CHAPTER 10

The 21st Century CISO

Leadership is the art of mobilizing others to want to struggle for shared aspirations.

—Jim Kouzes and Barry Posner,
The Leadership Challenge

The finance director sounded frustrated and exhausted. Our IT auditors had been trying to tell her about an obscure yet important data backup problem that affected SOX compliance. But her background was in accounting, not technology, and as the IT experts presented page after page of technical information elaborating the intricacies of backup processes, her eyes glazed over. The more they tried to explain by adding yet another layer of detail, the more confused and frustrated she became.

That's when I thought of a solution. "Imagine," I said, "we've got a passenger train running from station A to station B. That's what our backups are like; they're carrying data from our servers to tape."

"We know the train arrived at station B, so we know the backup occurred," I said. "But we don't know how many passengers got on at station A, and we don't know how many got off at station B. So we can't definitively say we actually backed up all the information, and to comply with SOX, we need to be certain."

The finance director sat up. For the first time since the start of the presentation, she seemed alert and engaged. And from that point on, we made progress. She asked how we planned to solve the problem, we briefly mentioned a couple of the possible solutions, and the meeting ended on an upbeat note.

My storytelling, using an off-the-cuff metaphor, succeeded where the more traditional approach had failed. It communicated a technical security issue in terms that a senior businessperson could understand and remember. And it illustrates one of the key skills of the 21st century CISO. We need to extend our reach outside the security organization to communicate with and influence people at all levels, from all backgrounds.

Chief Trust Officer

In this chapter, I'll explain some of the skills and traits I believe CISOs need in order to fulfill their changing role. To set the stage, I'd like to step back for a moment and briefly recap the changing focus of information security overall.

M.W. Harkins, *Managing Risk and Information Security*,
DOI 10.1007/978-1-4842-1455-8_10

As I've discussed earlier in the book, every company is becoming a technology company. And as the potential impact of information risk expands, it is becoming essential to manage security and privacy as a corporate social responsibility. The CISO's role should therefore expand to span the full breadth of information-related risks, as described in Chapter 1. At many organizations, this is already happening. CISOs are taking on responsibility for privacy, regulatory compliance, and product and service security, in addition to more traditional IT security functions.

This is a huge opportunity for CISOs to step into a more valuable, high-profile role within the organization. The core skills of information security professionals—evaluating and mitigating risk—are as essential for mitigating new risks associated with product security, privacy, and regulatory compliance as they are for more traditional IT-related threats. But perhaps this broader role requires a different title that more accurately reflects the convergence of risk responsibilities, such as Chief Trust Officer or Chief Information Risk Officer.

Taking on a larger role requires a broader view and a corresponding set of skills. We need to communicate in terms that business people understand, and build relationships that enable us to influence people at all levels across the organization. We also need extensive management and leadership skills, both to operate at an executive level and to inspire our expanded risk and security team.

The ability to manage the full range of information-related risks is a necessity, not just for the CISO, but for the organization. If we do not step into a broader role, the organization must acquire these abilities elsewhere. Because of this, CISOs who do not adapt to this role run the risk of becoming irrelevant to the organization. Alternatively, these risk areas will be managed in a stove-piped, fragmented way, in which case the organization may never discuss the aggregation of risks and the controls necessary to manage them. If this occurs, organizations will certainly generate unmanaged risks to themselves, their customers, and to society.

Until recently, one of the CISO's biggest challenges was obtaining funding for security initiatives. Today, due to the prevalence of large breaches, it's often easier to find funding. But more funding doesn't always lead to greater security or a better outcome for the organization. Sometimes the fear of breaches drives organizations to invest heavily in controls that generate a high degree of control friction, restricting users' ability to do their jobs. For example, some organizations have installed controls that prevent users from downloading apps or files, or even accessing some web sites. These controls threaten to stifle users' ability to innovate and hinder overall business velocity. Furthermore, determined users will find ways around the controls, such as using less-secure personal systems to access "forbidden" resources.

