection priority. But the IT strategy should be the secondary prioritization lens to help pick investments in controls for strategic and thus future-proofed IT systems.

If an up-to-date, approved IT strategy is available, security leaders can align the security strategy, architecture, and road map cleanly and completely to it. Tying security control solution architectures into the known quantity of an IT strategy and road map does wonders to clarify security priorities from the technical control perspective.

If no strategy is published, try to determine the de facto IT strategy by understanding the assumptions and road maps of IT leaders and major LOBs. Work with IT leaders, EA, digital initiative leaders, and risk management functions to resolve open issues or answered questions on strategic IT or digital targets to secure. The goal is to determine which applications, infrastructure platforms, and integration patterns are core to the business and are considered strategic priorities by the leadership. Align security priorities for capability deployment and improvement to those. Ensure that any gaps in the business's understanding of the IT strategy get reflected as gaps in the security road map as well.

Of course, trying to fill a gap in IT strategy isn't always easy. Security leaders can find themselves in an awkward position. IT leaders may not be ready or interested.

"Most organizations are barreling along in one direction 'driven by culture,' and you won't succeed by standing out in front and telling folks they're going the wrong way. If you want to steer in a new direction you first need to find ways to influence the drivers by identifying shared interests and finding their pain."

Jack Jones, Chairman of FAIR Institute

Work collaboratively on common priorities or pain points. Security teams should always be able to identify opportunities to work with IT on shared priorities because often much of the micro-complexity of IT comes from "kludgy" security bolted on in a haphazard manner. Refactoring security services such as monitoring, patching, and access management to use loosely coupled, API-enabled components can reduce technical debt and set the stage for further modernization.

Collaborate with IT on developing security controls. Every control from cutting-edge new DevSecOps capabilities to traditional patch management affects IT, by its nature, and is a natural meeting ground for IT and security staff to work together. Pick at least two different control groups from different categories in the control baseline (e.g., asset inventory, secure system configuration, or logging and log review) for joint projects with IT. Involve IT staff in the design, follow a repeatable project methodology, and document the results such that the project can showcase security and IT working together.

7.2.5 Take Opportunities to Position Security as a Coordinating Function

It's not uncommon for organizations to have a decentralized IT environment where business units control much of the IT budget and staff. Security can often serve as a coordinating function between IT, LOBs, and corporate administration groups. Working on an informal basis across these groups, security professionals tend to have a useful cross-functional view. It isn't always realistic to formalize a coordinating role for security leaders, but some of them thrive on it.

ENGAGED SECURITY LEADERSHIP STORIES

"I work with a Security Business Liaison Committee run by the CISO to manage the timing and impact of technology and policy changes at the bank. The committee has sub-groups for executives, mid-level managers, and technical coordination. As a security strategist, I add value to IT and the business strategy by helping to solve multi-disciplinary problems that none of the groups could solve by themselves."

Randall Gamby, Vice President, Manager Security Strategy at U.S. Bank

"We have an EDGE team ('Everyone Digs Governance Eventually') for security, compliance, HR, legal, Growth, Finance, and all the business units. Through EDGE, we facilitate solutions to 'sticky yucky' business problems requiring multiple stakeholders to resolve. We've tackled everything from how to ship medical data extracts to partners in a secure and compliant manner, to vendor risk management, to securing merger and acquisition processes. I've spent a lot of time building up my Associate VPs to help me engage the business."

Joey Johnson, CISO, Premise Health (ISE Southeast Executive Award Winner 2017)

7.3 Learn from Digital Initiatives

The security team can be a fast learner that adopts good practices from formal or informal digital initiatives and pockets of innovation in the organization or even externally to it. Security leaders should maintain contact wherever possible with groups outside IT that are responsible for digital initiatives. At a minimum, keeping an open channel provides the opportunity to familiarize such teams with current security service catalog options, decision trees, or other implementation aids used for similar efforts in the past.

Recognize that as a digital business, parts of the IT and the application environment may be in a state of continuous transformation and disruption. Be open to the possibility that the digital team(s) is uncovering new or unique use cases and requirements for which IT and security leaders do not yet have a fit-for-purpose solution. Be prepared to partner with the digital team and learn from it, potentially assisting its efforts and bringing new skills, knowledge, and capabilities back into the security offering and/or strategy.

7.4 Provide Security for a Governed Multicloud Environment

To succeed, the IT and security leadership must make capabilities available to business units in an easy-to-consume, agile manner. Gone are the days when business units would live with lengthy IT schedules for delivering new capabilities or changes; today they can quickly put any one of hundreds of SaaS offerings on a credit card or hire a few

developers to build a custom solution on an IaaS platform such as AWS or Azure. Many businesses have adopted a "cloud-first" IT strategy where IT or LOBs deploying premise-based solutions must justify why this approach is superior to cloud-based options.

With some businesses even opting for a "cloud-only" IT strategy, one might ask is there even a need for an IT department? I think the answer is yes because the business needs IT expertise to deliver on the cloud's promise of lowered cost and increased agility as well as to manage security and risk. However, IT and security groups must prove this point to the business through action.

7.4.1 Identify the Risk of Shadow IT

Shadow IT can lead to unintended and undesirable security risks, compliance concerns, and hidden costs. According to the Oracle and KPMG Cloud Threat Report 2019,[3] 92% of 450 IT and security respondents were concerned about shadow IT; many of the respondents also found that policies against the use of unauthorized services were routinely flouted and had led to unauthorized use of data, introduction of malware, and other issues.

On the other hand, Entrust Datacard's report, "The Upside of Shadow IT: Productivity Meets IT Security,"[4] found that 77% of 1000 respondents believed shadow IT can make businesses more competitive and that efforts to eradicate it through cumbersome approval processes could actually drive business or IT users even farther into the shadows and compound the problem.

Rather than thinking of these as dueling reports, we can see them meeting in the middle on the need for a governed enterprise multicloud offering. Facing a clear and present danger, businesses will often empower security to develop a strategy for controlling shadow IT. When that happens, security leaders should resist the temptation to come down too hard on shadow IT offending LOBs with draconian policies. Instead they can engage the business leaders and help them understand risks and accountabilities.

[3] "Oracle and KPMG Cloud Threat Report 2019," Oracle and KPMG, April 2019, accessed at www.oracle.com/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf

[4] "The Upside of Shadow IT: Productivity Meets IT Security," Entrust Datacard, October 2019, accessed at www.entrustdatacard.com/pages/shadow-it

7-4

Work with forward-thinking IT leaders seeking to establish IT as a broker in the cloud environment.

With the security team's support and a business mandate, IT should be able to resolve the shadow IT conundrum, as also discussed in my article, "Shadow IT: Cultivating the Garden,[5]" and in the following section.

7.4.2 Align with the Evolution from IT-as-Provider to IT-as-Broker

A cloud-only or cloud-first approach is a game changer for the IT department. Now it must operate as a broker of cloud services as well as a provider. Businesses can mitigate the risks of shadow IT by having the IT and security organizations develop a service catalog of shared capabilities – both cloud-sourced and from in-house. IT can also help business units find the best cloud solutions for their needs and help the enterprise by curating all business unit requirements and satisfying them through the fewest possible number of reusable, flexible, and scalable solutions.

The first step is for IT to marshal cloud computing expertise from within its ranks to create one or more Cloud Architect and Cloud Security Architect positions with performance objectives to support LOBs and digital initiatives. Then open a communication flow such that

- IT Cloud Architects and Cloud Security Architects become familiar with cloud developments within the business and provide periodic internal briefings on IT projects, LOB projects, industry technology developments, and the state of the market.
- IT and security communicate the IT strategy, service catalogs, and road maps incorporating shared cloud services to the business.

[5]"Shadow IT: Cultivating the Garden," Dan Blum, November 2019, accessed at https://security-architect.com/shadow-cultivating-garden/

- LOBs engage IT and security from the beginning of capability sourcing decision processes.
- Business, IT, and security staff establish informal working groups (aka centers of excellence) to share knowledge of cloud applications and infrastructure platforms.

The cloud access security broker (CASB) is an example of a security tool that both controls and enables cloud users. By providing single sign-on (SSO) to cloud services, the CASB improves ease of use, user authentication, and user account management assurance. The CASB can also support financial controls by limiting cloud access for sanctioned services to users with centrally authorized accounts. Licenses for unauthorized users could be reclaimed.

Additional cloud-enabling services provided or supported by centralized IT groups could include consulting, implementation, DevSecOps, monitoring, IAM enablement, and more. As we unpack the topic of business-enabling technology services and topics, security comes into increasing focus and with it opportunities to encourage and influence a modern IT strategy and service delivery model.

7.4.3 Manage Cloud Risk Through the Third-Party Management Program

In practice, there is a natural tension between consolidating forces in IT and decentralizing forces in the LOBs and development organizations. How the business manages third-party relationships (or doesn't manage them) can end up becoming a battleground.

7-5

Work with third-party management to develop a portfolio process for managing the risk and utility of third parties.

Developing a tiered risk assessment process (see Chapter 5, section "Implement Tiered Risk Assessment") for third parties is not so difficult for smaller business with security staff ready to do their research. Larger business with multiple LOBs and a need for hundreds of third parties should consider obtaining a third-party risk management tool, such as BitSight, ProcessUnity, or Security Scorecard.

A BROKERAGE'S THIRD-PARTY RISK MANAGEMENT STORY

At a recent conference, BitSight copresented a case study of a third-party management process with one of its financial services brokerage clients.

BitSight is a Vendor Relationship Management (VRM) vendor that provides a security rating service for third-party vendors' and CSPs' security postures. At the conference the brokerage described how it used the technology to develop a successful process.

"Management liked how we required vendors with high risks to have high scores," said the speaker. "We operate similarly to a mortgage lender's loan pre-qualification service. Suppose a business unit brought us proposal to use a vendor with a low score. Using BitSight's database during a 30-minute meeting with the internal customer, we could explain the issues with the vendor and propose some alternatives.

"In general, we don't focus much on the low risk use cases, but we can really help with the medium-risk scenarios. For those, we have made the assessment and implementation into parallel processes. This lets us pick our battles. In high risk scenarios (e.g., ones requiring the vendor host our customers' personal data) we got the LOBs to agree to follow a policy of no implementation until an assessment using questionnaires and site visit is complete. The database tool also helps us determine what areas to dive into.

Bottom line – we've gone from taking 17 weeks to as little as 1 day for pre-qualification and have even been able to reduce the high risk review process to less than 8 weeks."

7.4.4 Collaborate with IT on Operationalizing Shared Security Responsibilities

Security and IT management across the industry are adapting to the "hybrid IT" model. As the business rationalizes core systems, some capabilities move to the cloud. These capabilities need to be deployed and operated using a shared responsibility model with the CSP as well as central IT and/or LOB-level groups. Many IT teams are not as experienced working in the cloud model, and shared responsibility arrangements tend to be addressed as one-offs in an ad hoc manner.

To simplify and rationalize the hybrid IT environment, businesses should systematize a shared responsibility model in technology processes for onboarding new CSPs or new cloud services, change management for existing services, and service

decommissioning. The process can engage appropriate groups from the business (i.e., third-party management for contracts, IT and security for risk assessments, and IT and the CSP for operations protocols). See Chapter 6, section "Apply a Shared Responsibility Model to the Control Baseline" for more information.

7.4.5 Include Security Services in the IT Service Catalog

The concept of a service catalog becomes increasingly compelling with hybrid IT and IT broker/provider operating models. The catalog is a documented set of IT service offerings that provides a unified view of IT capabilities independently of where they're sourced from, how they're operated, and who maintains them. Thus, the service catalog can broker both IT and CSP-provided services to internal customers. All that is required for a capability to be on the catalog is that it follows whatever contracts, service-level agreements (SLA), or cost model standards the catalog defines.

- **Contracts:** Usually internal agreements, but sometimes legal agreements, on how the service will be consumed or provided
- **SLAs:** IT or service provider commitments to uptime, support response time, or other performance metrics in operating the service
- **Cost model:** Chargeback or showback processes that enable the business to assess internal cost structures and how resources are allocated

Most cybersecurity capabilities and activities can be factored into IT service offerings – some to be exposed to the business and others measured only within internal IT processes. A security capability or activity can be

- **Provided as a stand-alone IT service catalog item:** For example, a business could offer both standard and enhanced email hygiene services to business units with different service descriptions and lower or higher SLAs and costs. The standard service could provide email anti-spam and malware scanning as well as anti-phishing awareness training. The enhanced service could add deep email anti-malware sandbox analysis and enhanced services for signed or encrypted email delivery.

- **Packaged into the IT service catalog and exposed to business stakeholders.** For example, a Standard Linux Server could be provided as a virtual machine (VM) on a private VMware cloud or on the AWS IaaS. In either case vulnerability management SLAs could specify how often the VM will be scanned and the patching windows.
- **Embedded into the IT service catalog but not exposed:** Certain capabilities such as user entity behavior analysis (UEBA) or security configuration checking could operate on critical systems without an exposed SLA and/or service description.

Notice how closely IT and cybersecurity services can sometimes be interwoven. To achieve higher maturity, the security function should be providing service catalog information. In doing so, it can either align with an existing IT service catalog process or engage with IT to develop one.

7.5 Upgrade IT Operations with DevSecOps and Disciplined Agile

DevOps benefits may come at the expense of losing separation of duty between staff roles and may even undermine the separation of IT development environments from IT production environments. If a fully automated continuous delivery, continuous deployment (CICD) model is adopted, the requirement for handover, or signoff, may be omitted. Fortunately, development teams (motivated to deliver more functionality on schedule) and operations teams (motivated to only deploy stable solutions that run reliably) tend to work well together for availability objectives. But what about privacy, confidentiality, safety, or integrity concerns?

7.5.1 Use Risk-Informed DevSecOps Practices

Although DevOps poses a challenge for cybersecurity, it's also an opportunity. Some of the DevOps principles – automation, systems thinking, continuous improvement, transparency, and shortened feedback loops – can be positive for assurance.

DevSecOps is the name for the practice of adding assurance into DevOps processes. As shown in Figure 7-1, it affects the timing, impact, and scope of security steps in the DevOps process.

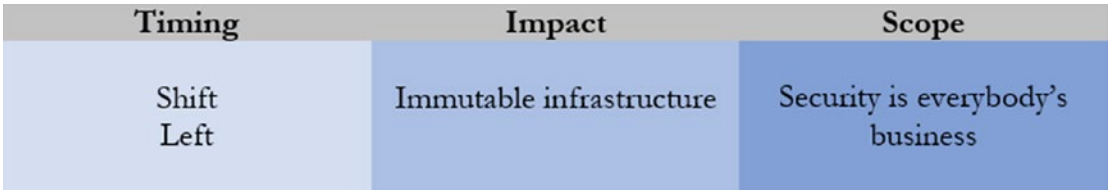

Figure 7-1. *DevSecOps Benefits*

- **Timing:** DevSecOps "shifts left" the security assurance steps in DevOps release process, enabling IT to build security practices in at the beginning of projects rather than bolting it on at the back end.
- **Impact:** Automated deployment, aka "infrastructure as code," eliminates one big vulnerability: the need for system administrators to get remote access into production server farms and applications to reconfigure systems or fix bugs. The "immutable infrastructure" is never reconfigured or patched directly in production. Instead, it is updated periodically from the latest stable development or QA version. Malware has fewer ways to infect immutable infrastructure and would be more easily detected.
- **Scope:** Not only are security steps automated, or semiautomated, into the development and release processes, they're also defined in a simplified manner so that the developers themselves can perform them with appropriate security training and review. DevSecOps can be a force multiplier for the security team.

7-6

Empower developers to easily perform security-related tasks (DevSecOps) as part of their normal workflow and/or cross-fertilize security staff or expertise into the development organization.

To start a DevSecOps initiative, security teams can engage developer communities using a combination of these approaches:

- **Work alongside pilot projects to instrument security steps:** Security staff can be temporarily embedded within key development organizations to build security instrumentation into the release process. The goal should be to configure development pipeline tools to invoke security steps in an automated manner to minimize the developer impact of the extra work on successive releases. Work with developers to capture the learnings on how to analyze reports from security tools (such as static and dynamic code testing) on their systems, simplify the process of fixing problems, and develop training curricula for others based on the pilot project experience.
- **Designate security champions:** Matrix key software architects to the security organization. Identify persons on the developer teams who are willing to take on the opportunity for an expanded role via a security championship program. Provide executive support and other incentives to encourage participation.

TECH COMPANY'S SECURITY CHAMPIONSHIP STORY[6]

"We were able to improve our vulnerability metrics and expand the extended security team from 15 to 40 participants without adding security headcount. We did this using business engagement, collaboratively developed metrics, and a security championship program that followed three principles: Inclusion, Transparency, and Governance.

We engaged security champion volunteers on every major team. With the approval of their VP each security champion dedicated 15% of their time for hands-on security-related work in their area. In return they got recognition and reimbursement for training courses through which they earned paid security certifications.

[6]"Democratizing Security: A Story of Security Decentralization," Harshil Parikh, March 2019, accessed at https://published-prd.lanyonevents.com/published/rsaus19/sessionsFiles/13748/HUM-W03-Democratizing-Security-A-Story-of-Security-Decentralization.pdf

We also worked with business leaders to build consensus on security metrics and ways to improve them. We developed tools to show the measurements to leadership frequently using positive messaging (not a wall of shame).”

Harshil Parikh, Security Leader, Medallia, Inc.

Cover the Full Software Development Life Cycle (SDLC) Process

The scope of DevSecOps may cover anything from lightly customized commercial software and services integrated together in test and production environments to large, custom-coded applications. As we discussed in Chapter 6, software security then becomes a critical part of the control baseline and typically involves DevOps teams adhering to enterprise SDLC standards.

Figure 7-2 details a sample DevSecOps-inspired development and release process diagram. Security steps track each stage of the process and can be highly automated. Training for new staff on the SDLC and its embedded security steps can be delivered just in time or at the beginning of projects. As developers create and unit-test software modules, they perform code scans or static security tests. Once developers integrate code into larger modules, dynamic application security tests attempt exploits against the runtime interfaces.

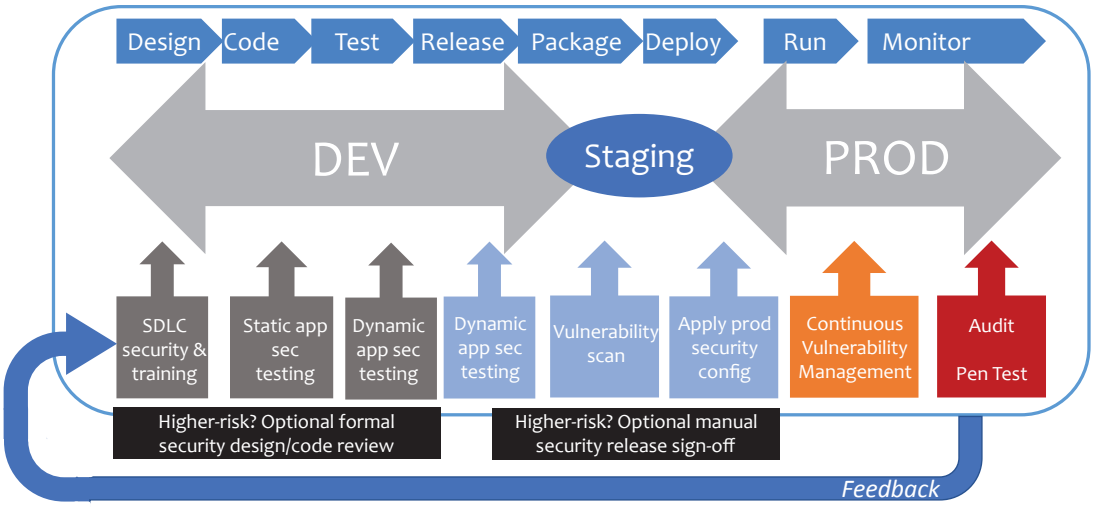

Figure 7-2. *Sample DevSecOps Process Diagram*

As DevOps teams prepare the product for production, they perform vulnerability scans and apply production security configuration. In production, continuous vulnerability scans and patch updates begin, the security team does periodic penetration tests, and security operations or internal audit monitor events or logs.

Security teams can also consider performing formal security design or code reviews for higher-risk projects, as well as requiring manual security release signoff before promoting changes to production. Note, however, that formal reviews are expensive and require specialized security expertise. They are typically reserved for the most sensitive modules (i.e., cryptographic processors, automated teller machine (ATM) user interfaces) in high-risk systems. Another alternative is to provide guidance or training to help senior developers that perform design reviews for integrated systems to look for specific kinds of security issues.

Finally, security and development organizations can collect continuous feedback from the DevSecOps process, including both automated metrics, such as the results of the security tests, and qualitative lessons learned or suggestions to improve the SDLC process. Track such feedback in an issue management system, such as Jira or ServiceNow.

7.5.2 Embrace the Disciplined Agile Approach

In the "Address Common Challenges" section, we noted that, sometimes, the "agile" methodology is used in practice as an excuse for no process at all. Agile's silver lining, however, is the notion that agile development teams, or "squads," should have end-to-end accountability for delivering their minimum viable product. This can and should be construed to include mitigating risk. If one of our goals for Rational Cybersecurity is to "make security everybody's business," what's not to like about a methodology that emphasizes accountability?

