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?

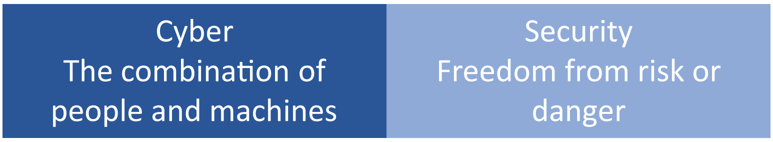

Cyber
The combination of people and machines
Security
Freedom from risk or danger

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/

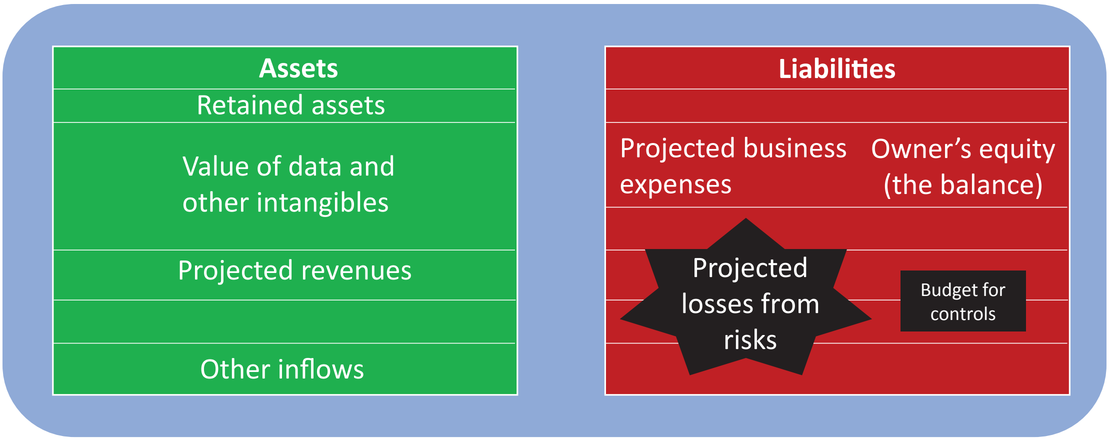

Assets
Retained assets
Value of data and other intangibles
Projected revenues
Other inflows
Liabilities
Projected business expenses
Owner's equity (the balance)
Projected losses from risks
Budget for controls

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)

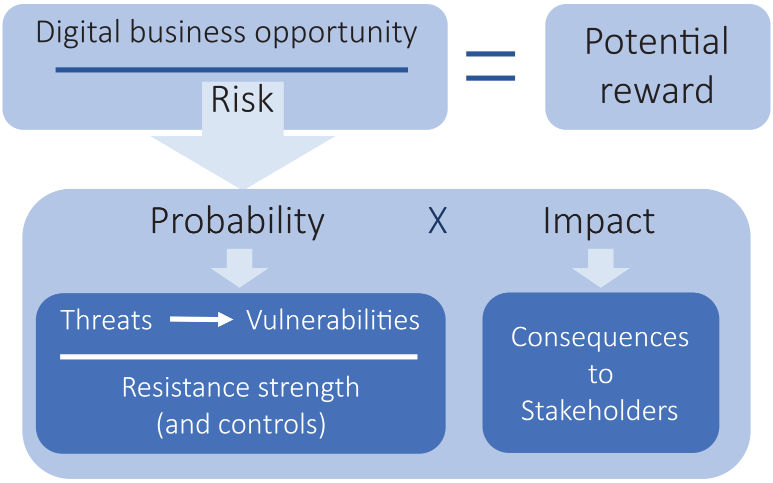

Digital business opportunity
Risk
=
Potential reward
Probability
X
Impact
Threats
Vulnerabilities
Resistance strength (and controls)
Consequences to Stakeholders

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.

Business Alignment

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.