CISOs need business acumen to understand the impact of security controls on others in the organization. As I discussed earlier in the book, our approach to security architecture should start with an understanding of the 9 Box of Controls, including the friction that controls can generate. Business acumen is also necessary to communicate technical risks in language that nontechnical people in the business can grasp, and to understand that some risks are worth taking. Risk-taking is fundamental to business. Without it, no business value would be created.

The Z-Shaped Individual

If we don't already have the skills required of the 21st century CISO, we need to acquire them.

To some extent, this trend parallels what is happening in most technology-related professions: IT professionals need to acquire business acumen as well as depth of IT knowledge. The concept of "T-shaped" individuals has been widely used to describe the idea that IT professionals need to be able to provide value horizontally, across business groups in the organization, as well as vertically at all levels within IT.

This concept is useful, but it doesn't fully encompass the skills of the 21st century CISO. The unique role of CISOs and other security professionals might be better represented as a "Z-shaped" individual, as shown in Figure 10-1. Adding the third dimension of core security skills, such as risk assessment and understanding of controls, allows us to deliver value across the business and all areas of IT.

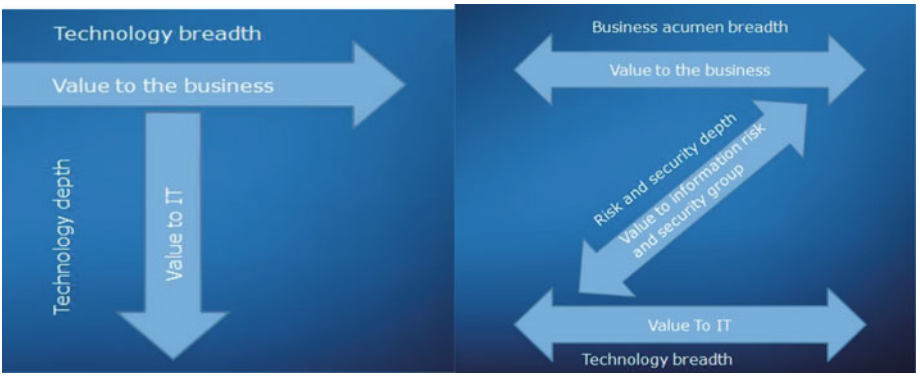

Figure 10-1. *The T-Shaped IT professional (left) and the Z-shaped CISO (right)*

The 21st century CISO needs to understand business priorities and processes well enough to identify how security controls help or constrain the business. To gain this level of understanding, he or she has probably gained experience in areas that are central to the company's business, which, of course, vary depending on the company's core focus. For example, the CISO might previously have worked in manufacturing operations, services, or mergers and acquisitions.

The CISO needs technical knowledge too, although the depth of technical knowledge required remains a subject of intense debate among my peers. I've observed CISOs at smaller and less-complex organizations who feel they need deeper technical skills to do their jobs. This is not surprising. With much smaller security teams, CISOs at smaller companies may need to be more involved in day-to-day technical details as well as managing people. At larger and more complex organizations, CISOs are less likely to spend time delving into technical detail.

However, all CISOs need to be able to understand enough about the technology to absorb the important issues and communicate these issues to other managers outside the security group. This means that our technical knowledge must be broad, ranging from devices to data centers. We need to know enough about devices, such as smartphones, PCs, tablets, and new evolving device types such as wearables, to understand the security implications as well as the benefits. At the other end of the scale, we need to know enough about data centers and physical access controls to understand and communicate the important security requirements and challenges.

Our core risk management and security skills provide the link that completes the "Z" by connecting technology and business. We understand how to assess and manage risk by applying procedural, technical, and physical controls to meet the organization's legal, privacy, and security requirements.

Foundational Skills

Becoming a Z-shaped individual is the foundation for one of the 21st century CISO's essential traits: establishing credibility across the organization. We must be credible in order to build trusted relationships with executives and specialists across the organization and to discuss the vast range of issues that affect the business. This credibility is built on the competence that comes from understanding the business and technology as well as possessing core security skills. By becoming Z–shaped, we will also be better positioned to influence risk management for the company's product and service strategy, as opposed to having those risks managed independently by another group.