Enter the Disciplined Agile Delivery (DAD) model.[7] It adapts agile methodologies, such as Scrum and Kanban, to make them more suitable for larger projects requiring cross-functional coordination or higher-risk projects requiring assurance and oversight.

[7]"Disciplined Agile Delivery," Wikipedia, accessed at https://en.wikipedia.org/wiki/Disciplined_agile_delivery

DAD enables agile teams to continue using their agile methodology of choice while extending it to support coordination and assurance at project inception, construction, and transition stages.

- **DAD inception:** Kicks off the typical series of agile work streams broken up into two-week "sprints" with a "Sprint 0" inception stage. Sprint 0 has just enough up-front planning to solidify the vision for the project or application as well as the scope of the effort, overall data model, and technical architecture. Also, the inception stage can identify the expected risks, testing strategy, and whether the application will be reused by others.
- **DAD construction:** Actual DAD development proceeds similarly to Scrum or Kanban's; however, teams include an architecture owner role and have the remit to coordinate with colleagues in supporting roles for testing, integration, and project-specific specialties.
- **DAD transition:** Adds sprints as necessary for the DAD team(s) to transition a capability into production. The primary DAD team(s) coordinates with infrastructure, security, operations, and support during the release process.

DevOps and DevSecOps teams can adopt key concepts from DAD for projects that exceed agreed risk thresholds. The security organization can also use DAD for its own security engineering efforts and share knowledge, tools, and lessons learned with development organizations so as to influence DAD's inclusion in the SDLC. DAD procedures and supporting roles can be coordinated with DevSecOps. For example, a project inception stage could specify a test plan with requirements for the manual or automated security steps during development and integration with security tools for functions such as encryption or vulnerability management.

7.6 Call to Action

The core recommendations for security leaders from this chapter are to work with IT on simplifying and rationalizing the IT environment as follows:

- Identify and help solve IT and business leaders' security-related pain points in IT systems.
- Leverage the cross-functional roles security is naturally asked to perform – as policy establisher, access gatekeeper, and security service enabler – to help improve the IT architecture and strategy.
- Prioritize security solutions based on an already written or de facto IT strategy.
- Coordinate work on controls such as asset risk profiling (as part of asset inventory) with application consolidation and rationalization efforts.
- Develop security architecture patterns, recommended solutions, and decision trees to apply controls in core infrastructure platforms.
- Support forward-thinking IT leaders seeking to establish IT-as-broker in the cloud environment and/or finance projects working to put technical debt on the balance sheet.
- Work with third-party management to develop a portfolio process for managing the risk and utility of third parties.
- Include security services in the IT service catalog.
- Cross-fertilize security staff or expertise into development and/or operations organizations to establish risk-informed DevSecOps and Disciplined Agile practices.

Action – Make a quick assessment of the state of the organization's IT security strategy and architecture

Ask yourself the following short set of questions and score the answers in the Success Plan Worksheet's[8] Section 3, Table 3. Base the scoring criteria on whether you would answer most of the questions with a strong "no" (1), a strong "yes" (5), or something in between.

1. Does the business have a simplified and rationalized IT environment?
2. Is there a published, up-to-date IT strategy?
3. Has the security strategy aligned to the IT strategy?
4. Is the business use of a hybrid multicloud environment governed well?
5. Does IT publish a service catalog and are security services included in it?
6. Does the security organization work closely with third-party management to assess risk early in the commercial evaluation process?
7. Is the security organization working with DevOps teams to develop DevSecOps processes?

Action – Define 1–3 improvement objectives for simplifying IT and security
Note improvement objectives in Section 4, Table 8, of the worksheet.
The following are examples of IT and security strategy–related improvement objectives:

- Locate document(s) labeled as an "IT Strategy" or serving that purpose. Provide security organization commentary on them and discuss with the IT stakeholders. Align them with the current security project portfolio or road map as appropriate.
- Help the IT organization operate in the "IT-as-broker" mode by collecting information on cloud-based security services options (e.g., vulnerability scanning, multifactor authentication, etc.) already provided.

[8]"Rational Cybersecurity Success Plan Worksheet," Dan Blum, Security Architects LLC, May 2020, accessed at https://security-architect.com/SuccessPlanWorksheet

- Analyze development tool chains in use and discuss potential DevSecOps solutions with development managers.
- Evaluate the opportunity to set up a Security Championship Program(s) in IT. Discuss the idea with senior IT managers that might support it and/or identify staff members in IT that might be good candidates in championship roles.

Don't limit yourself to these examples. Look for improvement objectives that fit the gaps and priorities you've identified for your business.

CHAPTER 8

Control Access with Minimal Drag on the Business

Access control is required for most IT assets, and many of the access rules must be managed by nontechnical business users. The work of managing access controls ("access governance") involves both identity and access management (IAM) and data protection disciplines such as information classification and data governance.

IAM and data governance are vital for reducing breach risk and complying with privacy-related regulations. IAM alone represents three of the control domains from Chapter 6's list of 20 control domains. IAM is technically complex and highly people centric. It requires cross-functional engagement across many business, IT, and development teams. In short, the perfect storm for Rational Cybersecurity!

Most digital businesses literally can't run without digital identity authentication, authorization, and access management capabilities. Paradoxically, the more dependent digital business becomes on digital identity, the more privacy risk it creates for persons, and that feeds back into regulatory and reputation risk for the business. Personal data has been termed "the new oil" – as much as it powers business, it's toxic when spilled. And yet we rely on IAM not only to identify and authenticate users, services, and devices but also to enable digital relationships.

Access control may protect the business, but digital identity enables it. If a business were committed to being agile and flexible at all costs, it would tend to grant high levels

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8_8

of access to all staff members and make it easy for privileged users to change the rules on a dime. If, on the other hand, the business was committed to security and compliance at all costs, it would minimize access grants and create extremely rigorous processes for any rule changes.

This chapter provides guidance for security leaders on how to

- Understand access control and data governance models
- Build up IAM control baseline capabilities
- Balance access control and accountability
- Modernize IAM to enable digital business
- Monitor identity-related events and context
- Build up identity, privilege, and data governance services
- Implement IAM and data governance in a cross-functional manner

8.1 Understand Access Control and Data Governance Models

Access control is about enforcing access policies at runtime in systems based on roles and rules defined through access management processes. Those processes may empower data owners (appointed through data governance) to approve access requests or make changes to rules for accessing the data that they control.

Figure 8-1. *Elements of Access Control*

Access control based on predefined roles and rules can be automated. But all the other elements of Figure 8-1 depend on decisions by people in the organization about data ownership, system ownership, and role ownership.

One can describe the IAM components of access control in terms of the four core services in Figure 8-2.

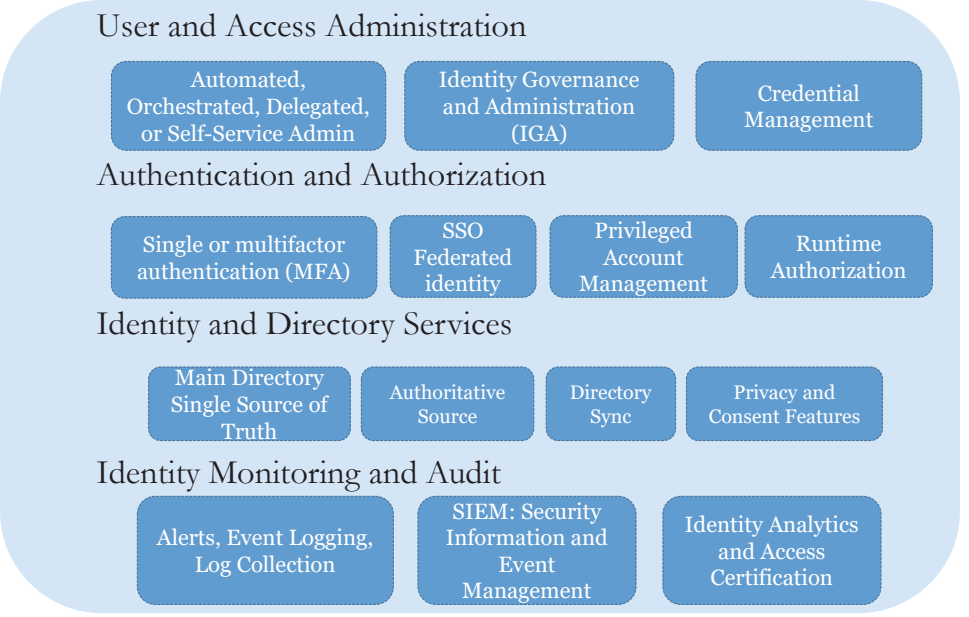

Figure 8-2. *Core IAM Services or Capabilities*

8.2 Address Common Challenges

It's tempting to jump right into the observation that digital identity is both cause and content of many, if not most, security breaches. Let's just lock it down! But that would be to overlook a fundamental point captured here.

"My job as a CISO is actually very easy. Fundamentally, just three things: Provide authorized access to data and services, block unauthorized access to data and services, and prove it."

Andrew Yeomans, CISO

Access control needs to be viewed from a dual perspective of *enabling* and *protecting*. Whatever one does to protect using access controls must be calibrated to risks that could arise from access. Multifactor authentication (MFA) is a great control when it can be combined with single sign-on (SSO) mechanisms, but otherwise the need for users to repeatedly enter longer passwords and one-time codes and take other actions to authenticate for each different site or application introduces friction. Consider the risk context of what is being accessed. Rigorous authentication may make sense for airport security, but to identify users reading free, public content? Not so much.

Perhaps more than any other discipline, IAM must be aligned with the business culture as per section "Address Common Challenges" in Chapter 4. Is the culture flexible and trusting, or are stability and authority more important?

8.2.1 Immature Data Governance and Access Management Processes

Many businesses possess IAM tools such as directory services and identity administration systems and think the tools in themselves will provide a state-of-the-art IAM solution. But unless the business also has mature processes for access management, the tools can be ineffective and the business vulnerable to the risks of inappropriate access. To manage access in a logical and scalable way, identity administration systems need to route access approval requests to data owners or data stewards of sensitive information.

Most businesses have at least rudimentary information classification in that they've defined levels of data sensitivity and identified which types of data belong at which sensitivity level. For example, pricing information may be confidential (available on a need-to-know basis) and customer records restricted (need to know with the highest level of control). However, most businesses tend to suffer from information sprawl and cannot enumerate all the repositories or systems where each type of sensitive data does (or should) reside. Nor can they programmatically identify the data owners for all the many instances or aggregations of sensitive data.

My colleagues and I have done many IAM consulting projects and have put together an IAM resources page for readers.[1] We typically find directories and identity administration systems in place that meet some of the business needs. Every business

[1] "Identity and Access Management Resources," Security Architects LLC, January 2020, accessed at https://security-architect.com/IAMResources

has password-based authentication, but many still lack stronger MFA capabilities, even for critical systems. Generally, the business can identify some of its critical assets and the names of the responsible business owners. However, unofficial copies of sensitive data or other critical assets tend to proliferate and lack clear ownership.

We usually find a deprovisioning capability to remove access for employees leaving the business, but it rarely does a good job of handling contractor or partner access removal. And although it may handle staff terminations, the deprovisioning process rarely cleans up account access rights that aren't required after a user transfers to a new department. The policy data – roles, groups, and rules – that would be required for such precision in access management are rarely rationalized. Cleaning them up would be onerous, requiring the aid of specialized identity governance and administration (IGA) tools.

IGA systems without well-defined processes, access policies, and models tend to operate in an ad hoc manner. Users are overprivileged with too few roles and groups in place or with too many and no one in charge. Access once granted is rarely removed when users transfer assignments or positions. On IAM consulting engagements, it is not uncommon for us to find businesses with more groups than users in the directory.

Finally, despite being included in the SANS Critical Controls lists and in the control baseline recommendation for this book, user account monitoring is often absent.

8.2.2 Outdated IAM Deployments Meet Generational Challenges with Cloud, Privacy Rights, and Forced Digitalization

Most in-place IAM deployments are outdated and don't scale to current volumes of people, data, and things. Poor identity data quality, silos in IT, infrastructure and business changes, and the proliferation of incompatible systems multiply IAM challenges.

Prior to the growing popularity of cloud deployments, many businesses consolidated their in-house directory and authentication services to the Microsoft Active Directory during the early 2000s. Over a decade later, cloud computing began to undo that consolidation, and by now many businesses are back to square one. IAM's gyrations from a mature, consolidated state (on-premises) back to once again straining to support too many directories and user sign-ons (in the cloud) suggest that rationalizing and

simplifying IAM (and IT) is not a one-time fix, but a generational challenge the industry experiences each time new infrastructure platforms, applications, and use cases appear.

Businesses are still adapting IAM to more loosely coupled and decentralized models necessary to support the hybrid multicloud environment. Fortunately, most cloud services consume Security Assertion Markup Language (SAML) assertions as well as other standard IAM protocols. (SAML is an identity federation (aka federated identity) standard that, very simply put, can signal to cloud-based applications "Hey, I've already authenticated my user, log him in!") Federated identity reduces the need to maintain complex, integrated directory services as well as multiple sign-on burdens on users.

There is also a generational shift from the Baby Boomers and Generation X workforce to Millennials. Millennials have grown up immersed in, and more comfortable with, consumer technology. Consumer mobile devices are more intuitive and easier to use than business workstations. Millennial workers and many older ones who caught onto consumer technology expect to use consumer-grade devices at work, to be empowered with enough access to be effective, and to keep growing in their understanding and mastery of the technology. Recognizing this, the concept of people-centric security began to emerge about 5 years ago.[2,3]

PEOPLE-CENTRIC SECURITY

This model of security emphasizes individual accountability and trust. It deemphasizes restrictive, preventative controls. It favors expanding the "trust space" within which staff discretion to operate is encouraged. It assumes the security culture will instill awareness of responsibilities and peer group support for taking responsibility.

At the same time, international privacy and data residency rules are becoming more stringent. Few businesses are fully adapted yet to the notion that in many jurisdictions it is a legal requirement to obtain customers' *informed consent* for using their personal data and to provide other privacy rights. Businesses face increased risks of consequences

[2]"Lessons in How to Implement People-Centric Security," Heather Pemberton Levy, Gartner, Inc., June 2015, accessed at www.gartner.com/smarterwithgartner/lessons-in-how-to-implement-people-centric-security/

[3]*People-Centric Security*, Lance Hayden, McGraw Hill, 2016

from privacy breaches due to regulations such as the European General Data Protection Regulation (GDPR). However, stricter controls on how to access identity information and share it between applications and partners – if implemented – create a drag on the business.

As if all this wasn't enough, the COVID-19 pandemic in 2020 forced many businesses to institute sweeping work from home programs, massively increase remote access to premise-based applications, or move those applications to the cloud. But work from home breaks the trust model for many businesses that have required staff to physically be in a building in order to access sensitive resources. These businesses must now pivot to acquire, deploy, and test logical, identity-based controls such as multi-factor authentication (MFA).

8.2.3 The Red-Headed Stepchild IAM Team

For a critical security control domain, IAM is unusually cross-functional and business enabling. IAM architectures can be highly complex and subject to disruption from IT, regulatory, and business changes. You'd think IAM would fall under the security organization, but I've often seen IAM teams under IT, business units, or other parts of client organizations. It's common to find an IAM working group promoting cross-functional engagement at the grassroots level. Unfortunately, these teams often don't have an executive sponsor engaged with them.

"We're working with baling wire and duct tape here."

Talented IAM team engineer

8.3 Build Up IAM Control Baseline Capabilities

Many breaches either involve unauthorized access to personal information stored directly in IAM directory services or another IAM failure such as weak credentials or inadequate identity proofing before issuing credentials. Unfortunately, it's common to find deficiencies even in the most basic IAM controls.

From Chapter 6, there are several control domains related to IAM, data protection, and privacy. These control domains in turn comprise multiple control activities required to attain a Level 3 (Defined) maturity.

Table 8-1. *Controls for Protecting Access to Data*

Control Domain	Control Activity	Remarks
Asset inventory (prerequisite)	Identify critical assets	List critical assets, such as applications, servers, or databases. Identify their system or data owners.
Security policy and awareness	Information classification	Categorize data (e.g., public, proprietary, confidential, restricted). Identify types of confidential or restricted data such as personal information or trade secrets. Publicize policy and require policy acceptance.
	Compliance training	Make business and IT staff aware of basic privacy and other personal data handling compliance requirements.
Authentication and account control	Account management	Use the business's main directories or user repositories to manage the users' identity lifecycles.
	Authentication	Provide and standardize authentication services. Enable MFA for higher-risk access.
	Centralized single sign-on (SSO)	Provide SSO as a control point for user access to disparate systems while also improving the user experience.
Access control	Manage administration critical systems	Establish and verify access policies (groups or roles) are valid and periodically reviewed for critical systems.
	Deprovisioning	Remove terminated user accounts to revoke access to enterprise infrastructure and critical systems.
User account monitoring	Monitor user accounts and changes	Monitor privileged user and administrator account changes on critical systems for anomalous activities that may indicate account takeover.
Data protection	Encryption, tokenization, other controls	Protect privacy of personal data and credentials in transit, in storage, and in use.

Chapter 6's section "Tune Controls to Security *and* Business Needs" clearly applies to IAM and data governance; both need to be tuned to capture the right balance between the use of restrictive controls and accountability-based controls. They must also be modernized to enable ongoing technology advancement for digital business.

8.4 Balance Access Control and Accountability

Businesses need to strike a balance between risk reduction and productivity or the ability to get work done – between risk and drag, in other words. There is no way to completely eliminate risk even with highly restrictive controls. It is also imprudent to operate a digital business without some drag from controls. Figure 8-3 depicts the notion that between the two extremes of having too many restrictive controls or too few, businesses have a broad area of realistic operating conditions.

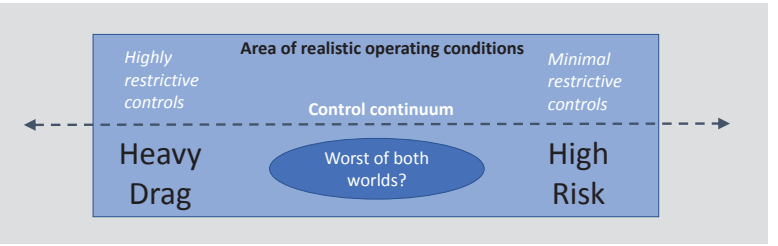

Figure 8-3. *Control Continuum*

One might ask, couldn't we end up still having too much risk *and* too much drag if we took a middling approach? Fortunately, additional tools are at our disposal. We have protect controls (i.e., restrictive) to prevent inappropriate access and detect or response controls for an accountability-based approach. Detect controls create less impact on the user experience and allow users to have more access rights. For example, some banks use a control called "passive authentication" to log users into online banking sessions instead of requiring highly complex passwords or authentication devices. The bank operates sophisticated monitoring tools in the background to detect any suspicious activity.

In the realm of access control, we can choose to "trust but verify" or promote high standards of accountability to control risk without deploying controls that restrict user activity. Staff could be allowed more discretion to make subtle choices, that is, *Should a salesman send an "internal" document to a prospect? What is the classification of that document anyway? Is it OK to let this vendor into the building on Saturday for a meeting*

when the receptionist is gone? Is it OK to edit a confidential company document on my personal tablet device while I'm on vacation? Arguably, security policy could cover any or all of these circumstances, but in the real world of work, there is always more context and circumstances where the answer may be *it depends*. Figure 8-4 depicts a more nuanced view of businesses trading off risk and drag, restrictive access control, and accountability.

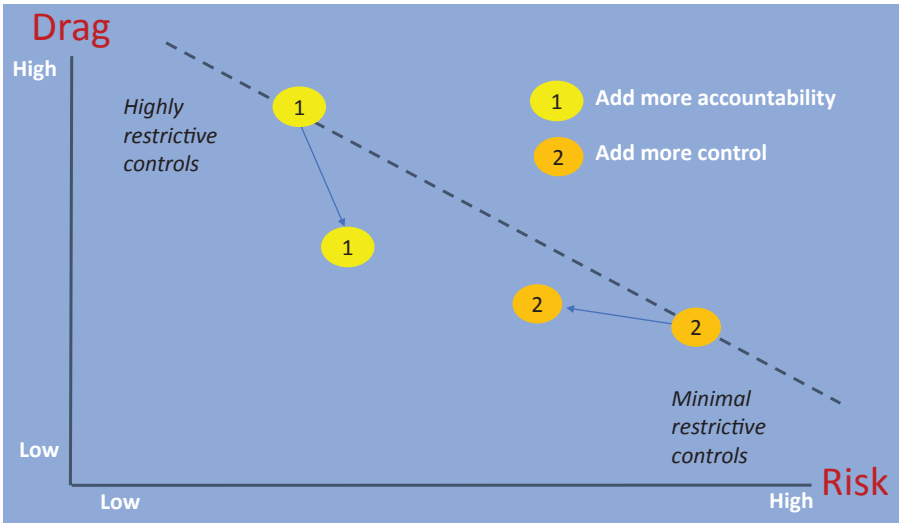

Figure 8-4. *Finding a More Comfortable Middle Ground Between Risk and Drag*

Where to end up on the control continuum is a function of security culture and the nature of inherent risks. Some businesses have a cultural inclination toward more trust, others toward more control. Regulatory guidance tends to emphasize control, often mandating least privilege and separation of duty. But regulatory guidance usually includes a caveat that the approach can be "risk based," thus allowing planners to mix and match "compensating controls." There are also opportunities, such as deploying privacy-enhancing controls, to reduce both risk and drag at the same time.