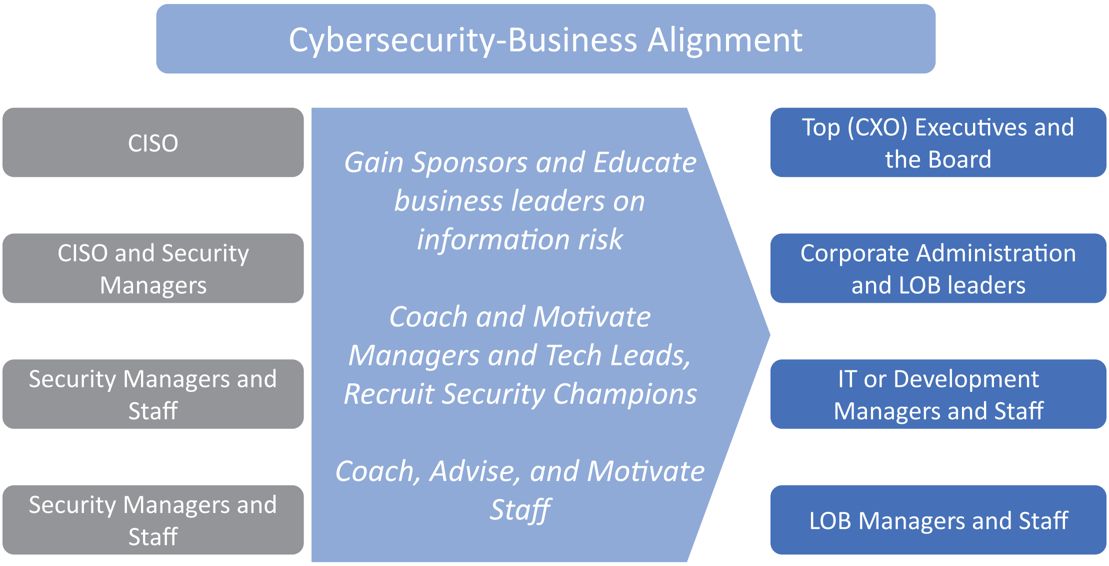

Cybersecurity-Business Alignment
CISO
CISO and Security Managers
Security Managers and Staff
Security Managers and Staff
Gain Sponsors and Educate business leaders on information risk
Coach and Motivate Managers and Tech Leads, Recruit Security Champions
Coach, Advise, and Motivate Staff
Top (CXO) Executives and the Board
Corporate Administration and LOB leaders
IT or Development Managers and Staff
LOB Managers and Staff

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.

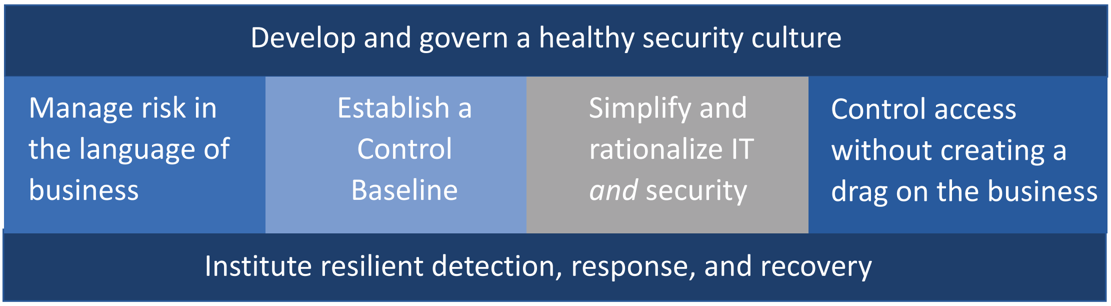

Develop and govern a healthy security culture
Manage risk in the language of business
Establish a Control Baseline
Simplify and rationalize IT *and* security
Control access without creating a drag on the business
Institute resilient detection, response, and recovery

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.

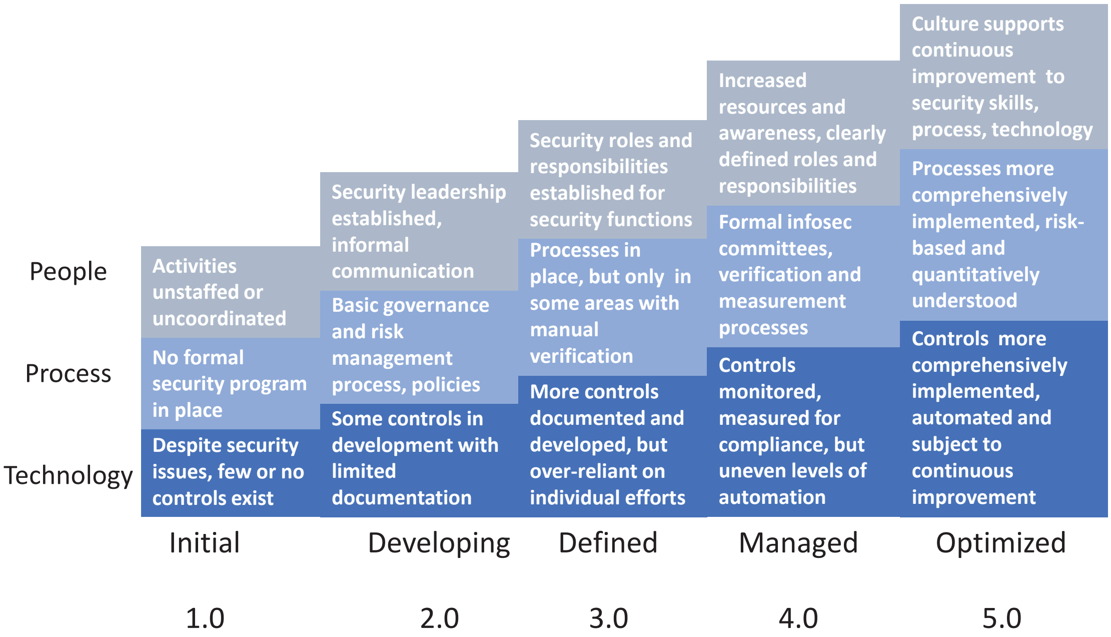
1.4.5 Maturity

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/



	Initial 1.0	Developing 2.0	Defined 3.0	Managed 4.0	Optimized 5.0
People	Activities unstaffed or uncoordinated	Security leadership established, informal communication	Security roles and responsibilities established for security functions	Increased resources and awareness, clearly defined roles and responsibilities	Culture supports continuous improvement to security skills, process, technology
Process	No formal security program in place	Basic governance and risk management process, policies	Processes in place, but only in some areas with manual verification	Formal infosec committees, verification and measurement processes	Processes more comprehensively implemented, risk-based and quantitatively understood
Technology	Despite security issues, few or no controls exist	Some controls in development with limited documentation	More controls documented and developed, but over-reliant on individual efforts	Controls monitored, measured for compliance, but uneven levels of automation	Controls more comprehensively implemented, automated and subject to continuous improvement

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