Our ability to influence the organization also springs from a clear mission. I use the term *centered* to describe this. We can effectively present our case because we have a strong sense of purpose and a clear understanding of why the security group exists and what we are trying to achieve.

This idea returns us to the theme of this book: Protect to Enable. In our global economy, most companies operate in highly competitive markets. As the security organization, our mission is to enable the free flow of information and rapid implementation of new capabilities to ensure success and long-term competitive survival. Other CISOs may work at more risk-averse organizations, and therefore some aspects of their mission may differ. However, the mission always needs to be aligned with the organization's business priorities. It is essential that this mission becomes a part of who we are and why we exist. It provides a sense of purpose that lends authenticity and consistency to our actions and helps us build credibility across the organization.

As we all know, security can be a particularly distracting profession, with a constant barrage of day-to-day emergencies and diversions. So we need a clear mission in order to retain a strong sense of direction. Like expert sailors, we can progress toward our goal amid the day-to-day distractions and diversions, making continual adjustments and corrections to stay on course as the winds shift.

We also need to retain a sense of curiosity. To engage with others, we need to be genuinely interested in what they do. This curiosity enables us to continue to learn, building on and broadening the competencies that then enhance our credibility.

Another major reason we need to be learners is to stay ahead of the enemy. Threat agents are always learning because they must. As new threats emerge, we put in place new controls. But once implemented, these controls tend to be static, while threat agents

are dynamic, coming up with new techniques to bypass the controls. Therefore, our thinking must also be dynamic, and we must continually learn in order to protect against ever-evolving threats.

Becoming a Storyteller

We cannot influence people unless we communicate with them. And as the scope of information risk expands, we need to communicate with a wider range of people across the organization.

Communicating with people isn't always easy, as most of us have discovered. If we start relaying technology details to those who aren't technologists, we won't capture their interest. In fact, we run the risk of doing the opposite, as I described in the example at the start of this chapter.

To communicate, CISOs must become chameleon-like, with the ability to blend into a variety of environments. We need enough knowledge of each business domain to be able to communicate with different groups using language they understand. And we need to discuss these subjects at different levels. A CFO may only want to hear a high-level summary expressed in terms of financial impact and return, which is often not easy when discussing security investments targeting hard-to-quantify threats. Product group managers want to hear security issues expressed in terms that relate to sales, marketing, and operational efficiency.

I've found storytelling to be a powerful tool for communicating with diverse people across the organization. When I frame security issues as stories and images that people can understand, they relate better to the issues even if they lack a background in technology.

I like to tell stories using metaphors and analogies. They are easily remembered, and they translate complex subjects into simple terms everyone can understand. In fact, the metaphors I've used throughout this book, such as the perfect storm in Chapter 1, the train backup in this chapter, and the roundabouts and traffic lights in Chapter 5, have helped me communicate security issues to many people. To use yet another analogy, orchestra conductor Benjamin Zander said, "The conductor of the orchestra doesn't make a sound. His power comes from awakening possibility in others." (Zander and Zander 2000). In the same way, I believe the power of the CISO comes from awakening the awareness of risk among people across the organization. I use stories based on metaphors to create that awareness.

For example, employees often find it hard to understand the dangers of stealthy threats. This is because the threats are unobtrusive, concealing themselves so they can steal information over the long term. Users are usually not even aware that a problem exists on their system. They still associate malware with obvious, annoying symptoms such as screen messages and system crashes. So when we tell them we've detected dangerous software on their machine, they have a hard time believing that it matters. That is why we have to focus on prevention using low-friction controls. If we do not achieve this as a profession, we will perpetuate the worsening cycle of risk we are experiencing today.

To communicate the danger, and the need for effective preventative controls, I sometimes use the analogy of ants and termites. "Malware used to be like food-eating ants in the kitchen," I explain. "You'd know when you had an infestation because you'd see ants crawling over the countertops and walls. Once you knew about them, you'd spray or set traps to eliminate them.