A restrictive control approach has long been the dominant theme for cybersecurity professionals, and we've tended to default to "protect." However, people-centric security (PCS) poses an alternative theory. At the intersection of IAM and PCS, we must ask how much discretion we can give access managers who grant other users' access. Do we want the access request process to be highly discretionary (and therefore flexible) or highly prescriptive (mostly rules based and potentially inflexible but more difficult to abuse)?

Observe that our second risk/drag figure (Figure 8-4) has a more nuanced notional continuum of controls than the previous (Figure 8-3). One business, such as a bank, might choose a restrictive control set to meet its regulatory requirements and to abate the constant risk of financial fraud. Another business, such as a technology startup, might choose a permissive control set. The control environment, in this example, likely varies due to the companies' difference in assets; perhaps the startup only needs to protect documents, but the bank must protect everything from documents to bank accounts to ATM machines.

The bank could, however, tune or optimize its control set to reinforce accountability for document access through awareness training and deterrent monitoring. This would reduce the need for restrictions on access in some use cases and might improve the user experience without increasing risk very much. On the other hand, a startup should formalize more restrictive access controls (and rely less on trusted staff) as it expands and takes on higher risk customers and regulated use cases.

Access control and data governance require cross-functional business alignment. Security and business stakeholders should work together intentionally to seek that middle ground as shown in the following alignment key.

8-1

Work with stakeholders such as the business's Privacy Office, executives, enterprise architecture (EA), and digital initiative leaders to understand how the business culture should drive design principles for identity governance, data governance, access control, and accountability.

Unlike restrictive controls, accountability-based controls operate within the trust space of empowered users and managers to raise the odds they will do the right thing. Accountability-based controls can use a mix of carrots and sticks.

Carrots include positive messages imparted through user awareness and training – discussed in Chapter 4 – to create the user perception that access is a privilege and help them understand why and how security policies (such as not sharing restricted information) should be followed.

Sticks, on the other hand, can be the awareness that monitoring systems (see the section on "Monitor Identity-Related Events and Context") will detect violations of policy and that policies will be enforced through disciplinary action. Sticks can be communicated through legal contracts, systems and applications' cautionary messages, and user awareness programs.

8.5 Modernize IAM to Enable Digital Business

IAM is also a key control for enabling digital business by managing digital relationships. To do this, IAM teams must often enhance identity interoperability standards support in the business applications and infrastructure. Often, security leaders aren't the drivers for IAM digital business initiatives. But don't be tempted to just stand aside and let an IAM team outside security or some other group handle it without your input. Remember – the IAM capabilities *are* a security priority. Even if security isn't leading an IAM initiative, make sure it has a seat at the table.

8.5.1 Manage Digital Relationships

Identity is not just a set of controls, it is a key part of the way the business manages its relationships with users both on-premise and in the cloud. These relationships are increasingly – in many cases entirely – digital.

Digital relationships that staff, partners, business customers, suppliers, and consumers have with the business are enacted through applications with user interfaces (UIs) and/or via application program interface (API)–based services. All require identity to authenticate, authorize, and personalize the user experience (UX) and functionality or do the same for APIs under the covers.

Digital business can be highly innovative, ranging far ahead of any IT strategy crafted even just a year or two ago. IAM is often "tip of the spear" in developing customer- or partner-facing digital business relationships. To understand the business's forward-looking requirements, security leaders should join with the IAM team to engage with IT and business unit planners and developers on their IAM use cases early and often. These use cases may introduce new capability or scaling requirements such as support for dynamic secrets management in a microservices environment, consumer IOT device authentication support, or new workflow approval processes for partner onboarding.

8-2

Work with the IAM team to engage with business units whose requirements push the envelope of existing standards and technology. Encourage and support innovation for business benefits and overall capability improvement.

The recommendations in Chapter 7's sections "Help Develop a Strategy to Consolidate and Simplify IT" and "Align with the Evolution from IT-as-Provider to IT-as-Broker" suggest another key to business alignment.

8-3

Work with EA and the keepers of the IT strategy to ensure that IAM and data protection controls operate in the strategic IT systems as well as over critical assets; coordinate with third-party management and internal development teams to get the controls implemented in new or changing systems on-premise or in the cloud.

8.5.2 Take a Proactive Approach on Privacy

As critical as managing digital relationships with people is for IAM, it is also an area of great challenge. Both traditional IAM systems and consumer IAM (CIAM) systems sold to businesses expressly to manage consumer identity must increasingly take account of privacy regulations that, in some jurisdictions, give consumers a great deal of choice about whether their data can be stored, how it can be used, who it can be shared with, and how long it can be retained.

This creates marketing technology dilemmas for businesses, which are highly dependent on the ability to ingest a great deal of personally identifying information (PII) and put it through machine learning and business intelligence systems to gather critical data for sales, support, and new product or service development. Businesses may also get a little extra revenue or tit-for-tat advantages by selling or sharing personal data to partners. Traditionally, consumers have received little information about or choice in the sharing or analytics processes. Today such PII-fueled business models are under regulatory pressure.

Marketing technology (martech or adtech) is beyond the scope of this book, so I won't opine on the optimal marketing approaches. But it is within our scope to say that IAM or CIAM will need to have the right capabilities to support privacy protection and that such processes and controls must be aligned with business models' assumptions about how personal information should be used. For example, customer consent for storing or using PII must be obtained through the UI or UX, which could be a shared IAM service or part of an application. Disclosing how customer data will be used in a transparent manner is good for compliance and can also be part of an engaging UI.

8-4

Work with the organization's Privacy Office as well as customer- and partner-facing LOBs and business developers to share new and existing applications' privacy requirements and business models. Work with the IAM team and business developers to learn about privacy-enhancing capabilities.

According to the third "Cisco Cybersecurity Series 2020 Data Privacy Benchmark Study,"[4] increasing numbers of organizations have been achieving positive return on investment from privacy programs. A common path to such gains has been to obtain privacy certifications such as ISO 27701 (a privacy extension for ISO 27001), EU/Swiss-US Privacy Shield, APEC Cross-Border Privacy Rules, and EU Binding Corporate Rules. These certifications can demonstrate compliance with European, Asian, or other privacy frameworks and provide legal cover for cross-border data transfers. For the average company in the study, the ratio of benefits to spend was 2.7, meaning that for every dollar of investment, the company received $2.70 worth of benefit. Companies reported positive results from building customer loyalty or trust, reducing sales delays, mitigating losses from data breaches, and other benefits.

Consider privacy-enhancing technologies such as tokenization, private pairwise identifiers in federated identity connections, and zero-knowledge proofs. Businesses can also monitor decentralized identity, or so-called self-sovereign identity models. A number of startups are developing decentralized identity solutions using blockchains as registries for users' core decentralized identifiers (DIDs) which then link to verified claims[5] (essentially, digitally signed attributes) or zero-knowledge proofs.

8.5.3 Enhance Identity Interoperability and Agility

Guess what, key security initiatives (such as zero trust perimeter security and API security) and key IT initiatives (such as container-based compute services) could all depend on identity interoperability.

[4] "Cisco Cybersecurity Series 2020 Data Privacy Benchmark Study," Cisco, January 2020, accessed at www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/02/2020-data-privacy-cybersecurity-series-jan-20201.pdf

[5] "Verifiable Claims Working Group documents," W3C, 2019, accessed at www.w3.org/2017/vc/WG/

SAML and OpenID Connect for authentication and single sign-on, OAuth 2.0 for authorizing API-based access to resources, and Structured Cross-Domain Identity Management (SCIM) for provisioning accounts or permissions are all federated identity interoperability standards that work across business domains. They can facilitate single sign-on, distributed authorization, API security, and ease of use to speed the process of forming secure digital relationships. Creating consistent IAM services for LOB cloud and Internet use cases enables the business to simultaneously move forward and reduce risk by avoiding ad hoc LOB solutions.

As business's IAM environments encompass more and more externalized, cloud-based systems, it will become increasingly important to also move identity functions to the cloud by leveraging standards-compliant identity-as-a-service (IDaaS) solutions such as Azure Active Directory, Okta, and OneLogin. IDaaS systems extend federated authentication and provisioning to hundreds or thousands of SaaS solutions.

Modern users are also highly mobile, pushing businesses to develop secure strategies for bring your own device (BYOD) access, at least to everyday email, collaboration, and similar tools. Fortunately, many IDaaS solutions provide lightweight mobile device management (MDM), adaptive risk-aware authentication, and highly scalable and extensible directory services. These tools can help protect mobile/cloud users and businesses against brute-force attacks on user passwords, rogue apps, and other threats in the open cloud.

To increase IAM flexibility to operate in a distributed, yet still secure, manner, businesses should set identity interoperability requirements for purchased applications or services and reference the industry standards in third-party assessments. Encourage or require

- UI flexibility, that is, browser-based and mobile support
- API enablement for most IAM services
- Ease of configuration and administrative update via APIs or UIs in a distributed environment
- Careful API design to avoid vendor lock-in and keep the implementation flexible

Also, specify the standards in the business's software development lifecycle (SDLC) standards for developers and provide guidance on leveraging standards implementations from strategic vendor or service provider platforms and related APIs.

8-5

Work with EA, the Chief Technology Officer (CTO), or leading application development teams to incorporate identity interoperability standards into the SDLC.

Finally, businesses must also bring modern IAM fully into their development environments to make both more agile without sacrificing assurance. Enable IAM in microservices and container environments to support DevSecOps initiatives for IaaS or private clouds.

8.6 Monitor Identity-Related Events and Context

Solutions enabled for enterprise use through modern IAM architecture in today's hybrid cloud environment may have a downside. When cloud services are exposed to the Internet for business use, they're also exposed to brute-force password retry attacks, denial of service, and other automated exploits.

Fortunately, MFA can fend off the brute-force attacks, but other attack vectors remain. Just as businesses run on empowered users, IT systems run on privilege, and privilege is a two-edged sword. It enables users to get the work done but can be exploited by rogue users or hackers in the event of account takeover. It is very difficult to protect your systems against attacks by authorized users.

Recall from Chapter 6 that we must use Detect and Respond controls to complement Protect controls. Identity monitoring, auditing, and analytics fit the bill perfectly. Some key capabilities now being offered by vendors include

- **User account monitoring:** It is critical to detect inactive accounts, stale group memberships, and potentially toxic combinations of privileges granted to users (i.e., the same user has the permission to pay invoices *and* to modify the vendor address file). A more advanced use of user account monitoring is to apply peer group analysis of user privileges, or even use machine learning tools to analyze activity and permissions, to help develop business rules for access management.
- **Adaptive authentication:** A smart feature that dynamically adjusts authentication requirements to the risk of the resource

being accessed. Also provides real-time detection of anomalous or suspicious behavior through machine learning at the back end.

- **IAM event logging:** Business IAM teams should work closely with security operations to develop comprehensive logging standards to capture IAM-related events. The logs can also capture context from system and application events in logs and alerts from all protected systems in the IAM environment.
- **Change monitoring:** Unexpected changes to access entitlements (e.g., adding a new user to the all-powerful Active Directory Domain Administrator Group) can be early indicators of compromise, and the business must be on the alert for them. That is another reason why rationalizing and simplifying the IT environment is critical. A simplified IT environment with well-defined procedural controls – such as change management for IT and a formalized request process for privileged access – is easier to monitor. Changes to sensitive objects – such as the Domain Administrator Group – can be immediately detected through automated processes. The software could verify that an IT service management (ITSM) service ticket authorizing the change exists, and if not, roll back the change.
- **Privileged user analytics:** Deeper analysis of what privileged users are doing, even down to the level of actual session monitoring is available from privileged account management (PAM) tools. These tools can issue alerts themselves and also forward the alerts to a security information and event management (SIEM) system which can correlate multiple indicators of compromise.

8.7 Build Up Identity, Privilege, and Data Governance Services

Identity and data governance services must provide an orderly and scalable way to manage access controls. They must manage the user information and access rights behind the scenes to ensure *the right people get access to the right resources at the right times in the right context*. Although identity governance and administration (IGA) tools

are powerful and comprehensive, additional controls are required to manage privileged user access, and these controls are typically provided by PAM tools.

IGA and PAM systems both help support enterprise IT security and regulatory compliance. An IGA system combined with IAM intelligence (monitoring, audit, and analytics) helps give the business a rich set of tools to use for both restrictive access controls and accountability-based controls.

The IGA and the directory services can be used to create and manage identity information and access rules in an orderly manner. It is this information that enables interoperable runtime authentication and authorization capabilities to support the business and the IT strategy, reduce risk, and enable digital relationships. Figure 8-5 captures the admin time, runtime, and policy model faces of IAM.

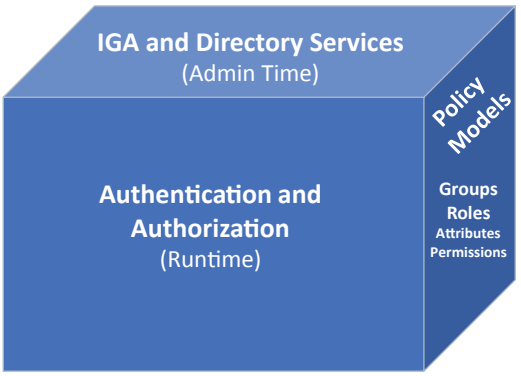

Figure 8-5. *IAM Admin Time, Runtime, and Policy Models*

8.7.1 Understand Identity Governance and Administration (IGA) Requirements

The IGA discipline is the most complicated part of IAM and requires a bit of explanation. IGA has its roots in "provisioning" tools that perform directory synchronization and automated account creation. These tools evolved into IGA suites.

Advanced provisioning tools once differentiated themselves primarily by supporting dozens of connectors for consolidating directory information into centralized systems such as Microsoft Active Directory and synchronizing identity information with other OS or application user account repositories. Today, literally thousands of connectors

are integrated into IDaaS tools to enable single sign-on with numerous SaaS services. Besides provisioning, other important IGA suite capabilities include

- **Identity administration:** Adds, updates, or deletes users, credentials, groups, roles, or other attributes that grant access permissions to resources. Allows users to perform self-service administration of some attributes (e.g., password reset). Enables administrators or application owners to delegate administration rights over security groups that grant privileges to the IT environment.
- **Access administration:** Processes access requests centrally, such as "add user to the operations group" or "give the user access to Salesforce." Typically received via an ITSM (e.g., ServiceNow) ticket or email message, these requests trigger access provisioning for automated fulfillment based on business workflows.
- **Access certification:** Also called access review, this function periodically prompts managers or data owners to validate access rights to IT resources. It is required for certain compliance regimens, such as the Sarbanes-Oxley Act in the United States.
- **Role models and business rules:** Provide the "brains" of the IGA that model how access should be controlled and map access rules from the abstract business role representation to concrete IT permissions such as groups or security settings.

8.7.2 Understand Privileged Account Management (PAM) and Just-in-Time (JIT) PAM Requirements

Powerful administrator accounts – such as the Amazon Web Services (AWS) root user, the Active Directory Domain Administrator, Azure Global Administrator, and Linux server root accounts – are called privileged accounts. PAM tools can be used to manage these accounts and gain additional control over them.

Privilege in IT is required to set up and administer servers, cloud systems, and applications. However, the same IT administrators who create security settings or access controls can easily change them, as could an external cyberattacker compromising the administrators' accounts.

As shown in Figure 8-6, PAM systems manage privileged account registration, credential issuance, revocation, and rotation. PAM systems can also provide runtime capabilities such as credential check-in/checkout, session monitoring, and privileged user analytics. The original PAM vendors such as BeyondTrust, CA, Centrify, and CyberArk centered their implementations around a password, or credentials, vault.

Today, privileged accounts are scattered through the hybrid multicloud environment, and businesses are increasingly using Just-in-Time (JIT) PAM capabilities that require a runtime assignment of a role to a privileged account. Because role assignment is usually an IGA function, PAM and IGA tools are starting to converge with some vendors, such as Saviynt, specializing in IGA-enabled "cloud PAM." Regardless of how it is deployed, PAM is critical to reducing the probability that a bad actor compromising a user account somewhere in the business will be able to move laterally, escalate privilege levels, and cause a breach.

8.7.3 Develop a Hybrid IGA and PAM Architecture

Modern digital businesses (and IAM vendors) have been much quicker to enable digital relationships with innovative use of identity interoperability protocols than they have been to also extend their back office IGA and PAM systems to the cloud. However, as balance of business activity and value shifts heavily into cloud and mobile environments, businesses must develop a hybrid IGA and PAM architecture to cover them as well.

The diagram in Figure 8-6 is adapted from a "to be" IAM architecture we developed for a large North American SaaS vendor's hybrid cloud deployment in 2019 and is representative of what this client and similar companies are deploying as of 2020. Note the following features of the diagram:

- The blue cloud symbolizes a hybrid multicloud environment in which all the systems, data, and IAM services reside. Today, however, most IGA and PAM systems are deployed on premises.
- The primary directory, authentication, and SSO services for this client are in the cloud (as part of an IDaaS) solution.

- The IGA uses a role model and business rules to enact permissions in the directory and in other user identity repositories, such as one attached to the PAM system.
- The PAM system is shown as a separate vendor solution from the IGA system because only a few vendors yet combine IGA and PAM, and that is the way the systems will be deployed for the client in this case study.

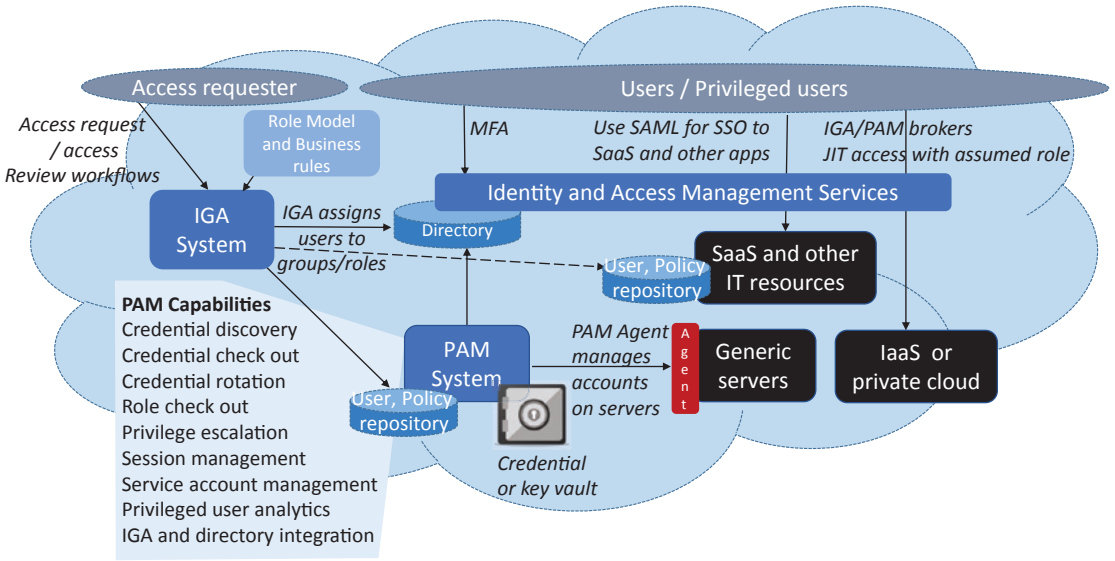

Figure 8-6. *Case Study of IGA, PAM, and Identity Services*

The IGA, PAM, and runtime IAM systems must often support billions of access control scenarios – just imagine how big a matrix showing all the combinations of hundreds of rules, thousands of users, and millions of resources (potentially comprising every field or button on every form of every web application) would need to be. The complete solution must therefore

- Model roles and business rules to drive IGA through policy abstractions that simplify the matrix
- Risk-inform access management functions to enable verification of correct operation at scale

8.7.4 Model Roles and Business Rules to Drive IGA

IGA systems manage access control by defining access policies in the form of roles for users and business rules that refer to roles, groups, or collections of users. These access policies must be managed and aligned at both the business and IT levels of abstraction.

Figure 8-7 illustrates how a business can map job functions (aka business role such as "Accountant") to the IT roles (such as a user account in the finance system which is a member of the system's local "Accountants" group) and then to the actual IT system and application or database permissions required for the work.

