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.
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.
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.”

---

**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 |
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:

• “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.”
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](http://www.gartner.com/smarterwithgartner/keep-your-job-after-a-cyberattack/)
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.\textsuperscript{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.

\textsuperscript{4}“Fortune 500 Faces Major CISO Challenges,” DH Kass, MSSP Alert, October 2019, accessed at www.msspalert.com/cybersecurity-talent/fortune-500-ciso-challenges/
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 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”, 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”, 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 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](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
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” 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](http://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/](http://www.nominet.uk/boardroom-battle-for-cyber-supremacy/).
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 turnover – businesses need an active hiring program. Some recommendations for effective turnover 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), burnout 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\textsuperscript{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.

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


| Management Practice | Board of Directors Executives | Corporate Executives | Chief Digital Officer | LOB Executives | Chief Risk Officer | CIO | CISO | Human Resources (HR) | Compliance and Audit | Security Management | EA/ARB | CTO/Dev | IT Ops | IT Service Manager | Incident Response | Security Manager | 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 | I |
| Manage security program | C | C | C | R | A | C | R | I | I | I | I | I | C | C |
| Manage security operations | I | I | C | A | C | R | I | C | R | 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.

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 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”

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\textsuperscript{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.

\textsuperscript{15}\url{https://security-architect.com/SuccessPlanWorksheet}
CHAPTER 2  IDENTIFY AND ALIGN SECURITY-RELATED ROLES

Open Access  This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.