"But today, threats are more like the termites that can live in your walls. You can't see them, and you may not even know they are there. But they're doing much more damage than ants ever did. In fact, they may be destroying the structural integrity of your house."

I've found using analogies helps quickly drive home messages. People immediately understand that these invisible threats can undermine the structure of the computing environment, just as termites undermine houses. This makes them more likely to accept the next step, which is that we have to perform the digital equivalent of tenting their computer to eradicate the vermin, but without toxicity to users or the computing environment.

THE NIST FRAMEWORK: A COMMON LANGUAGE FOR RISK MANAGEMENT

To discuss information risk management across the organization, it's helpful to use a common language that everyone, including non-technical people, can understand. I've found the National Institute of Standards and Technology (NIST) Cybersecurity Framework to be a helpful tool for communicating the issues. Development of the framework was triggered by a 2013 presidential executive order on improving the security of critical infrastructure. This led to a year-long private-sector–led effort to develop a voluntary how-to guide for organizations. Many companies contributed input about standards, best practices, and guidelines to that effort. I was one of the first security leaders among the Fortune 500 companies to engage the framework.

The framework creates a common taxonomy and terminology for managing risk, making it easier for security teams and others to communicate. It fosters collaboration. In addition, each organization can measure its risk management maturity level against the framework. As the framework is used by more people, including business executives, it may help to increase the overall understanding of information risk and how to manage it, which would be a good thing for all organizations.

Fear Is Junk Food

Just as building trusted relationships is essential to influencing the organization, I also think we need to transcend the doom-and-gloom that can pervade discussions of security topics.

The security industry has a tendency to use fear to sell products. Unfortunately, this tendency reflects the fact that many people in the security industry profit from insecurity: their revenue grows when more breaches and other incidents occur. Internally, as security professionals, we sometimes share this tendency to use fear as a tool to obtain additional budget or other resources. Of course, security really is about scary things: threats, vulnerabilities, and risk. But focusing on fear as the primary motivator is like living on a diet of junk food. It may provide immediate gratification, and it's somewhat addictive, but ultimately it's not healthy for either the CISO or the rest of the organization.

In the short term, fear can scare people into action and help drive funding for security projects. However, relying on fear alone can only work for so long. Eventually, it has the opposite effect. It causes the CISO to lose credibility. In fact, I think relying on fear may even contribute to the high rate of job turnover among CISOs. Those who rely too much on selling fear are snacking on an unhealthy diet, and eventually the organization realizes this and rejects them.

Ultimately, fear doesn't work for other reasons too. Most people don't want to listen to a continuous stream of negativity. If we are always seen as the source of negativity, we will lose our audience. If we are continually viewed as the group that says no, we will be ignored. People will bypass security restrictions in order to meet their business needs.

Even within the security organization, fear can become a gravitational force, a black hole drawing ever-increasing attention to the negative side of security issues and draining energy that should be directed to enabling the business. This is why we need to focus on solutions that deliver the three key benefits I discussed earlier in the book: a demonstrable and sustainable bend in the curve of risk; the ability to lower the total cost of controls; and low control friction to improve business velocity and the user experience.

Accentuating the Positive

So how do we take a more positive approach? By focusing on our mission, which is to Protect to Enable. This mission shifts the emphasis from the negative to the positive: how we can help the business achieve its goals by solving these information risk and security problems. It puts hope and optimism before the challenge.

This mission is aligned with the business. Rather than being antagonistic, it is based on common values. It sets an optimistic tone, and, in the long term, optimism is a far better motivator than pessimism. Threats may be frightening, but our goal is to see past the threats and identify the opportunities. To paraphrase the noted Stanford University behavioral scientist Chip Heath, there's no problem that cannot be solved without a new framework. Therefore, if we can't see a solution, we have the wrong framework. Protect to Enable provides a new framework. So does the 9 Box of Controls, with its focus on cost efficiency and control friction as well as effectiveness. These tools help us focus on finding solutions.