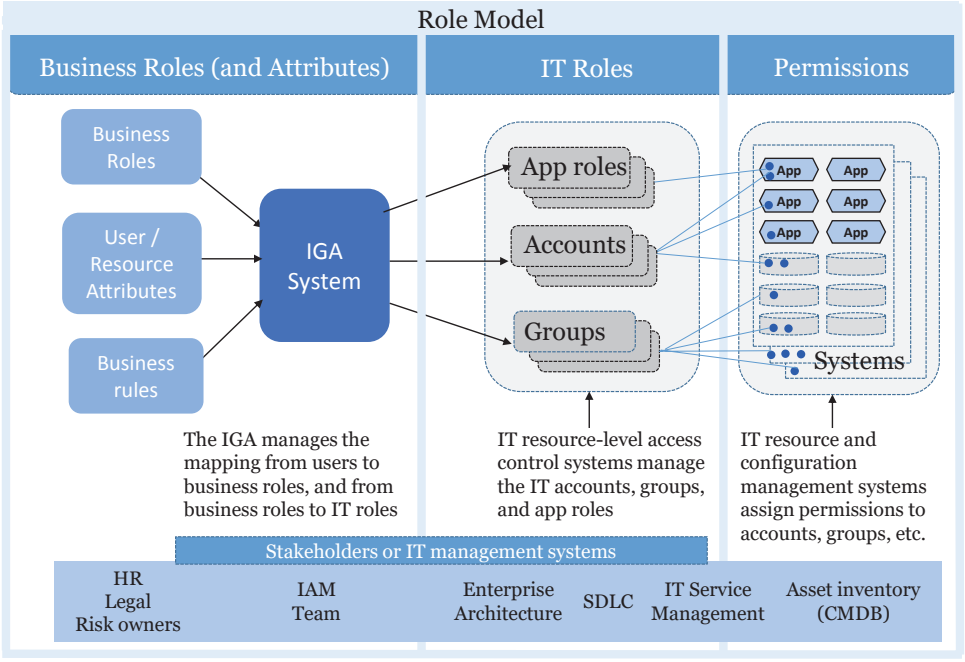

Figure 8-7. *Building a Role Model for IGA*

All users, and other active entities such as machines and services, should have defined digital profiles in the business's directory service(s). Changes to a profile trigger changes to access via the IT roles, such as security group memberships. Access managers or the users themselves can request access changes. Depending on business rules, the IGA system may perform automated provisioning, or it may orchestrate a workflow seeking approval for the change.

When a new user joins the business, the business roles and user attributes in the profile trigger the IGA system to initiate the new accounts, group memberships, and permissions that comprise the "birthright" entitlements for the user. When the user's business roles or attributes change, the IGA system adjusts IT roles and permissions. When the user's entry is removed or suspended, the IGA system removes or disables access.

Finally, the IGA system continuously reviews user access rights against the business rules or signals from IAM monitoring systems, and it may periodically orchestrate access certification campaigns requesting (for example) managers to certify an employee should continue to have certain access rights or that a contractor is still engaged with the business.

8-6

Engage HR, compliance, and appropriate IT or development functions on creating roles for provisioning birthright accounts, managing centralized IT services, and securing applications with compliance-mandated roles.

8.7.5 Risk-Inform Access Management Functions

Businesses and their identity operations teams need to risk-inform the IGA function. Otherwise, the business is likely to have high levels of inappropriate access or experience "drag" from excessive rigor and delays for users requesting necessary access.

Sometimes both risk and drag run rampant across an IT environment that doesn't have a well-defined and well-managed role model or role-specific training for users. During the discovery phase of one IAM assessment, we discovered that IT administrators could easily reset information classified by the business as "Strictly Confidential" to a lower level without data owner involvement. Yet, in the same organization, business users who didn't know the access rules for certain situations held back from sharing information with customers even when they knew it would cost them a deal.

The IGA processes and role models must be appropriate to the business's security culture. Returning to our earlier discussion of people-centric security and accountability, it is probably neither possible nor desirable to completely automate all access assignments. An automated role-based access management system is beneficial

when many identical or similar roles can be assigned, such as to users of manufacturing resource management systems in a large factory environment. In other cases, at least some role assignments or access grants must be orchestrated through workflows. Workflows give managers or resource owners constrained discretion over access decisions. Sometimes it's expedient to allow delegated administration of IT roles; that is, appoint an application owner or a business partner to be the owner of a group that controls who can access to an externally facing application.

Excessive access privileges are often granted when managers rubber-stamp access requests or reviews because they're working under deadlines and perhaps don't understand the applications' access model or the full extent of access granted by a privilege when multiple systems are integrated together. Often the unwelcome chore of access certification (aka access review) gets handed off to compliance; we heard of one case where a compliance officer was tasked to certify 20,000 accounts in just two weeks! But, with the right tools, the compliance officer's mission could be accomplished without gross errors. Here's how: Advanced IGA tools can run analytics or respond to clever queries such as "Which users have been granted access to critical systems in the recent review period? What are all the changes to critical systems' access? Which users are outliers with more access than anyone else on their team?" The compliance officer can then investigate or ask for manager approvals on just those cases.

Implement Advanced Data Governance and IGA When Required

Businesses should fully advance IGA and data governance in cases where their legal and compliance functions already require data governance and/or the business has many types of sensitive data and complex requirements such as avoiding conflict of interest or maintaining information barriers.

Otherwise, using the basic IGA process with simplified data stewardship for the most critical information only should suffice. One common scenario is to implement formal data stewardship for PII in response to GDPR requirements for a Data Protection Officer function. Information classification is another area where most organizations need to improve even just on the basic issues. Data classification levels should reflect the role the data plays in the business rather than a textbook. For example, many organizations still use a category called "Internal Use Only," and that can confuse employees when a business process needs such data to work with "external" partners such as contractors or suppliers. In addition, data handling guidelines must be clearly specified, including for collaboration use cases.

More advanced IGA requirements are most common in financial services, law firms, and specialized niches of other vertical industries. Figure 8-8 depicts IGA processes informed by data governance. Data governance includes formal data classification, data stewardship, and automated sensitive data discovery and reporting. The sensitive data discovery and asset risk profiling processes could identify data stewards for certain assets as the approvers for access request or access provisioning workflows.

Figure 8-8 also shows integration points between IGA and supporting processes. For example, "map permissions to role/group" may be controlled by IT operations. The IAM team and IT operations must coordinate their knowledge of how access policy or entitlements map in the applications. For applications developed in-house, the

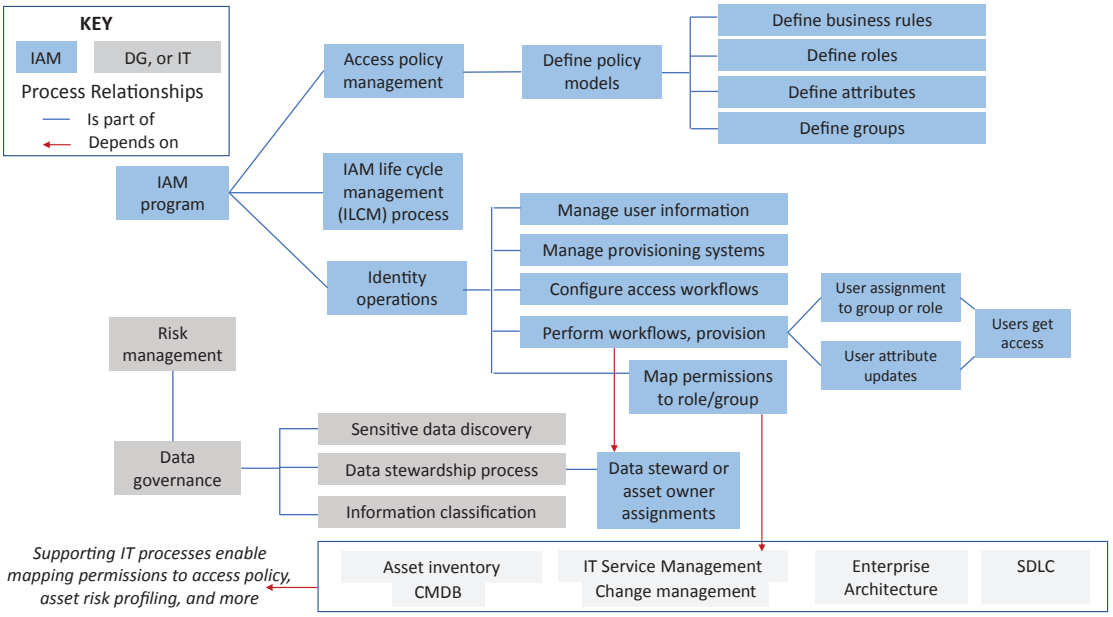

Figure 8-8. *A Risk-Informed IGA Process Map*

business's software development lifecycle (SDLC) standards should specify role model guidelines (e.g., for consistent use of custom applications' administration or approval roles) based on the IAM program's models. EA should be consulted on the architectural principles behind identity services, access policy models, and integration.

8.8 Implement IAM and Data Governance in a Cross-Functional Manner

Because data pervades the business and everyone needs access, IAM and data governance (DG) must be aligned at the technical and business level through appropriate forums.

8-7

Consider creating an IAM working group under the sponsorship of the information security steering committee to enable the IAM team, developers, and other IT or security groups to exchange knowledge and work on processes, role models, or technical standards.

Because IAM is cross-functional and critical to security and the business, I've included a sample Responsible, Accountable, Consulted, Informed (RACI) matrix in Table 8-2. As the IAM and data governance programs mature, the business should formalize more and more of the roles and responsibilities shown.

Table 8-2. *Access Control and Data Governance RACI Matrix*

Management Practice	Board of Directors	Corporate Executives	LOB Executives	Chief Privacy Officer	CIO	CISO	IAM Team Manager	Compliance and Audit	Human Resources (HR)	EA/ ARB	CTO/Dev	IT Operations	Service Manager	Security Incident Response	Business Continuity
Maximize IAM business value			R	C	A	C	C	C		C	I	I	I		
Manage identity operations			I		A	C	R	C			I	R	C	R	I
Manage identity and privacy risk	A	R	R	A	R	C	C	R	C	I	I		C		
Manage advanced access governance			I	A	R	C	R	C	C	I	I	I	I		

Table 8-2 adapts the RACI from Chapter 2's Table 2-2 and suggests role assignments for the following identity, privacy, and data governance management practices:

- **Maximize IAM business value:** The CIO is accountable, the IAM team lead responsible, and the CISO consulted in this matrix. This division of labor varies with different organizations.
- **Manage identity operations:** This practice is devoted to managing all the moving parts of the IAM and IGA infrastructures (see Figures 8-6, 8-7, and 8-8). The CIO is typically accountable for identity operations, as for everything in IT. The IAM team manager has responsibility for operations and monitoring, but IT operations and security incident response may share the responsibility for monitoring.
- **Manage privacy and identity risk:** Accountability for these risks goes up to the top but is shared with the Chief Privacy Officer (or Data Protection Officer position). The CIO has the responsibility. Generic compliance and audit functions also have responsibility and perhaps even accountability for identity-related risks not handed off to a Chief Privacy Officer.
- **Manage advanced access governance:** Where implemented, the Chief Privacy Officer (or another compliance function) should have accountability. Responsibility lies with the CIO and the IAM team management.

8.9 Call to Action

The core recommendation for security leaders from this chapter is to control access as follows.

Security or IAM teams should

- Ensure that IAM and data protection control baseline activities operate in the strategic IT systems as well as critical assets; coordinate with third-party management and internal development teams to get the controls implemented in new or changing systems

- Work with stakeholders on design principles for identity governance, identity interoperability, data governance, access control, and accountability
- Engage with customer- and partner-facing LOBs to learn from their work on identity interoperability or privacy-enhancing technologies and business models to enable digital relationships
- Work with business developers to share new and existing applications' privacy requirements and business models

Large businesses and small or mid-sized businesses with complex environments or high security pressure should also

- Deploy IGA systems to manage role-based access to critical processes and PAM systems to protect critical assets
- Engage HR, compliance, and appropriate IT or development functions on creating roles for provisioning birthright accounts, managing centralized IT services, and securing applications with compliance-mandated roles
- Establish an IAM working group enabling the IAM team, developers, and other IT or security groups to exchange knowledge and work on processes, role models, or technical standards

Action – Make a quick assessment of the organization's access control and data governance capabilities

Ask yourself the following short set of questions and score the answers in the Success Plan Worksheet's[6] Section 3, Table 3. Base your score on whether you would answer most of the questions with a strong "no" (1), a strong "yes" (5), or something in between.

1. Does the business have a cross-functional identity and access management (IAM) team?
2. Does the IAM team report to or coordinate with security?

[6]"Rational Cybersecurity Success Plan Worksheet," Dan Blum, Security Architects LLC, May 2020, accessed at https://security-architect.com/SuccessPlanWorksheet

3. Does the business have coherent access policy models (roles, rules, and groups) in key IT environments?
4. Can IAM systems quickly enable new digital relationships for new applications or business partners?
5. Does the business have someone working on data governance?
6. Does the business have a Chief Privacy Officer or a Data Protection Officer?
7. Are data stewards, or data owners, assigned for sensitive or business-critical information?
8. Does the security department know where all the sensitive data is stored?
9. Are privileged access rights (i.e., root account or domain administrator) restricted to small groups of users?
10. Is privileged access controlled or monitored?

Action – Define 1–3 improvement objectives for the access control and data governance.

Note improvement objectives in Section 4, Table 9, of the worksheet. The following are some sample improvement objectives:

- Conduct a rapid security assessment focused on IAM and data governance[7]; together they constitute a large and critical piece of the security program.
- Identify quick-hitting IAM improvement projects. Use the business impact assessment (BIA) and the enterprise risk map to find critical assets and risk owners; map the IAM and data governance control baseline (Table 8-1) against the assets and connect with one to three stakeholders to learn their IAM and data governance pain points.

[7]"IAM Assessments," Dan Blum, Security Architects LLC, January 2020, accessed at https://security-architect.com/IAMresources

If you are the CISO (or "Head of Security") but the IAM team reports to another organization and isn't closely aligned to security:

- Strengthen the dotted-line reporting relationship of the IAM team to security. To do this, work with the CIO or other higher executive functions over IAM.

Don't limit yourself to these examples. Look for improvement objectives that fit the gaps and priorities you've identified for your business.

CHAPTER 9

Institute Resilience Through Detection, Response, and Recovery

Cyber-resilience provides the ability to withstand and mitigate the impacts of information risks. Businesses can start to become more resilient by identifying their critical assets, top risk scenarios, and basic contingency plans. Then, by aligning technical security capabilities with IT operations and other business functions, security leaders can enable the business to detect suspicious or anomalous events earlier, and respond and recover faster from incidents such as breaches or system outages.

Incident response (IR) is closely linked to security monitoring and detection. It should be managed by a dedicated group (or person) that coordinates closely with security operations, legal, HR, and other functions. Businesses should develop response plans for common types of incidents and for potential incidents from top risk scenarios. Enact response in a structured manner wherein each business function has a script for its part; for example, after a data breach, IT restores affected systems to normal operation, public relations communicates with the media, and the legal team notifies customers or partners of lost personal information.

Businesses can lay the groundwork to enable recovery from serious incidents by performing business impact assessments that identify critical assets and developing business continuity plans to restore or recover the assets. Recovery plans may overlap response plans in the case of cyber-incidents, requiring that business continuity teams and IR teams coordinate. Strictly operational incidents such as hardware failures fall purely in the purview of the business continuity function.

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8_9

This chapter provides guidance for security leaders on how to

- Understand cyber-resilience requirements
- Address common resilience challenges
- Identify critical business assets, risk scenarios, and contingency plans
- Detect cybersecurity events consistently and promptly
- Respond to incidents
- Recover from incidents caused by cyberattacks and operational outages

9.1 Understand Cyber-Resilience Requirements

Businesses can achieve cyber-resilience by implementing smart risk management, robust security monitoring, and well-planned incidence response as well as business continuity/disaster recovery (BC/DR) programs that reduce cybersecurity breach impacts and/or operational impacts from IT outages.

Figure 9-1 illustrates cyber-resilience in terms of the NIST Cybersecurity Framework. “Identify” controls pinpoint critical assets, interdependencies, risks to the assets, and grant authority to defend them. All other cyber-resilience controls depend on this. “Protect” controls reduce probability of successful attacks. However, the probability of *any* attack getting through can rarely be reduced to zero. “Detect” and “Respond” controls can mean the difference between a cyberattack penetrating the IT environment but ultimately falling short of success and that same cyberattack materializing into a major breach. Incident response also sets the stage for recovery and business continuity.

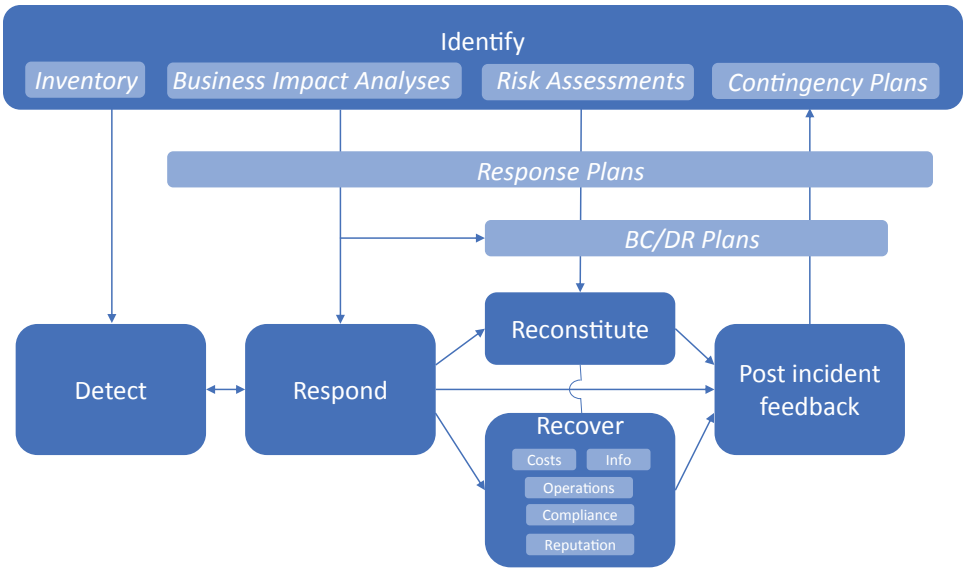

Figure 9-1. *A CSF-Inspired Cyber-Resilience Framework*

The following sections detail ways that Identify, Detect, Respond, and Recover controls can reduce the impact of cyberattacks and operational failures. They also describe good practices for aligning the technical work on controls with business stakeholders.

9.2 Address Common Resilience Challenges

Although Figure 9-1 charts a clear path to resilience, numerous challenges must be overcome. These include

- Business unpreparedness for response
- Lengthy cyberattacker dwell time
- Lack of visibility or access to all IT systems
- Difficulty hiring and retaining skilled incident handlers

9.2.1 Business Unpreparedness for Incident Response and Recovery

Most businesses have immature and/or underfunded incident response and recovery strategies and capabilities. They have not planned for, may not have experienced, and may not have retained staff who are knowledgeable about breaches of personal information, loss of trade secrets, outages, ransomware, or all the other types of incidents that can befall a digital business.

Above-average risk management, business continuity, and response processes are requisites for cyber-resilience. Without them, critical systems and their interdependencies may not be identified, detection is uncertain, recovery time objectives don't reflect business needs, and response or recovery could be ineffective. And yet according to surveys such as the FAIR Institute's "Road to Risk Management Maturity,"[1] the average overall level of risk management maturity was low at 33% in 2018.

Businesses in the 2020s will continue to face an elevated threat environment, with growing levels of automated malware attacks as well as, in some industries, nation-state attacks. Yet due to immature risk management and business continuity processes, they may not have their defensive priorities clearly focused on critical systems.

To monitor complex environments and investigate incidents, larger businesses may require both a security operations center (SOC) team operating 24x7 and a Computer Security Incident Response Team (CSIRT). Maintaining these capabilities at this level requires more than a dozen highly trained staff. Faced with these resource requirements, some try to get by as if they were much smaller organizations with just one person to perform the CSIRT role and SOC services during daylight hours only. What do you think happens when cyberattackers come in the night?

You guessed it – a breach (or its beginnings). Once the breach is discovered, the business lands in a maelstrom of trouble with technical, budgetary, customer, public relations, and human resources concerns colliding. Just when the need for cross-functional collaboration is at its highest, the organization is not prepared. No plans covered this type of incident, not even to specify who to notify or what to do. At best,

[1] "The Road to Cyber Risk Maturity 2018 Risk Management Maturity Benchmark Survey," FAIR Institute, January 2019

the incident becomes a huge distraction. Opportunity costs as well as response costs mount rapidly as executives call meeting after meeting to thrash through the issues and take hurried reactive actions. Inevitably they make some mistakes. If management also succumbs to internal infighting during the response process, the situation gets even worse.

9.2.2 Lengthy Cyberattacker Dwell Time

According to sources such as the "Verizon Data Breach Investigations Report,"[2] the average "dwell time" during which a cyberattacker can maintain a covert presence in an organization's digital systems before detection and eradication typically lasts for months. This can be disastrous because skilled attackers can progress from their initial beachhead to the target objective within minutes or hours,[3] and even lower echelon attackers have ample time to plan and attempt exploits.

Long dwell times offer attackers ample windows to exploit the victim organization's trade secrets, customer information, funds, or other targets. They enable observation and recording of individual or organizational activities to identify additional targets. Attackers have time to implant malware, backdoors, or logic bombs that assure their future access and ability to cause damage. And because criminals and spies can collaborate or share information on targets, other attackers may come in to "join the party" at the victim business's expense.

An organization could end up suffering multiple breaches, find some systems being used for botnet activity, others to mine cryptocurrency, and still more held for ransom. As soon as it fixes one breach, it confronts another. Without drastic measures to burn down and rebuild IT systems, the business could find itself in a state of continuous compromise.

Fortunately, businesses can take action to institute cyber-resilience along with our other priority programs and be leagues ahead of many of their peers and better prepared for many risk scenarios.

[2] "2019 Data Breach Investigations Report," Verizon, May 2019, accessed at https://enterprise.verizon.com/resources/reports/2019/2019-data-breach-investigations-report.pdf

[3] "2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed," Crowdstrike, March 2019, accessed at www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

9.2.3 Lack of Visibility or Access to All IT Systems

As we described in Chapter 7, many businesses have a fragmented IT environment spread across multiple operating units or international subsidiaries. These environments sometimes span complex hybrid cloud topologies over which they have poor visibility. The more fragmented the environment, the more difficult it is to establish centralized or coordinated security monitoring capabilities, log or event collection, and detection, response, or recovery services. Such difficulties arise due to both noninteroperable systems across silos of IT functionality and internal politics.

The larger and the more decentralized the business, the more political challenges complicate or kill security monitoring projects. Although a technical monitoring solution may exist, some units aren't forthcoming with data from workstations, network systems, or security tools such as secure web gateways or secure email gateways.

Technical immaturity in any of the following areas can compound political or IT interoperability issues:

- Incomplete monitoring infrastructure (i.e., lack of log collection or security information and event management systems (SIEM))
- Immature detection processes and alert triage
- Legacy antivirus (AV) solutions not well suited to investigative or forensic work

To remedy this problem, develop the capability to detect cybersecurity events consistently and promptly in critical systems and eventually to all systems in the IT environment.

9.2.4 Difficulty Hiring and Retaining Skilled Staff

According to surveys such as one from the Enterprise Strategy Group and the Information Systems Security Association International (ISSA),[4] over half of North America's organizations report "a problematic shortage of cybersecurity skills."

[4] "The Life and Times of Cybersecurity Professionals 2018," Enterprise Strategy Group and the Information Systems Security Association International (ISSA), April 2019, accessed at www.esg-global.com/esg-issa-research-report-2018

Anecdotal evidence from Rational Cybersecurity project interviews indicates that a shortage of skilled IR staff is a major gap; CIO James Rutt observed, "It's nearly impossible to source qualified IR professionals and retain them for long in the New York City area."

Even businesses that have staffed up find it difficult to satisfy and retain staff in security monitoring or IR roles over the long term. High skill requirements, a demanding work schedule, stressful incidents, and (in some cases) soul-destroying regulatory investigations make managing and retaining workers a constant struggle. Anton Chuvakin, a former Gartner Research VP and Distinguished Analyst who used to field multiple IR program inquiries from clients weekly, commented: "SOC managers tend to be chronically short-staffed and under pressure to fill entry-level positions with people who may be smart and dedicated, but are not yet trained."

Under these circumstances and in a hot cybersecurity job market, it isn't easy to keep one's best analysts happy and retain them in their critical SOC or IR positions. But failing to keep those functions staffed with trained people is a leading factor in security breaches.

9.3 Identify Critical Business Assets, Risk Scenarios, and Contingency Plans

The core processes for detection, response, and recovery depend heavily on identifying the critical assets of the business, their interdependencies, and the risks to those assets. IT and security leaders should conduct rolling business impact assessments (BIA), enterprise risk assessments, and cybersecurity maturity assessments at least every two years to provide a list of top information risks, a current state baseline, and a gap analysis of cyber-resilience capabilities. Contingency plans should be developed for how to perform response and recovery for probable types of incidents and outages.

9.3.1 Perform Business Impact Analysis (BIA)

A BIA is the first step in the business continuity planning process. Use BIAs to

- Identify a prioritized list of critical enterprise resources or services ("critical assets")
- Map critical assets to business processes

- Stipulate any legal and regulatory requirements for the assets
- Itemize interdependencies between the assets and other business systems
- Set goals for critical assets' recovery time objectives (RTOs)

The BIA focuses on identifying the impact to the business if a critical asset becomes unavailable. It specifies maximum acceptable downtime, or loss levels, and sets recovery objectives accordingly.

BIAs should normally be performed at least every two years. Meetings (typically 2–4 hours long) should be conducted by a business continuity (BC) professional[5] or someone trained in that discipline. The BIA lead should facilitate meetings with experts on each asset. The IT and security leadership must ensure that senior business stakeholders support the BIA as an objective, fact-finding exercise and that senior team members who work "hands on" with the services are in the room during meetings.

9.3.2 Analyze Top Risk Scenarios

Whereas the BIA identifies and prioritizes those assets or services most critical to the business, information risk analysis describes the top scenarios wherein threats exploit vulnerabilities to create adverse impacts of different kinds on the tangible IT assets identified in the BIA or on intangible assets such as brand reputation. As we wrote in Chapter 5, risk analysis is an ongoing process within information risk and enterprise risk management (ERM) programs.

A CISO's risk team should perform an enterprise risk assessment at least once every two years. As described in Chapter 5, section "Perform Enterprise Risk Assessments to Identify Top Risk Scenarios," the risk assessments should be aligned with the BIA but also look for top risks in other areas.

[5]BC professionals may be trained in the ISO 22301 standard and/or in industry-specific standards such as the Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook in the United States

9.3.3 Develop Contingency Plans and Cybersecurity Strategy for Resilience

Using the BIA and the risk assessment inputs, the IT and security organizations should prepare contingency plans for coping with outages, breaches, and other material incidents. The contingency planning process should draw information from the following work streams:

- **Cybersecurity maturity assessment:** Determine the organization's level of maturity at risk management, security monitoring or detection, IR, and BC/DR. What level of maturity and capability does the organization have currently, and what level should it target one or two years from now? Where are the gaps?
- **Incident response planning:** These plans (described in the "Respond to Incidents" section) will drive IR procedures for different types of incidents and must be created through an iterative capability building and learning process.
- **Business continuity planning:** These plans (summarized in the "Recover from Incidents Caused by Cyberattacks and Operational Outages" section) will prepare the ability to recover systems that have been damaged in breaches or outages.
- **Cyber-insurance coverage acquisition:** Chapter 5, section "Treat Risks Holistically," suggests cyber-insurance as a means of risk transfer under certain conditions. Based on the business's top risks, business leaders from the finance, legal, IT BC/DR, and security functions can work closely together to obtain the right kind of cyber-insurance policy and conduct operations to preserve the organization's eligibility for coverage. Because some cyber-insurance policies require the business's IR function to coordinate with the insurance company's breach responder, any constraints and opportunities from the actual cyber-insurance policy must be factored into IR contingency plans.

Contingency plans for cyber-resilience should be part of a business's IT and security strategies. IT and security leaders can recommend ways for business risk owners to deal with IT failures or incidents arising from strategic risks. The actual plans can summarize and reference existing and more detailed risk registers, IR plans, and BC/DR plans. If none are yet developed, the contingency plans can develop preliminary assumptions and starting points for them.

Once the business has a maturity assessment covering the cyber-resilience functions, IT and security leaders should work with business executives to set direction on three key cyber-resilience decisions considering the business's maturity level and future needs:

- **Roles and responsibilities:** Who is responsible for security monitoring? Incident response? Recovery of various types of systems? Accountabilities must be identified among executives, business process owners, CIOs, and CISOs and responsibilities or consultations to the CSIRT, SOC, business continuity team, service managers, and others.
- **Security monitoring – organization and staffing:** Does the business need a SOC with 24x7 coverage? A 24x7 SOC requires 8 to 12 highly skilled (and expensive) staff. Alternatively, the organization could stand up a "SOC lite" with fewer persons but reduced hours. It could use managed security services providers (MSSPs) and managed detection and response services (MDRs) that provide round-the-clock services to augment small (even one person) in-house security monitoring teams. However, outsourcing security monitoring requires careful management, and it may reduce the business's ability to cover all locations and to tailor detection to its unique applications, configurations, people, and processes.
- **Computer Security Incident Response Team (CSIRT):** Where does the CSIRT function reside in the organization? In larger businesses, different groups should provide security monitoring and CSIRT functions. However, technical staff and duties overlap. The CSIRT also requires support from nonsecurity stakeholders, such as legal, human resources (HR), marketing, PR, and others.

9-1

Because cyber-resilience requires considering business drivers, top risks, risk appetites, and IT security governance questions get as much input on the strategy as possible from executive management.

"Everyone has a plan until they get punched in the face."

Mike Tyson

9.3.3.1 Plan for Unexpected Incidents

Many incidents fall into known types. Even if some of the details of threats, impacts, and response or recovery strategies have to be discovered or developed on the fly, existing playbooks for the incident type provide a place to start.

Completely new types of incidents could throw the CSIRT, the CISO, and the whole company into a state of chaos or panic. Businesses in some industry sectors, such as the retail clothing, might reasonably expect to never encounter a nation-state attacker (aka advanced persistent threat (APT)). Suppose, now, one of those businesses receives forensic evidence from their national intelligence agency that indicates it has just experienced its first APT attack. What should the business do now, and how could it have prepared?

I hate to say this: Preparing for unexpected incidents requires having a "plan for a plan." This needs to be one of the CSIRT's playbooks and a subject for training exercises. Part of stakeholders' orientation to their role in the CSIRT should state that "If you get a meeting request with a subject line such as 'Urgent: Critical New Incident Planning Meeting,' you attend that meeting." Such meetings could have a simple objective to create a playbook on the spot, at a minimum identifying

- An incident commander and accountable executive(s)
- An incident team
- Internal or external resources to draw on (in our example) to come up to speed on APTs very fast

- Any existing playbooks (from other incident types or provided by vendors or security information groups) to use as template or starting point
- Next steps

9.3.4 Develop Business Continuity and Disaster Recovery Plans

Preparing a business continuity plan helps the business recover quickly if an incident does happen. Although it isn't possible to predict every kind of incident that could threaten the business, one can develop plans that cover a range of incidents (e.g., natural disasters, computer problems, staffing issues, pandemics). A business continuity plan helps to identify and prevent risks where possible, prepare for risks that can't be controlled, and respond and recover if an incident or crisis occurs. The size and complexity of BC/DR plans depend on the size and type of business, but IT and security leaders and service managers should ensure that they include

- Information required to recover from catastrophic failures, to get the business running again
- Procedures for restoring critical systems or applications within defined recovery time objectives
- Periodic testing of recovery processes
- A schedule for updating the plan itself to account for any changes to the business, the industry, or the operating locations

9-2

Ensure that senior business stakeholders support the business continuity program and that the key IT team members who work "hands on" with mission-critical services are in the room during BIA and BC/DR planning meetings.

Some companies routinely purchase extra capacity (e.g., 25% above current demand) to all IT procurements as cyber-resilience requirement. Occasionally such procurement policies pay off. For example, over-provisioning spare notebook computers and remote access solution capacity would have made businesses more resilient

to the COVID-19 pandemic. In general, BCP/DR plans should also be informed by requirements to provide cyber-resilience in the event of infrequent but high impact events such as hurricanes, prolonged power outages, and pandemics. BC/DR team members should be informed of these scenarios by the risk management team and (since they are infrequent) devise ways of increasing resilience – whether by design, procedural contingency plans, or incremental capability – that don't add much to cost but do leave the business better prepared. Rather than overstocking licenses and VPN gateway appliances, for example, a pandemic prepper could arrange and test cloud-based remote access capacity for use during crisis or peak demand periods.

9.4 Detect Cybersecurity Events Consistently and Promptly

Per the NIST CSF, "Detect" controls must backstop "Protect" controls. Businesses must collect logs, generate and receive real-time notifications, and investigate events which could be indicative of security problems. Detecting advanced (or stealthy) threats requires more sophisticated monitoring tools and processes, skilled staff, and enough event context to distinguish normal from malicious activity. Monitoring capabilities must be deployed in all IT domains (i.e., on-premise data centers, end user networks, cloud infrastructure, and applications). Outside the enterprise IT systems' domains, businesses should also monitor user feedback to the company as well as security-related notifications from external parties.

Security monitoring systems process information and analyze it to find indicators of compromise, precursors to attacks, or vulnerabilities. A good monitoring infrastructure will detect many issues, most of which are unimportant, repetitive, or false alarms. Security monitoring can be like looking for needles in the haystack, such as

- Threats, human or automated, attacking or already inside the systems
- Security controls not operating in compliance with policy
- Information assets that are missing or failing to pass security tests or health checks

9.4.1 Monitor Event Logs, Alerts, and Reports

First, we must capture the data! Basic event logging gives visibility of IT and security-related activity, establishes baselines for normal activity, and provides data for an audit trail. Monitoring and logging processes and tools must cover log creation, collection, and management as well as real-time notifications to security consoles, operators, or tools.

Security teams can employ log management and SIEM tools to collect logs and events. The tools can understand and normalize many kinds of log data from different systems (such as security systems like firewalls, endpoint protection systems, and directory services) as well as server, application, and endpoint resources. However, standards are required for custom applications' logging and alerting function and for configuring off-the-shelf systems.

After collecting log data, alerts, and notifications, businesses can run this information through automated analysis, perform human log review on selected issues, and retain certain log records. If we could capture all the events in the enterprise that are meaningful to IT and security objectives, it would be as if these events were pouring into a giant funnel for filtering, refinement, and processing.

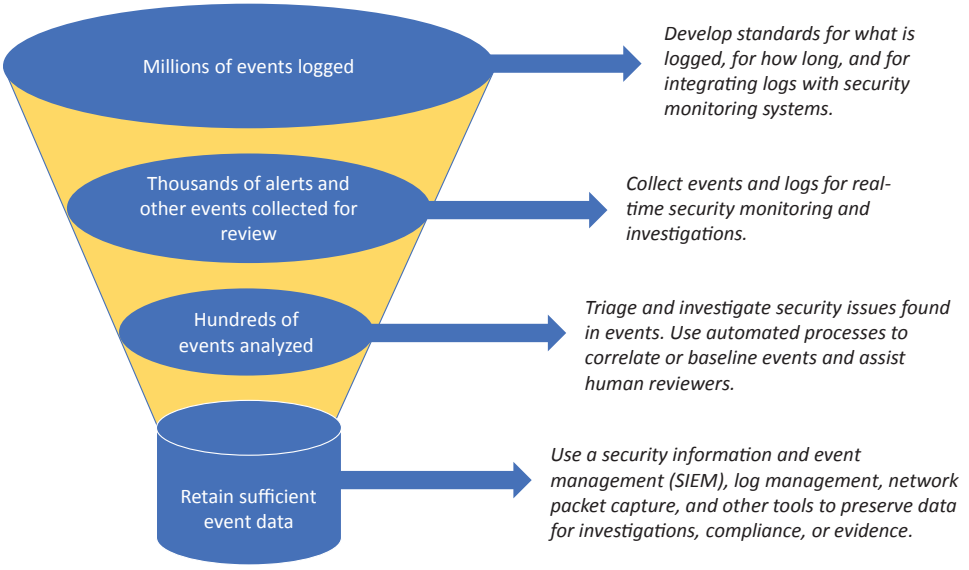

Figure 9-2. *Log and Event Data Generation, Collection, and Processing*

9.4.1.1 Collect Data for Investigations, Retain It for Compliance and Evidentiary Purposes

Many logs collect IT and security data. Even for a small business with less than 100 employees, the security department should be monitoring the firewall, endpoint anti-malware, directory services, email server, and production web/commerce site logs. Use log collection tools to collect some or all the logs' information to a central server. Tool options range from open source Logstash and Elasticsearch to perform basic log collection at the low end all the way to enterprise class SIEMs from vendors such as Splunk, IBM, RSA Security, and others.

A good log collection tool should have some default settings for which events to collect and which to drop. Businesses should generally take advantage of the tools' capabilities to normalize, summarize, or compress events to increase capacity. However, in some cases, business, security, and legal departments should also retain raw logs for evidentiary and forensics use against attackers.

Log data can accumulate fast, even with summarization. To avoid storing too much or too little, work with the legal and compliance functions to set data retention requirements where they apply for critical systems or regulated systems. Even where no regulatory retention requirements exists, note that the longer the retention period, the longer the lookback period available for investigations. For example, suppose we find a hacker penetrated the organization's systems at least two months ago; full network packet capture systems can prove invaluable in tracking down which systems were compromised and which external command and control sites were used in the attack.

9.4.1.2 Use Context to Enrich Events

To avoid generating too many alerts, or false positive alerts (e.g., on *every* instance of multiple login failures to a user account or *every* attempted hack against a server), SIEMs and other tools can automatically correlate events from multiple log and notification sources to gain additional confidence that something is wrong or to prioritize among the many potential issues. For example, a SIEM could prioritize an alert about a system logging port scans (indicative of hacking interest) if the SIEM also learns that said system is

- An executive's laptop (context source: Active Directory)
- A server with unpatched vulnerabilities (context source: vulnerability scanner)
- A server in the scope of Sarbanes-Oxley (SOX) audits (context source: asset management system

In short directory services, vulnerability management systems, asset management systems, and many other IT security capabilities can provide context to the SIEM or other monitoring tools. Monitoring tools can also use enterprise context information to enrich events and reports with additional information. Keeping context information accurate, up to date, and accessible is a critical success factor for effective security monitoring. Security engineering resources can be dedicated to integrating monitoring tools with context sources.

9-3

Identify IT or security administrators responsible for context sources and engage them in efforts to improve security monitoring capabilities.

9.4.1.3 Automate Monitoring Tools, Processes, and Use Cases

Collecting all the logs and notifications in the world is useless unless the organization reviews the information and investigates and acts when necessary. However, given the high volume of events even in a small organization, human log review can become an insufferable burden. Although required in many cases, it should be supplemented by automated detection systems.

There's a wide spectrum of tools and approaches to automated review. At the low end, security staff can develop in-house tools and scripts to search or summarize log information. We can hire an MSSP to monitor our networks, firewalls, and other systems or logs we give it access to; the MSSP will certainly employ automated log review and analysis on our behalf. We can also obtain a SIEM. At the high end of automated review, we can invest in automated machine learning and other security analytics techniques. Other advanced types of tools include network traffic analysis (NTA), anti-malware sandboxing, data leakage protection (DLP), user entity behavior analytics (UEBA), privileged identity analytics, database activity monitoring (DAM), and more.

A large organization generally employs multiple approaches. It may retain an MSSP to monitor its firewalls and externally facing systems, leverage cloud-native tools such as the Microsoft Azure Security Center, and use a SIEM to monitor internal systems. Also, groups responsible for mission-critical custom applications or specialized tasks such as running DLP may develop homegrown scripts to parse through the logs or customize a general-purpose SIEM. For organizations that have limited budgets or lack most of the tools noted here, there is an opportunity to combine some security monitoring use cases (such as detecting login failures and certain types of vulnerabilities) with IT operational monitoring for service availability or early warning of logical or physical system failure. Automated tooling for operational monitoring can provide a rapid entry for automated security monitoring.

With so many events that could be monitored, businesses need to focus on important use cases such as

- **Monitoring critical assets**, such as *any* suspicious events on a large credit card database
- **Monitoring controls** to prove they are operating correctly for compliance or assurance purposes
- **Monitoring activity against a baseline for anomaly detection:** For example, alert on record spikes in network activity or root administrator access to servers from unusual locations at unusual times

Prioritize developing those use cases that solve the most critical issues or easy ones that have some value to implement. Also prioritize use cases that improve the security monitoring group's capability (e.g., developing a new context source, log integration, monitoring tool capability, or staff skill).

9.4.1.4 Use Human Review to Supplement Automated Systems

Automated monitoring capabilities such as the use of artificial intelligence (AI) in security analytics may seem more glamorous, but the human element continues to comprise an important part of security monitoring. What security teams need to do is *progress from tedious and repetitive log review to tuning and backstopping automated systems*. Human expertise is required to

- Review logs and notifications for indicators that can't (yet) be automatically detected and spot check that automated systems are detecting what is expected
- Provide compliance signoff that logs have been reviewed manually and/or that automated monitoring is operating as intended
- Detect new threats or control failures that haven't been instrumented for automated monitoring
- Complete deployment of automated monitoring use cases and fine-tune them
- Provide human oversight of monitoring change control processes

During early maturity stages, businesses tend to rely more heavily on manual review. Logging standards should include provisions for human log review. In addition, operations runbooks, or procedures, should contain checklists for administrators to verify that all monitoring capabilities are functioning. Looking forward, human expertise is also required to develop automated monitoring use cases.

9.4.2 Investigate and Triage Real-Time Alerts and Issues Found in Logs

By Murphy's law ("What can go wrong, will go wrong"), once the organization begins logging, generating notifications, and performing automated or manual review, many issues get raised. But how does the organization determine which need action and what to do with them?

Issues from security monitoring may fall into the following classes, and the monitoring team should have instructions on what to do with each as shown in Table 9-1.

Table 9-1. *General Security Monitoring Instructions (SAMPLE)*

What to Monitor	What to Do
Precursors to compromise, such as cyberattacks in progress	Investigate and/or escalate to CSIRT team
Indicators of compromise	Investigate and/or escalate to CSIRT team
Signs of control failure	Notify appropriate security operations support team
Signs of system failure	Notify appropriate IT operations support team

Issues relating to indicators of compromise or precursors remain with the security monitoring function and/or the IR function for further investigation and triage. As we'll discuss in the "Respond to Incidents" section, businesses have different approaches for dividing work between the security monitoring and IR functions. Events requiring investigation can go into a "response identification" queue. Some issues should also go to the tiered risk assessment process discussed in Chapter 5.

9.4.3 Modernize and Scale Detection for Distributed Infrastructure

A White Paper for Rain Capital[6] takes us to the frontier of automated detection in widely distributed public or private cloud infrastructure and application architectures. These architectures, especially when combined with ephemeral workloads or services, challenge traditional static security approaches. Detection must be automated, decentralized, distributed to the cloud-native control plane, adaptable to changing service fabrics, and instrumented with response capabilities.

[6]"DevSecOps and Detection Engineering: New Approaches to Security," Jamie Lewis, Rain Capital, December 2018, accessed at www.raincapital.vc/resources

DEVSECOPS AND DETECTION ENGINEERING: NEW APPROACHES TO SECURITY

"Technical solutions for problem detection in distributed architectures require new security solutions. These solutions require real-time visibility and iterative feedback loops for security measures to adapt continually to rapidly changing environments and conditions. Automated detection engineering must be built in to take continuous measurements and make real-time adjustments.

The emerging practice of security chaos engineering proactively probes for failures in security controls through controlled experiments such as randomly shutting down an instance or changing a protection setting. These experiments can be "controlled" in the sense that they occur within a limited blast radius and test failure modes the system is already supposed to cope with. Still, we recommend they be closely-supervised by skilled engineers and DevOps teams."

Jamie Lewis, Venture Partner

Lewis also wrote that detection engineering in distributed architectures involves decentralizing operational security roles and functions. These conclusions align with those from Chapter 7, section "Upgrade IT Operations with DevSecOps and Disciplined Agile." For business building or running large-scale distributed infrastructure, detection engineering and security chaos engineering could become core competencies and require alignment between skilled security, IT, and application engineering teams' resources.

9.4.4 Hunt for Threats Proactively

Considering the "dwell time" survey findings discussed in the section on "Address Common Resilience Challenges," businesses desperately need to overtake cyberattackers. Knowing that in large, complex enterprise environments some threats are probably always present, businesses under regulatory and security pressure should consider maturing their detection processes to proactively hunt for incidents in what is almost a continuous process of investigation and response.

Threat hunting doesn't just require tools (such as UEBA, advanced security analytics, etc.). It requires skilled and dedicated personnel to

- **Increase investigation frequency and cadence** to hone capabilities and anticipate adversaries
- **Perform periodic indicator sweeps** to find specific indicators or precursors of compromise based on threat intelligence such as suspect insider activity, suspect IP addresses or accounts, or malware types and configuration anomalies seen at compromised organizations
- **Pivot or "clone" a hunt** when searching for one indicator leads to signs of other indicators or precursors

9.4.5 Coordinate Detection with Users, Business Stakeholders, and External Parties

An organization's IT systems, their logs, and their notifications may be the most important information sources for detection, but by no means the only sources. Security organizations can develop a Threat Actor Library (see Figure 9-3) identifying the categories of threat agents most motivated to attack the business and also analyze the types of threat events such agents could (or already have) created.

9-4

Engage knowledgeable internal and external sources to understand the risks and early warning indicators of compromise from each type of threat.

As they break threats down by category, and classify threat actions as shown in Figure 9-3, security and risk analysts can find many opportunities to improve detection by aligning with knowledgeable internal and external sources. Engage human users as sensors and develop processes for obtaining specialized security tips from other departments (such as HR, procurement, or facilities). Analysts should also take advantage of third-party security monitoring information or notifications and obtain threat intelligence from security information sharing bodies.

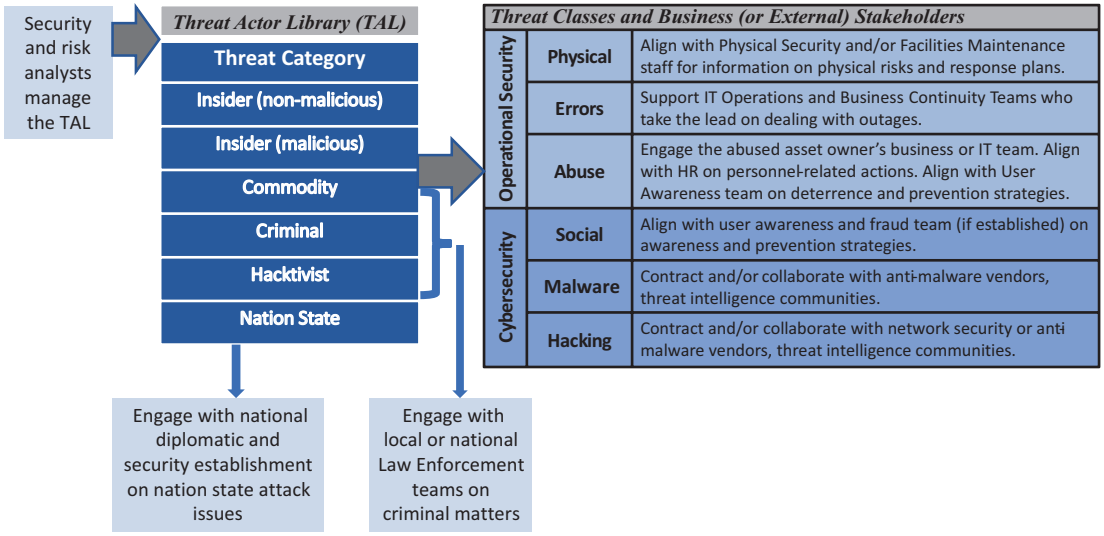

Figure 9-3. *Aligning with Business and External Stakeholders to Detect and Respond to Threats*

9.4.5.1 Engage Human Users as Sensors

IT users, developers, business users, partners, customers, or even someone in the general public – that is, anyone outside the security organization itself – may be the first to notice something unusual in the IT environment or pick up on some other threat to the organization. In the case of social engineering or physical attacks, human intelligence ("humint") may be the only notification source.

Establish well-publicized ways for users to contact or notify the security team about issues they observe. Notification methods can include ticketing systems, contact email addresses, and web forms. There may be a public-facing security contact mechanism. The security organization should also focus awareness training on IT or customer support functions (such as help desk and sales account representatives) to encourage such staff to look for security issues and report them through the notification process.

9.4.5.2 Develop Collaborative Processes with Business Functions

In addition to using IT or customer support functions as notification intermediaries, security functions should work with other corporate administration functions such as HR, physical security, third-party risk management (TPRM), facilities, and sales to obtain early warning of security issues (or even risk scores on individual users, vendors, or facilities) as follows:

- **Legal and HR** may be the first to see early indicators of insider risk, such as formal disciplinary actions and complaints against staff. At a minimum, HR staff (or an employee's manager) should give the security organization a "heads up" about certain types of issues with key users, e.g. a highly privileged IT administrator being formally disciplined. Consult the legal department, however, before monitoring or profiling internal staff. The rules may vary by jurisdiction and based on whether monitoring targets the user's personal device or a company-issued device.
- **Sales, marketing, research, and other business functions** are the data owners and risk owners. They are often best positioned to identify sensitive data and decide when to block use or transfer of sensitive data.
- **TPRM or vendor management** should track negative press reports, financial reports, or complaints about suppliers or partners as a matter of course. At a minimum, it should notify the security organization when a vendor is in the process of being terminated.
- **Facilities teams** should track break-ins, reports of thefts, and other issues with facilities and make the information available to the security organization.
- **IT and development functions** are well positioned to discriminate alerts that are harmless anomalies from those that are precursors to compromise. One CISO we interviewed described a practice of holding contests[7] for IT and security staff to develop original

[7]"Crowdsourced Splunking for Security Exploits," Dan Blum, November 2014, accessed at https://security-architect.com/crowdsourced-splunking-for-security-exploits/

correlation rules for the Splunk SIEM tool. Correlation rules had to use data from two or more logs, at least one of which was not under that author's control.

- **Vulnerability disclosure intake and bug bounties:** Provide an easy-to-find web page and other contact points through which "white hat" vulnerability researchers, law enforcement personnel, and vendors can submit bug reports for custom business applications or tips on potential threats to the business.

Information from these sources should be evaluated by security monitoring or IR teams in case it poses immediate risk. In some cases, it should also go to the organization's information risk team.

9.4.5.3 Integrate Workflows and Notification Processes with Contracted Detection Services

Contracted detection services – such as full-service MSSPs that monitor selected networks and applications and cloud security services like Azure Advanced Threat Protection or AWS GuardDuty – have useful capabilities, but rarely cover an organization's full IT environment. When outsourcing security monitoring tasks, businesses must coordinate closely with the vendor on monitoring and investigating

- Internal areas that are difficult to instrument for MSSP sensors (e.g., custom applications) or highly sensitive (e.g., executive workstations and devices)
- Keeping MSSPs or cloud vendors up to date on asset disposition, points of contact, and other enterprise context information
- Coordinating alert triage or investigation and remediation workflows with vendors
- Jointly developing, maintaining, and testing new monitoring use case capabilities
- Monitoring MSSP or CSP performance against SLA's and other contractual obligations

9.4.5.4 Obtain and Share Threat Intelligence from Security Information Sharing Bodies

Threat intelligence (TI) is especially important for businesses within industries under high security pressure – such as financial services, government, or critical infrastructure. Examples of information sharing bodies include

- Security vendors and other organizations providing open source intelligence or providing threat telemetry for a fee
- Other vendors or partners reporting incidents or breaches they have experienced in their environments, or from your organization, either proactively or under contractual obligation
- Vulnerability researchers disclosing vulnerabilities or exploits (perhaps in response to the organization's bug bounty program)
- Industry Information Sharing and Analysis Centers (ISACs)
- National Computer Emergency Response Teams (CERTs)
- Law enforcement organizations

In its Computer Security Incident Handling Guide (SP 800-61),[8] NIST advises that organizations plan coordination with external notifiers and information sharing organizations in advance. The security organization can work with "coordinating teams" such as US-CERT or an ISAC for the relevant vertical industry. Businesses should also develop communication guidelines for sharing their own information with external parties. Often, sharing technical information such as a suspect IP address or malware sample is low risk and helps establish the organization as a valued member of the information sharing community (and thus making it more likely to receive higher-quality TI). Sharing information about incidents that might have to be reported as breaches, certain kinds of control failures or security configuration information, and any user identity information should only be done with business and legal guidance.

[8]"Special Publication (SP) 800-61 Rev 2 Computer Security Incident Handling Guide," National Institute of Standards (NIST), August 2012, accessed at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

9.5 Respond to Incidents

Most businesses have an underdeveloped and underfunded IR capability. Yet ironically, the ability to interrupt a cyberattack on the organization's crown jewels, or even just provide a satisfactory response to an already large breach, could easily pay the full costs of a multiyear IR program.

Just as police must be able to solve most murder cases within the "first 48" hours, security responders need to stop or contain the spread of potentially dangerous cyberattacks within the first hour or even minutes. I spent considerable space in the previous section on Detection, which is the prerequisite to Response, and I'll refer between these codependent functions often.

With that, let's look at how to plan, establish, and evolve a well-planned phased response model, such as the SANS Institute's six-step process[9] shown in Figure 9-4, for many types of incidents.

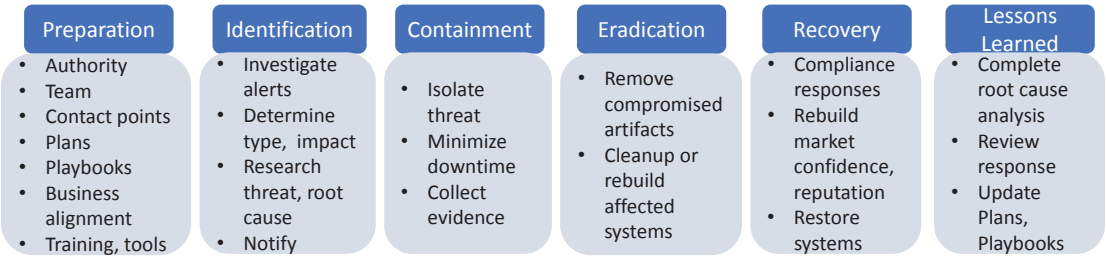

Figure 9-4. *The Phased Response Process*

9.5.1 Plan for Incident Response

Recall from the "Develop Contingency Plans and Cybersecurity Strategy for Resilience" section that the cybersecurity strategy should set directions for both IR and monitoring as well as for outsourcing to MSSPs and breach responders. However, detailed IR procedures for different types of incidents must be created through an ongoing process. Start by crafting an initial response plan that defines types of incidents, provides general guidance and objectives for responding to them, establishes lines of authority or decision rights, and organizes a robust IR function.

[9]"Incident Handler's Handbook," Patrick Kral, SANS Institute, February 2012, accessed at www.sans.org/reading-room/whitepapers/incident/paper/33901

Define: What is an "Incident?" Per NIST SP 800-61: "An information security incident is a violation or imminent threat of violation of data or computer security policies, acceptable use policies, or standard security practices." For example, finding malware on a production server, getting a report of a lost company laptop, or discovering unauthorized accounts, data transfers, or applications (such as cryptomining) would all be considered incidents at many businesses. Security leaders should identify common types of incidents and others that correspond to the business's top risks.

Provide guidance: How should the business respond? The business should already have direction on key staffing, outsourcing, and target IR maturity level decisions. Now it's time to expand the strategy into detailed response plans. Develop plans for a phased response for each type of incident. (Consider one objective: *Quickly eradicate malware using device reimaging tools and get staff working again.* This requires strong backup and restore capabilities, but may trade off most efforts at forensics, evidence gathering, and prosecution to a later time when the IR process becomes more mature.)

Establish authority: Who is in charge of the IR function? Continuing at the most basic level, businesses must designate lines of authority for coordinating IR functions and leading the IR team. Considering basic types of incidents, responses, and impacts, what does the IR function have authority to do (e.g., monitor user accounts, shut down production servers, cut network links, call vendors or partners, notify law enforcement) and under what circumstances? IR authorities and responsibilities vary with the type of incident and are highly contextual to location and other factors. For example, IR leaders may be required to notify law enforcement immediately on discovering threats to human safety and child pornography on a company system but in all other cases defer law enforcement notification to the Corporate Counsel.

9-5

Establish an incident response team to prepare response plans with business executives, legal, HR, vendor management, and public relations. Coordinate their responses during a breach.

Organize IR team: How can we build and maintain a healthy IR function within a security operations team? Security monitoring, technical response, and CSIRT functions require different – though overlapping – staff, skill sets, and personalities. Security monitoring can be somewhat repetitive and predictable, a

stable job. Technical incident response activities are more dynamic and exciting. CSIRT leaders must be able to play the politician, gain support for recovery or response internally, and be prepared to deal with law enforcement, the media, and irate partners or customers.

Figure 9-5 diagrams the interrelationships between the security operations functions supporting IR. The "resource flow" arrows show that although three different functions should exist in security operations, they must all support IR. Very few businesses permanently retain enough staff to cope with major incidents, so IR will tax all security operations functions whenever major incidents materialize.

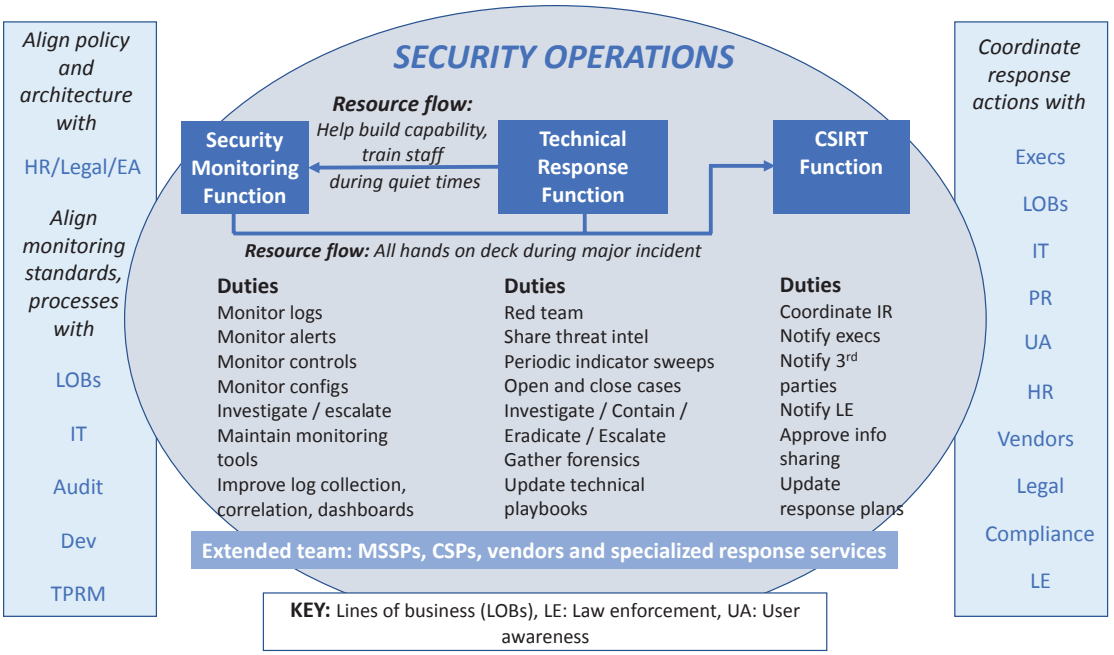

Figure 9-5. *Security Monitoring, Response, and CSIRT Functions*

Just as security leadership must align with the business before and after IR to prepare and coordinate, it must organize itself to endure the IR resource demand peak that occurs during major incidents. However, security leaders must also be aware that the effects of major incidents can persist for some time, especially in the event of legal issues, regulatory investigations, or repeated cyberattacks. With many security teams already under-resourced or under stress, take care to avoid excessive staff burnout and attrition.

Correctly structured, security operations can

- Give burned-out responders a rest when they can be spared; they can train others, update documentation, or work on automating monitoring processes
- Move bright but still junior monitoring staff seeking career advancement into the breach to augment responders during a major incident
- Provide learning opportunities, travel, conference tickets, appropriate time off, and reasonable work-life balance accommodation to all staff
- Work with the teams on developing job improvement strategies, response plans, and playbooks to give them the sense of efficacy that only a well-planned security program operating according to its plan can bring

Consider the guidance from Chapter 2, section "Hire, Motivate, and Retain Key Security Staff," to be especially pertinent for the security operations and CSIRT teams.

9.5.2 Establish the IR Program

Based on the cybersecurity strategy and the initial response plans discussed so far, the business can establish a full set of IR policies, plans, and procedures as well as build out its security operations teams to cope with the ebb and flow of incidents.

Regardless of organization size, a business must prepare for response by specifying policy, identifying points of contact for incidents, and designating a response team. Establish relationships with external IR resources, such as law firms specializing in different types of incidents as well as expert cyber-breach responders on retainer.

Policy: Formalize response plans in a policy identifying IR authority, purpose/objectives, scope, definitions and prioritizations, and basic team structure as well as guidelines for escalation, coordination with external entities, information sharing, and performance metrics. Because recovery should follow response, IR policies must be kept in sync with business continuity plans and policies.

Processes: Establish processes under the policy guidelines for escalation, case management, phased incident handling, and information sharing. Coordinate process development for dealing with suspected insider abuse, law enforcement, media, customers, partners, and facilities with HR, legal, public relations (PR), marketing, and facilities management groups, respectively. Design processes as living documents

implemented through continuously evolving security operations, CSIRT, and IT or development procedures and playbooks.

- **TIP:** Recognize that the CSIRT and security operations functions have major dependencies on the business functions identified in Figure 9-5's sidebars as well as on IT help desk or support and other security specialists. Build business alignment integration points to fulfill these dependencies into processes and procedures. Strong management and communication skills are required for the CSIRT to coordinate with multiple groups affected during incidents. Organizations under high security pressure should provide role-specific awareness training throughout the business to prepare staff for IR needs.

Staff up: All but the very smallest businesses should have the three distinct security operations functions shown in Figure 9-5. The number of staff providing security operations and IR can range from a pair of employees with several roles covering all three functions to multiple teams totaling many more than 20 people for very large businesses with 24x7 SOCs and per-incident leaders in the technical response and/or CSIRT functions. Ensuring sufficient resources are available to provide coverage for all three functions is critical; otherwise IR outcomes, staff retention during long-running incidents, and the ability to continue normal monitoring to head off further incidents could all be negatively impacted.

- **TIP:** Retain enough staff to handle the security monitoring workload plus technical response to ongoing incidents such as malware remediation, system restoration, and lost devices. Consider combining internal monitoring and response with a robust MSSP to reduce the need for in-house staff. Employ a core CSIRT team and (if risk warrants) technical response staff experienced in threat hunting. Institute job rotation and cross-training to get the best "mileage" from the security operations and CSIRT staff. Consider retainer contracts for specialized cyber-breach responder resources for further staff augmentation during major incidents.

Tool up: Most of the tools required are security monitoring tools identified in this book's Glossary, such as SIEM, UEBA, DLP, anti-malware, and others. IR also requires a case management tool. At the low end, an ITSM tool can track incidents. However, specialized case management tools provide more IR-specific functionality, such as forensics support and connections to threat intelligence sources. At a minimum, ensure that IT help desk and

other support staff outside the CSIRT cannot access sensitive incident information. Finally, don't forget that responders need adequate resources such as documented playbooks for common incidents, standard *and* investigative workstations and laptops, private conference rooms, redundant and protected communication methods, baseline virtual machine files available to quickly reimage or restore systems, and more.

9.5.3 Evolve the IR Program for Cyber-Resilience

The IR program is the centerpiece of cyber-resilience in the sense that it not only embodies Respond controls but also interacts with Detect and Recover controls. Response requires Detect controls to identify the threat (triggering response) and to verify containment and eradication. Then, Response initiates Recovery.

Businesses can evolve cyber-resilience capabilities up to Level 3 maturity (Defined) by creating contingency plans, IR policies, processes, and playbooks as well as basic automated monitoring capabilities. Level 3 IR already requires expanding staff, establishing the dedicated IR function, and spreading awareness of basic IR plans, roles, and responsibilities to security, business, and IT stakeholders.

Businesses under medium security pressure should consider – and those under high security pressure must – attain at least the Level 4 maturity (Managed) for security monitoring and IR. Getting to Level 4 requires yet more advanced tools and processes, including context- and correlation-enabled automated detection, alert investigation/triage, threat intelligence sharing, staffing a dedicated response function, and implementing all defined cyber-resilience processes more comprehensively across the business.

As the IR program evolves to Level 3 or Level 4 (Managed), it can develop the skills, resources, and playbooks for incidents the organization expects to eventually experience, as well as frameworks to address unexpected incidents. Conduct simulated incident exercises to prepare staff. Ensure response capabilities cover multiple IT environments including private clouds, public cloud such as AWS or Azure, and enterprise applications or SaaS. In some cases, CSPs such as Amazon[10] or Microsoft Azure[11] provide cloud-based detection and response tools and processes; customers should use these capabilities but must keep driving the response process themselves.

[10] "AWS Security Incident Response Guide," Amazon, June 2019, accessed at https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

[11] "Tutorial: Respond to Security Incidents," Microsoft, August 2018, accessed at https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-incident

Standard operating procedures or playbooks for incidents should describe in detail how to identify, contain, and eradicate the incident-inducing threat. Make sure that playbooks identify all the integration points (contacts and procedures) that align IR to other business functions. For example, IR processes will hand off the technical response function to IT groups when it is time to "recover." Provide detailed guidance and decision trees in the playbooks on how and when to communicate with law enforcement, the media, and other third parties. Use NIST 800-61[8] Appendices A.1 and A.2 as starting points; the Appendices provide a list of questions to leverage for playbooks on multiple types of incidents.

9.6 Recover from Incidents Caused by Cyberattacks and Operational Outages

Recovery is different for incidents caused by cyberattacks than for those caused by IT system outages. In the case of a breach from a cyberattack, the technical security response team takes the lead during the IR recovery phase and may later hand off to IT or business continuity teams to lead recovery. In the case of an outage, IT and business continuity teams handle the recovery, and security operations may not need to be involved. Figure 9-6 depicts the high-level sequence of response through recovery activities for breaches and/or outages.

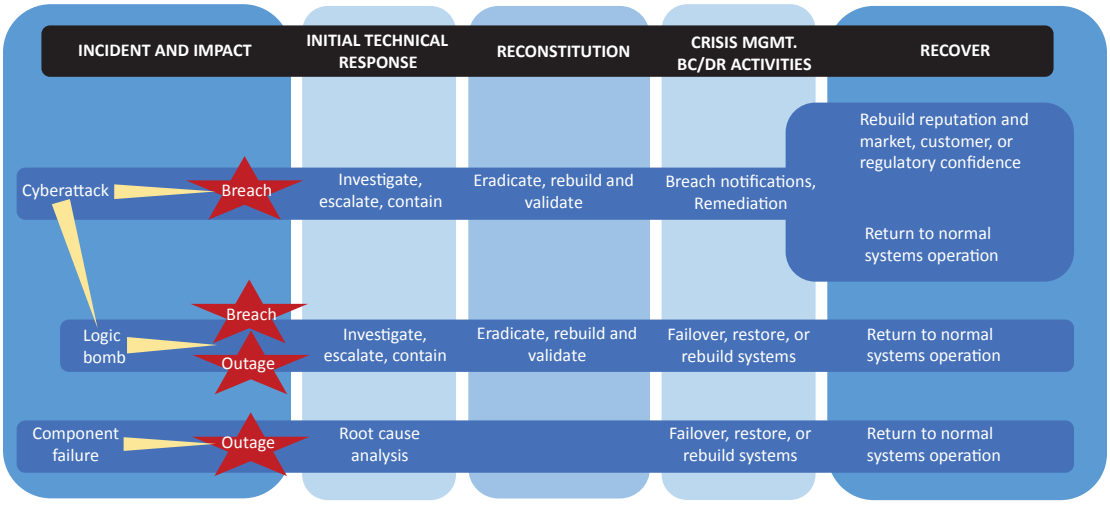

Figure 9-6. *Breach and/or Outage Response and Recovery*

Incident and impact:

- **Cyberattack scenario:** Figure 9-6 depicts a breach – such as theft of personal or confidential information. Once it is discovered, staff should perform an investigation to assess the impact of the breach and deny the attacker reentry, but in this case may not need to take down production systems.
- **Logic bomb scenario:** Suppose the same malicious actor causing the breach also left a logic bomb that damages production systems. This incident requires the IR team to lead a response, but because it also causes an outage, BC/DR plans should be activated.
- **Component failure scenario:** Figure 9-6 also depicts an operational outage due to a component failure, which could have been caused by human operator error, hardware failure, or some aberrant interaction of software and services. No malicious actor is suspected.

Initial technical response: For all breaches and outages, it's important to pinpoint the threat event. Why has the incident occurred, is it over, or is it just beginning? In the event of a cyber-incident, expect the worst from the malicious actor. Contain the cyberattack from causing further damage. Escalate notifications, support requests, or decisions to business functions such as legal, HR, IT, development, and executive management as required.

Reconstitution: Only after initial technical response and investigation completes can the IR functions fully reconstitute affected systems or applications by eradicating cyberattack artifacts such as malware, backdoors, compromised accounts, and so on. In some cases, systems are down and must be rebuilt to recover from an outage due to a cyberattack. In other cases, systems don't go down but some must be taken offline and surgically rebuilt to ensure no trace of malware remains. When rebuilding systems in this way, be sure to perform thorough scans and take other measures to validate they are clean. Reconstitution involves returning systems to fully operational states. It reflects mission and business priorities and may be driven by recovery point/time objectives and other metrics.

Crisis management, BC/DR activities: Any major breach of confidential information can provoke a crisis. In the case of an identity data breach, the IR team must coordinate notification of authorities, partners, the affected persons, and the media.

In the case of a breach of trade secrets, the business must notify partners where contractually required, and may have to scramble to contain further legal and market impacts.

Treat crisis management as the tactical problem that it is. The sequence of steps required to investigate and remediate the breach, notify interested parties, or make restitution vary with the type of breach. Response plans rarely cover 100% of the actions needed during a crisis but should lay down guidelines, requirements, and responsibilities to facilitate and speed decision making.

Recovery: Although business systems such as ecommerce sites may never actually shut down during the breach and the recovery goal is usually to continue normal operation, few businesses emerge from a breach unscathed. Post-breach businesses may move into a "new normal" of partner dissatisfaction or regulatory scrutiny that requires short-term changes to pricing, business practices, and supporting technologies. Over the long term, the business must work to rebuild damaged reputation, market share, and regulatory confidence.

9.6.1 Activate Business Continuity and Disaster Recovery Plans

BC/DR activities: In the event of an operational outage, BC/DR plans kick in. These plans should call for a root cause analysis, though this may be a quick process for outages that are due to a known and expected failure mode. Based on the BC/DR plans, determine the best course of action to restore normal operation: Failover has the least impact and may be possible for known incidents to critical systems with a hot standby capability. Restoring or rebuilding systems has more impact but continues to be an IT or development-led project.

9.7 Call to Action

The core recommendations for security leaders from this chapter are to develop cyber-resilience as follows:

- Identify critical assets through a BIA and create a BC/DR plan.
- Identify top risk scenarios through enterprise risk assessment and document risk appetites.

- Identify contingency plans for response and recovery.
- Identify strategic decisions (or phasing) for use of MSSPs, cyber-insurance, breach response services, and 24x7 SOC.
- Create detection capability by
  - Standardizing basic logging, log collection, and log review across IT environments
  - Developing basic automated event and alert monitoring
  - Engaging knowledgeable business and external stakeholders to understand and help monitor for threats
  - Advancing security analytics, detection engineering, and proactive threat hunting (required for organizations under high security pressure)
- Prepare response capability by
  - Designating a dedicated CSIRT role or forming a team; coordinating response plans with business executives, legal, HR, TPRM, public relations, and so on
  - Developing playbooks and procedures for technical response, investigation, escalation, and stakeholder notification during a breach
  - Ensuring response (and recovery) plans include a lessons learned phase in which gaps can be identified and procedures updated
- Lay the groundwork for recovery by
  - Planning separate but overlapping processes for responding to cyberattacks and operational outages
  - Ensuring that senior business stakeholders support the business continuity program and that the key IT team members who work "hands on" with mission-critical services are engaged

Action – Make a quick assessment of the organization's cyber-resilience

Ask yourself the following short set of questions and score the answers in the Success Plan Worksheet's[12] Section 3, Table 3. Base your score on whether you would answer most of the questions with a strong "no" (1), a strong "yes" (5), or something in between.

1. Does the business have
   a. Log standards?
   b. A security operations center (SOC) and/or an MSSP?
   c. A security information and event management system (SIEM)?
   d. A Computer Security Incident Response Team (CSIRT)?
2. Does the business have incident response plans and playbooks?
   a. Have these plans and playbooks been proven effective in real incidents or tests?
3. Does the business have an asset inventory and a current business impact assessment (BIA) identifying critical assets?
4. Does the business have a business continuity and disaster recovery (BC/DR) plan and program?
5. Has the BC/DR plan been tested?

Action – Define 1–3 improvement objectives for cyber-resilience

Note improvement objectives in Section 4, Table 10, of the worksheet. The following are some sample improvement objectives.

- Review contingency plans for incident response for the business's top risk scenarios or critical assets. Identify and list which are missing. If none are complete, develop a detailed outline for at least one plan and discuss it with affected stakeholders.
- Review incident response policies and procedures with affected stakeholders to ensure they are up to date and still agreed on.
- Review BC/DR plans with affected stakeholders to ensure they are up to date and still agreed on.

[12]"Rational Cybersecurity Success Plan Worksheet," Dan Blum, Security Architects LLC, May 2020, accessed at https://security-architect.com/SuccessPlanWorksheet

CHAPTER 10

Create Your Rational Cybersecurity Success Plan

This has been *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment*. I've made this guidance as detailed and specific as possible because all too often, we get only platitudes or generalizations on the topic. We can't afford that anymore. Misalignment between security and the business has a corrosive effect on any security effort it touches. And as organizations transform into digital businesses, they fall under increasing IT-related risk and regulation. Aligning security to business leaders and business processes is exponentially more important now.

In this final chapter, let's go through what we've covered in the book and help you complete a Rational Cybersecurity Success Plan Worksheet[1] to record your progress pursuing cybersecurity-business alignment.

The Success Plan uses a simple methodology with just a few steps:

1. Scope out priority focus areas.
2. Make a quick assessment of your current state.
3. Identify stakeholders (in security-related business roles).
4. Define improvement objectives (within your priority focus areas).
5. Identify metrics.
6. Track progress.

[1] "Rational Cybersecurity Success Plan Worksheet," Dan Blum, Security Architects LLC, May 2020, accessed at https://security-architect.com/SuccessPlanWorksheet

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8_10

The priority focus areas, or priorities, always refer to the six Rational Cybersecurity Pareto Priority areas described in Chapter 1 and throughout the book.

Action: *Don't skip this chapter!* Even if you're an extremely busy CISO it will be worth your while to work through these exercises (or delegate them to a trusted staff member and monitor the learnings and improvement opportunities).

Print out or open a copy of the Success Plan Worksheet to edit online as you go through Chapter 10.

Note If you have already filled in parts of the worksheet during earlier chapters, use this chapter to recheck or complete your work on steps 1–4, then proceed to steps 5 and 6.

10.1 Scope Out Your Priority Focus Areas

Not all readers head up the whole security program. Not all CISOs or security leaders have the same starting point or wish to work on all the priority focus areas simultaneously. Starting where you are, here's how to calibrate the scope of your Success Plan. New CISOs or CISOs with a mandate to expand or reshape the security program should consider acting on all six Rational Cybersecurity priorities. Other security leaders – such as well-established CISOs just wanting to tweak their program, part-time interim CISO caretakers, or security managers under the CISO – should primarily focus on the priorities within their own area of responsibilities or where they see the greatest gaps and opportunities.

Action: Check mark your priority focus areas in Table 1, Section 1, of the Success Plan Worksheet.

10.2 Identify Stakeholders

Chapter 2's section "Clarify Security-Related Business Roles" and Table 2-2 contain a list of typical stakeholder roles. In a small business, some of the roles may not exist and others will be combined in a few people. In a large business, multiple people may fill some of the same roles across business units. Prioritize relationships with all stakeholders or just with the ones covering your priority focus areas.

Action: Fill in the name of the person holding each role identified in Table 2 of Section 2 in the worksheet. If a role doesn't exist or is called something else at your organization, then remove, edit, or annotate the rows in Table 2 as necessary. In the Contact Plan

column, note whether the person should be contacted now or later and who will be the relationship manager (i.e., you or someone else from the security team). Fill in the Notes column with any known projects, issues, or pain points to cover with the stakeholder.

10.3 Make a Quick Assessment of Current State

The following exercise doesn't replace a more in-depth, formal assessment, but it can help set quick, actionable improvement objectives.

Make a quick assessment of the current state of security practice for each of your priority focus areas. **Base the scoring criteria for each area on how you'd answer the majority of the questions for it provided in the following "Sample Criteria to Consider During Scoring":** Strong "no" (1=strongly disagree), qualified "no" (2=disagree), a balance of "yes, no, maybes" (3=neutral), qualified "yes" (4=agree), or strong "yes" (5=strongly agree).

If you can't provide an educated guess at the 1–5 rating for an area, leave it blank and proceed to the next exercise. You'll be able to come back and finish this once you've had more time to think about it and/or talk with specialists or stakeholders. Also, if you're actively working on improving security practices and business alignment in a focus area, return to the worksheet to make changes in your assessment at later milestones (3 months or 6 months).

Action: Mark the scores from 1 to 5 for each row in Table 3 of Section 3 in the worksheet corresponding to your priority focus areas. Record any notes about your assessment score for each priority focus area in Table 4. Be brutally honest – no one has to see this except you.

Sample Criteria to Consider During Scoring for each focus area:

Develop and Govern a Healthy Security Culture:

Security governance:

1. Does the security governance structure align well with the way IT and the business are organized?
2. Is the business's definition of security (mission, structure, and operating principles) captured in the security charter, and is it reflective of the way the business really works?
3. Does a security steering committee meet regularly; do security, IT, corporate administration, and LOB representatives with signing authority regularly attend it; and is it effective at addressing cross-functional security issues and moving security projects forward?

4. Does a risk management forum exist and does it hold business risk owners accountable for risks and serve as a useful venue for reviewing top risk analyses and treatment recommendations?
5. Are security policies, standards, processes, and procedures generally up to date and do day-to-day practices in the business generally follow them?
6. Is the security budget centralized, or are multiple security budgets rationalized in the sense that relatively little overlap exists?

Security culture:

1. Do business executives prioritize and support cybersecurity (i.e., consider it strategic)?
2. Do business, IT, and development managers provide resources to security projects and help enforce security policies?
3. Do security team members have positive relationships and communications with business stakeholders?
4. Does the CISO treat communicating with IT and business leaders as being a top priority?
5. Are security leaders incentivized to
    a. Maintain regular communication with IT and business leaders in their functional area?
    b. Improve their communication skills and those of their team members?
6. Does the security organization have a user awareness function sized to the business?
7. Does the user awareness and training function
    a. Communicate in an efficacious manner ("we can do this," "here's how others have been [safe, successful]")?
    b. Target awareness programs to specific audiences?
    c. Coordinate programs with the audiences' leadership?
    d. Provide role-specific training?

e. Recruit champions among the target audiences and "train the trainers"?

f. Provide information or free tools that will help staff and their families improve cybersecurity at home?

g. Coordinate with the marketing organization's internal communications program?

h. Use innovative and entertaining communications mediums, products, or services?

8. Does the security leadership or awareness program itself measure whether awareness and training programs are improving

   a. Security-related behavior?

   b. Attitudes and perceptions about the security program?

   c. Understanding of policies, tools, and procedures (cognition and compliance)?

   d. Compliance audit results?

Manage Risk in the Language of Business:

1. Are business owners held accountable for information risk?
2. Are business, IT, and security teams using consistent terminology for discussing risk and consistent criteria for assessing risk?
3. Are stakeholders coming to security for guidance or advice before taking important decisions that could create risk?
4. Are risk assessments used to prioritize security projects, manage third parties, or make other decisions?
5. Is a quantitative risk analysis methodology in use?
6. Are issues, risks, exceptions/acceptances, and top risks monitored in an issue management system; IT governance, risk, and compliance (IT GRC) tool; and/or risk register?
7. Are top information risks being regularly communicated to executives and the Board, and is the dialogue constructive?

Establish a Control Baseline:

1. Does the business have a "control framework" and/or a "control baseline" document that lists the control objectives for IT and the business?
2. Does the security organization have published guidance mapping the control objectives to the required control activities for different levels of risk or different situations (e.g., data classifications, use of third-party services)?
3. Is the control baseline mapped to requirements documents and solution architectures for critical operational systems in IT and security environments?
4. Is the control baseline updated and followed?
5. Do IT, security, or third-party management groups have a shared responsibility framework to aid in evaluating third-party services?
6. Does an architecture document specify how the controls should be deployed?
7. Does the business have an assurance or an audit function to verify controls are operating?

Simplify and Rationalize IT and Security:

1. Does the business have a simplified and rationalized IT environment?
2. Is there a published, up-to-date IT strategy?
3. Has the security strategy aligned to the IT strategy?
4. Is the business use of a hybrid multicloud environment governed well?
5. Does IT publish a service catalog and are security services included in it?
6. Does the security organization work closely with third-party management to assess third-party risk early in the commercial evaluation process?

7. Is the security organization working with DevOps teams to develop DevSecOps processes?

Control Access Without Creating a Drag on the Business:

1. Does the business have a cross-functional identity and access management (IAM) team?
2. Does the IAM team report to or coordinate with security?
3. Does the business have coherent access policy models (roles, rules, and groups) in key IT environments?
4. Can IAM systems quickly enable new digital relationships for new applications or business partners?
5. Does the business have someone working on data governance?
6. Does the business have a Chief Privacy Officer or a Data Protection Officer?
7. Are data stewards, or data owners, assigned for sensitive or business-critical information?
8. Does the security department know where all the sensitive data is stored?
9. Are privileged access rights (i.e., root account or domain administrator) restricted to small groups of users?
10. Is privileged access controlled or monitored?

Institute Resilient Detection, Response, and Recovery:

1. Does the business have
    a. Log standards?
    b. A security operations center (SOC) and/or an MSSP?
    c. A security information and event management system (SIEM)?
    d. A Computer Security Incident Response Team (CSIRT)?

2. Does the business have incident response plans and playbooks?
    a. Have these plans and playbooks been proven effective in real incidents or tests?
3. Does the business have an asset inventory and a current business impact assessment (BIA) identifying critical assets?
4. Does the business have a business continuity and disaster recovery (BC/DR) plan and program?
5. Has the BC/DR plan been tested?

10.4 Identify Improvement Objectives

Consider each of the Rational Cybersecurity priorities you've selected or all of them. Define one to three improvement objectives for each priority and enter them into the Identify Improvement Objectives table row for each priority. As much as possible, emphasize quick-hitting improvement objectives to keep this effort fluid, maintain momentum, and expose problem areas sooner.

The following subsections provide some example improvement objectives for each priority focus area. The reader can consider the examples, but understand they are only a few of many possible areas to improve.

In general, the examples focus on improving the kinds of issues a security organization with low maturity in the Focus Area could have. They also emphasize work that can be done in alignment with stakeholders outside the security organization.

Choose improvement objectives that fit the business's current gaps, maturity level, and priorities. It should be possible to accomplish each objective in the short term (less than 90 days). If necessary, break critical but large improvement objectives down into smaller chunks.

10.4.1 Develop and Govern a Healthy Security Culture

Action: If "Develop and Govern a Healthy Security Culture" is one of the selected priority focus areas, note improvement objectives in Section 4, Tables 5a and 5b, of the worksheet. Use the examples in this section to help choose three to six improvement objectives based on Chapters 3 and 4.

Security governance:

- Create or revisit the security charter and work on getting business buy-in for a definition of security that is fully aligned with the business needs.
- Review Chapter 2's Table 2-2 listing security-related business roles to find any that seem appropriate for a business like yours but aren't being fulfilled. Communicate with stakeholders and find out the reason.
- Plan for a security policy refresh and identify business stakeholders affected by the current policy documents and potential new ones.
- Review the minutes or records from the last 6–12 months of security steering committee (or other coordinating group) meetings, review its strengths and weaknesses, and propose improvements.
- Work with the business finance office to collect information on all security budgets, sources of funding, and funded project charters. Call out any obvious gaps or overlaps.

Security culture:

- Continuously maintain the worksheet stakeholder engagement information in Table 2.
- Assess your communication style or habits and improve at least one practice.
- Get the security team to assess group communication styles or habits and improve at least one practice.
- Create and manage at least one practice for user awareness and training improvement (e.g., task key team members to collect feedback from one to three business or IT stakeholders on security-related communications).
- Prepare an informal briefing on security culture (using this chapter as a resource) and present or discuss it with at least one of your business or IT executive sponsors.

10.4.2 Manage Risk in the Language of Business

Action: If "Manage Risk in the Language of Business" is one of the selected priority focus areas, note improvement objectives in Section 4, Table 6, of the worksheet. Use the guidance and examples in this section to help choose one to three improvement objectives based on Chapter 5.

If the business doesn't yet have a formal information risk management program, look for improvement objectives in section "Establish the Context for the Risk Program." For example:

- Perform a PESTLE analysis[4] to understand and document the risk program's business context and discuss it with at least one business or IT executive sponsor.
- Task security and risk team members unfamiliar with FAIR to read section "Open Factor Analysis of Information Risk (FAIR)" and the Open Group Standard: Risk Analysis (O-RA)[7] and other FAIR resources.[2]

To improve a risk management program that's up and running, consider the following sample improvement objective:

- Review the organization's asset inventory program and identify an IT champion willing to work with the risk management function on devising a method to capture asset risk scores and risk metadata as described in section "Implement Asset Risk Profiling."

To improve identification of top information risk at the executive level, consider the following sample improvement objective:

- Meet with executive stakeholder(s) responsible for reporting risk to an Audit Committee (or other risk management forums). Identify or discuss
  - Who are, or could be, accountable risk owners for categories of information risks
  - Potential overlaps between information risks and top enterprise risk scenarios

[2] "FAIR Resources," Dan Blum, Security Architects LLC, January 2020, accessed at https://security-architect.com/RiskManagementResources

Readers seeking more assistance or guidance on building a risk program can contact us via our website (https://security-architect.com/contact-us) or visit our risk management resources page.[3]

10.4.3 Establish a Control Baseline

Action: If "Establish a Control Baseline" is one of your priority focus areas, note improvement objectives in Section 4, Table 7, of the worksheet. Use the guidance and examples in this section to help choose one to three improvement objectives.

As you'll recall, the purpose of a control baseline is to create the minimum viable list of controls from the security control domains that apply to the business, map the controls to the business IT environments, and develop applicability guidelines for them. From Chapter 6's section "Address Common Challenges," however, we found many issues and gaps in the way businesses typically address controls. The following are suggestions for quick-hitting improvement objectives:

- Evaluate the current control baseline document(s) to see if they can be used as is or as a draft starting point.

If the business requires a new or rewritten control baseline:

- Create an initial detailed outline for a new control baseline using a spreadsheet or a governance, risk, and compliance (GRC) tool. Populate the draft using information from the 20 security control domains in Chapter 6.

If a current and credible security assessment is not available:

- Perform a rapid enterprise risk assessment based on the methodology from Chapter 5, section "Perform Enterprise Risk Assessments to Identify Top Risk Scenarios," using available data to identify at least a rough list of top information risks.

[3] "Risk Management Program Review," Dan Blum, Security Architects LLC, January 2020, accessed at https://security-architect.com/RiskManagementResources

- Perform a control gap assessment against the control baseline and the list of top information risks. Depending on the size of the business, rapid or deep security assessments[4] can be performed within a 30-60-90-day period.

Note A good security assessment is a control assessment aligned to a list of top information risks.

10.4.4 Simplify and Rationalize IT and Security

Action: If "Simplify and Rationalize IT and Security" is one of your priority focus areas, note improvement objectives in Section 4, Table 8, of the worksheet. Use the guidance in this section to help choose one to three improvement objectives based on Chapter 7.

Understand that a secure digital business must be one that continually plans, curates, and aligns IT capabilities in a defensible architecture. From Chapter 7's section "Address Common Challenges," however, we found many issues with technical debt, lack of IT strategy, and difficulty keeping pace with LOB requirements and shadow IT. The following are some example improvement objectives:

- Locate document(s) labeled as an "IT Strategy" or serving that purpose. Provide security organization commentary on them and discuss with the IT stakeholders. Align them with the current security project portfolio or road map as appropriate.
- Help the IT organization operate in the "IT-as-broker" mode by collecting information on cloud-based security services options (e.g., vulnerability scanning, multifactor authentication, etc.) it could provide or encouraging adoption of services already provided.
- Analyze development tool chains in use and discuss potential DevSecOps solutions with development managers.

[4] "Security Assessments," Security Architects, LLC, May 2020, accessed at: https://security-architect.com/SecurityAssessmentResources

Evaluate the opportunity to set up Security Championship Program(s) in IT. Discuss the idea with senior IT managers that might support the idea and/or identify staff members in IT that might be good candidates in championship roles.

10.4.5 Control Access with Minimal Drag on the Business

Action: If "Control Access with Minimal Drag on the Business" is one of your priority focus areas, note improvement objectives in Section 4, Table 9, of the worksheet. Use the guidance and examples in this section to help choose one to three improvement objectives based on Chapter 8.

Access control and data governance are critical for enabling digital businesses to use applications and tools productively, to form new digital relationships with customers and other external parties, and to stay in compliance with regulations. From Chapter 8's section "Address Common Challenges," however, we found many IAM infrastructures are outdated, IAM and data governance processes are immature, and IAM teams lack cross-functional buy-in.

Of all the Rational Cybersecurity priorities (with the possible exception of risk management), IAM and data governance are the most complex ones.

- Conduct a rapid security assessment focused on IAM and data governance[5]; together they constitute a large and critical piece of the security program.
- Identify quick-hitting IAM improvement projects. Use the business impact assessment (BIA), the enterprise risk map, or other sources to find critical assets and risk owners; map the IAM and data governance control baseline (per Chapter 8, Table 8-1) against the assets and connect with one to three stakeholders to learn their IAM and data governance pain points.

[5]"IAM Assessments," Security Architects, LLC, May 2020, accessed at: https://security-architect.com/IAMResources

If you are the CISO (or "Head of Security") but the IAM team reports to another organization and isn't closely aligned to security:

- Strengthen the dotted-line reporting relationship of the IAM team to security. To do this, work with the CIO or other higher executive functions over IAM.

10.4.6 Institute Resilient Detection, Response, and Recovery

Action: If "Institute Resilient Detection, Response, and Recovery" is one of your priority focus areas, note improvement objectives in Section 4, Table 10, of the worksheet. Use the guidance in this section to help choose one to three improvement objectives based on Chapter 9.

As we discussed in Chapter 9, section "Business Unpreparedness for Incident Response and Recovery," businesses in 2020 will continue to face an elevated threat environment. Due to unpreparedness or immaturity as well as "Lack of Visibility or Access to All IT Systems," IT and security leaders may not have their defensive priorities clearly focused on critical systems. It's inevitable that "Protect" controls will sometimes fail.

The following are examples of cyber-resilience improvement objectives:

- Review contingency plans for incident response for the business's top risk scenarios or critical assets. Identify and list which are missing. If none are complete, develop a detailed outline for at least one plan and discuss it with affected stakeholders.
- Review incident response policies and procedures with affected stakeholders to ensure they are up to date and still agreed on.
- Review BC/DR plans with affected stakeholders to ensure they are up to date and still agreed on.

10.5 Specify Metrics

Some improvement objectives are one-time projects. But others require recurring activities or processes.

Note any ongoing improvement objective whose progress you'd like to track in the Specify Metrics in Table 11, Section 5, of the worksheet. For each, list one to three top metrics. I filled in examples for the "Increase CISO and security team communication with stakeholders" objective:

- #Stakeholder 1 on 1 meetings
- #Stakeholder team briefings

"Cybersecurity is a contact sport."

Craig Callé, CEO at Source Callé, LLC

10.6 Track Progress

Action: For each priority focus area where you have improvement objectives

- Use Section 3's Tables 3 and 4 to update your quick assessment ratings of the priority focus areas at the 30, 60, and 90 days' marks.
- Use Section 5's Table 11 in the worksheet to track your progress with each of your identified improvement objectives' metrics.

10.7 This Is Not the End

Cybersecurity-business alignment is an ongoing effort. We do it because security is an inherently cross-functional activity. Per Chapter 7, Harvard Business Review research found that 75% of cross-functional teams are dysfunctional, but that projects with strong governance support have a 76% success rate. The cross-functional challenges – and the potentially disastrous consequences of business *disengagement* – are why security leaders should prize alignment so highly and constantly work to make it happen.

But maybe you finished the book and wonder, what now? Hopefully not, because if you took the opportunity to work through the Success Plan, you'll have written down some action items. I've concluded the book in an actionable manner precisely so you wouldn't have put it down with that "So what?" feeling.

We have much to do just to accomplish the six Rational Cybersecurity priorities. That's why the Success Plan encourages setting quick-hitting improvement objectives and provides a framework to track progress. Don't try to boil the ocean with your first Rational Cybersecurity Success Plan; make it an iterative process. If you stick with it, you'll still be here 90 days from now moving forward with cybersecurity-business alignment. Step by step. "Baby steps can take us up Mount Everest," as my life coach likes to say.

You'll want to continue taking action after 90 days, setting successively more impactful improvement objectives.

Meanwhile, I'm hoping that the work of Rational Cybersecurity continues to evolve. Together, we can create additional iterations of the guidance in the "Define Rational Cybersecurity Improvement Objectives." In the published edition you've just read, I've assumed we're just getting started and suggested very basic improvement objectives. But I have to believe that – if security leaders focus on cybersecurity-business alignment – our capabilities will mature significantly and improve business's cybersecurity outcomes. If we reach the point where the example improvement objectives in this chapter seem like baby steps and more advanced ideas online take them up a few levels, we will have succeeded.

There is a great opportunity for the security leader with strong communication skills and an understanding of what's needed to make cybersecurity more strategic to the business and better aligned with stakeholders. Be that leader. You don't have to do it alone. Engage your staff in the vision of a Rational Cybersecurity program. Engage with a community of others in a journey of continuous learning about how we can become more effective at aligning and running our cross-functional projects.

10.8 This Is the Beginning of an Open Information Flow

Rational Cybersecurity for Business has been released via Open Access under the Creative Commons license so that we can create an open information flow to fully use and build on this material. As readers, you can continue to evolve the work. You can take pieces of this material, improve it, and please do share it (with attribution) for the rest of us. And, since good reviews are invaluable to help a book be found by potential readers, please review it on Amazon and/or your preferred social media outlet.

The journey of this book doesn't end with publication, it begins. I will be doing more in the coming months and years to connect us. For now, here's how we can connect.

Connect with me on LinkedIn: www.linkedin.com/in/dan-blum-author-architect/

Join the LinkedIn Security Architecture Group: www.linkedin.com/groups/3394596/

Follow me on Twitter: Daniel Blum @RationalCybrSec

Subscribe to the Security-Architect.com blog

Check the links included in the book

https://security-architect.com/SuccessPlanWorksheet

https://security-architect.com/RiskManagementResources

https://security-architect.com/IAMResources

https://security-architect.com/SecurityAssessmentResources

Glossary of Terms and Acronyms

This glossary defines many terms and acronyms used in the text of *Rational Cybersecurity for Business*. It organizes terms and acronyms into three groups and alphabetizes them within each group:

- Security concepts
- Tools and technical capabilities
- Governance or process capabilities

Security Concepts

Accountability-based controls: Controls that promote a sense of accountability in users by heightening awareness or motivation to comply with business policies and create a deterrent effect against violating policies by imparting the sense that monitoring systems are in place to catch abuse. These kinds of controls are considered beneficial because they enable the business to allow users a broader set of capabilities than would otherwise be advisable.

Critical systems (or assets): Systems identified in a business impact analysis (BIA) or well known to the business as being of high value due to their revenue-producing nature or the dependence that other systems have on them.

Cyber-resilience: The ability to detect, respond, and recover quickly from cyberattacks or outages.

DevSecOps: The integration and orchestration of security tests or checks into the software release pipeline from development to production.

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8

Digital: The use of electronic information technology for personal or business activities, interactions, and processes.

Digital business: A business that relies heavily on digital capabilities to generate value and exchange goods or services with customers, suppliers, and trading partners.

Digitalization: The process of becoming a digital business. See Chapter 1, section "Risk and the Digital Business," for more discussion on digitalization, the digital business, security, and risk.

Restrictive controls: Controls that restrict users from accessing or using information or systems that haven't been pre-approved by management in advance. These controls are considered beneficial because, provided they operate correctly, users cannot violate or abuse management policies.

Risk: The probable frequency and probable impact of loss events.

Risk management: The process of identifying, analyzing, evaluating, treating, monitoring, and communicating information about risk scenarios. Risk treatment can include accepting, avoiding, mitigating, or transferring risks.

Security pressure: The level of risk that a business has due to threat actor interest, regulations, public scrutiny, and other circumstances. See Chapter 1, section "Security Pressure," for more definition.

Single sign-on (SSO): The ability to log in, or authenticate, to a system or a domain (aka "identity provider"), and thereby also be authenticated to other systems.

Threats: Individuals, organizations, or forces of nature that could exploit a vulnerability of an asset to create loss events for a business.

Vulnerability (FAIR): Per FAIR, vulnerability is the probability that an asset will be unable to resist the actions of a threat agent.

Vulnerability (common security industry usage): A defect, such as a software bug, in software or hardware.

Zero trust: A security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

Tools and Technical Capabilities

Anti-malware sandbox: An isolated computing environment that executes unknown applications, prevents them from compromising the target system, and monitors the applications to determine if they are malicious.

Cloud access security broker (CASB): An on-premises appliance or cloud-based security policy enforcement point that monitors, mediates, or controls communications between cloud service consumers and cloud service providers as cloud-based resources are accessed.

Cloud service provider (CSP): An IT service provided to customers from a vendor's Internet data center, generally using a pay-as-you-go billing model. It includes SaaS, PaaS, and IaaS service delivery models.

Data loss (or leakage) prevention (DLP): Security policies, tools, and procedures to monitor or prevent unauthorized transfer of information from a business-controlled environment to unauthorized persons or destinations.

Database activity monitoring (DAM): A security technology operating independently of the database management system to provide database monitoring, auditing, and real-time protection.

Infrastructure-as-a-service (IaaS): A category of cloud computing service that provides the hardware, computing, network, and storage platform enabling customers to use virtualized computing resources over the Internet.

Identity governance and administration (IGA): A core IAM component, usually provided through a software suite. It enables policy-based user identity administration, account provisioning, role model management, role administration, and access certification. It includes workflow capabilities and (in some cases) access analytics.

IT service management (ITSM): Tools or approaches to enable the design, planning, delivery, operations, and control of IT services and systems. Often equated with the Information Technology Infrastructure Library (ITIL) framework. Leading ITSM tools are marketing as suites incorporating a workflow management system, configuration management database (CMDB), change management, incident management, and other modules.

Network traffic analysis (NTA): Tools or solutions that enable security and network administrations to collect and analyze network flow data to detect security threats, potentially in near real time. They may include full packet capture capabilities enabling detection of malicious or policy-violating activities after the fact.

Platform-as-a-service (PaaS): A category of cloud computing services that provides an application and OS compute platform enabling customers to develop, run, and manage applications without the complexity of building and maintaining computer OS infrastructure.

Privacy-Enhancing Controls: Tools or techniques that inherently reduce the individuals' loss of privacy through their interaction with the business; these include tokenization of personal data items such as national identifier numbers, the use of private pairwise identifiers in federated identity relationships between providers, minimization of stored personal data in business respositories, and other controls.

Privileged access (or account) management (PAM): A tool or approach for managing and auditing accounts, permissions, and administrative actions by privileged user or services.

Privileged Users: Users, such as cloud subscription managers, system administrators, or database administrators that have the power to define the access rules for themselves and others within an IT environment.

Security information and event management (SIEM): Tools that collect security notifications and log events for the purpose of notifying security operations teams about abnormal or suspicious activity. SIEM systems also provide real-time analysis of security alerts generated by applications and network hardware.

Software-as-a-service: A software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted by a CSP.

User entity behavior analytics (UEBA): A category of security tools that use machine learning to build a baseline model of how users and services in an IT environment normally behave and detect and prevent (or alert on) abnormal behavior.

Vendor relationships management (VRM): Tools or processes used within Procurement, or third party management to track vendor risks, relationships, contracts, and other information.

Zero-knowledge proofs: A zero-knowledge proof is a cryptographic technique or protocol through which one party can prove to another party (the verifier) that they know a value X, without conveying any information apart from the fact that they know the value X. Zero-knowledge proofs can be used as a privacy-enhancing technology to minimize the need to share personal information.

Governance or Process Capabilities

Access control: A technique that regulates who or what can view or use IT resources. Physical access control limits access to physical IT assets or facilities. Logical access control limits access to networks, files, and data.

Access governance: Access governance is the process of managing access controls and the policies or processes through which access controls are managed (i.e., managing the roles in role-based access control).

Agile risk management: A risk management methodology aligned with FAIR and developed by Security Architects Partners that includes models and processes for tiered risk assessment and risk treatment.

Business continuity/disaster recovery (BC/DR): A set of processes and techniques used to help an organization recover from a disaster and continue or resume routine business operations.

Business impact analysis (BIA): A process to identify critical business operations and critical business assets and to identify the potential effects of their interruption or non-availability. Performing a BIA is the first step to developing BC/DR plans for a business.

Business rules: Business rules define or constrain some aspect of business and always resolve to either true or false. They can assert business structure or control the governance and behavior of security-related tools and processes, such as access governance by an IGA system.

Chief Risk Officer (CRO): A position most often found in financial services companies. The occupant is responsible for assessing and mitigating significant competitive, regulatory, and technological risks to a firm's capital and earnings. Organizations that establish the CRO role typically put it at the head of an ERM program.

Chief Information Security Officer (CISO): The senior-level executive within an organization responsible for establishing and maintaining the enterprise security vision, strategy, and program.

Computer Security Incident Response Team (CSIRT): A team of one or more persons responsible for coordinating and supporting the response to a computer security event or incident.

CXO: An abbreviation for a corporate executive at the “C-level” whose job title starts with "Chief" and often ends with "Officer."

Cybersecurity (Oxford dictionary definition): The state of being protected against the criminal or unauthorized use of electronic data or the measures taken to achieve this.

Data governance: A collection of practices and processes to oversee or manage the valuation, classification, ownership, stewardship, and protection of information assets within an organization.

Data owner: An organizational role typically occupied by business leaders or teams that “own” (produce, market, and use) an information asset. Accountable for defining the policies required to maintain the business value and compliance required of the asset.

Data steward: An organizational role typically occupied by IT or business administration professionals. Responsible for maintaining the business value and compliance required by the policies or regulations covering the asset.

Enterprise architecture: The organizational role or team responsible for conducting enterprise-level analysis, design, and planning as well as overseeing implementation of the business’s IT strategy. Also consulted on the development of the IT strategy.

Enterprise risk management (ERM): The methods and processes used by organizations to manage the business risk universe (e.g., financial, operational, market) as well as to seize opportunities related to the achievement of their objectives.

Factor Analysis of Information Risk (FAIR): A taxonomy (or model) of the factors that contribute to risk and how they affect each other and a method of quantitative risk analysis using the FAIR model.

General Data Protection Regulation (GDPR): A European Union (EU) law on data protection and privacy that gives control to individuals over their personal data and simplifies the regulatory environment for international business by unifying privacy regulation requirements within the EU. GDPR also addresses the transfer of personal data outside the EU and European Economic Areas.

Identity and access management (IAM): The technologies and processes to manage digital identity information for people, devices, services, and things (subjects). It also covers subject authentication and the use of identity information for authorization or access control as well as auditing identity administration or access events.

Line of business (LOB): A business unit, or part, of an organization that provides a product or service on behalf of the organization, for example, financing LOB at an automotive company, brokerage LOB at a bank.

Lightweight risk assessment (LRA): The name for a quick risk assessment in the ARM methodology. An LRA can calculate a risk scenario's order of magnitude to determine whether a business or IT team's local risk adviser can sign off on risk treatment (for lower risks) or whether the risk has to be escalated to a business unit executive and/or the centralized risk team.

Responsible, Accountable, Consulted, Informed (RACI) Matrix: Describes the form of participation by various roles in performing a project or business process. The Responsible role does the work to complete the task. The Accountable role may approve the work and is answerable to higher authorities, such as the public, for the result. Persons in the Consulted role provide subject matter expertise, guidance, or opinion supporting the work. Persons in the Informed role are kept up to date on progress but not asked for input.

Risk owner: The individual who is accountable for ensuring the risk is managed appropriately.

Roles: An organizational designation for a set of responsibilities or authorities to perform tasks or work within a business process.

Secure (or software or systems) development lifecycle (SDLC): The definition of distinct work phases which are used by systems, software, or security engineers to plan, design, build, test, and deliver information systems.

Stakeholder: A leader or key member of a group without whose support a project or business process would cease to exist.

Index

A

B

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8

C

D

E

F

G

H

I, J

K

L

M

N

O

P

Q

R

S

T

U

V

W, X, Y, Z