Imagine you're invited to attend a meeting to discuss whether the company should start using a specific cloud-based business application from a new supplier. Clearly, this product introduces risks: it comes from an unfamiliar supplier, it's accessed over the Internet, and it means sensitive data will be stored outside the enterprise.

A narrow security view might focus solely on minimizing the risk. However, this narrow view can lead to a Catch-22 situation, as discussed in Clayton Christensen's book *The Innovator's Dilemma* (Harvard Business School Press 1997). Typically, it goes something like this. To minimize the risk, the organization initially restricts the use of a new technology. For example, the technology can only be used for low-risk data, or by a narrow segment of employees. The problem with this approach is that it also reduces the business benefit to the point that the benefit of the technology cannot justify the expense and effort of adopting it. So we reach an impasse. To make the technology a viable proposition, we need to be able to show a business benefit, but we can't show a business benefit because we won't allow viable use of the technology.

Protect to Enable provides the new framework that frees us from the innovator's dilemma. It allows us to focus on the opportunity and identify benefits that outweigh the risks. For example, introducing a new supplier increases competition for our existing suppliers, leading to future savings for our organization. This benefit aligns with the business and is one that everyone in the organization understands. Perhaps less intuitive, but equally important, the savings can be used to fund security controls to mitigate the risk of using the technology more widely. Now our benefit/risk equation has a positive result rather than a negative one. By enabling the technology to be used more widely, we realize bigger business benefits that outweigh the additional cost of controls. This example also underlines the need for CISOs to build business acumen that enables us to see the opportunity and how it can be used to overcome the challenge of funding security initiatives.

Let's look at another example, this time from my experience at Intel in the days before I had defined our Protect to Enable mission. Several years ago, a highly damaging worm was discovered in our environment, requiring a significant emergency response from our team. Upon investigating, we traced the origin of the worm to an employee's personal system.

Our immediate response was that of a stereotypical security group. We shut down this usage to eliminate the risk of future infections. We immediately tightened security policy to ensure only corporate-owned PCs could access the network, and we ruthlessly went through the environment and cut off access by any devices not managed by IT.

Our response was successful in the sense that it reduced the risk of infection. But it led to other risks we hadn't foreseen. Eliminating personally owned PCs from the network meant we now needed to issue corporate PCs to contract employees. This meant that we had to provide more people with devices that allowed full access to the corporate environment. It also, of course, increased capital costs. The broader impact was that it eliminated the potential business benefits of letting people use their own personal devices for work.

Subsequently—driven largely by employee demand, as well as the massive proliferation of new consumer devices—we revisited this issue. This time, we examined it from the perspective of Protect to Enable. We looked at the business opportunities if we allowed personally owned systems on the network, and then how we could mitigate the risks. As I mentioned in Chapter 1, we rapidly discovered that the business value is enormous. Helping employees communicate and collaborate at any time can drive significant productivity gains. It also helps make employees happy. They love using their personal smartphones, PCs, and tablets, and they appreciate that we enable them to do so.

These benefits easily outweigh the cost of the technology required to reduce the risk of allowing access by personal devices. True, some of this technology wasn't available at the time we experienced the original security problem. But if we had focused on the opportunity first, perhaps we could have found ways to provide some level of access while mitigating the risk, and experienced at least some of the benefits we enjoy today.

Demonstrating the Reality of Risk

Of course, the security organization's role still centers on managing risk, which includes discussing the negative consequences of people's actions. If we frame this discussion carefully, I believe we can inform without fearmongering. By describing possible

outcomes and solutions without using emotional language, in terms listeners can understand, we create a context in which the organization can make the decisions that are best for the business.

Even when we have to highlight unpleasant outcomes, we're not fearmongering if our information is based clearly on reality. Here's another example from my experiences at Intel. As our customers' use of the Internet expanded, Intel's marketing groups naturally wanted to expand their external online presence by creating new web sites. So we, as Intel's information security group, began assessing the risks and the security controls required. Some of our marketing teams didn't find this an appealing prospect. They needed to move quickly, with the freedom to communicate however they thought best, and they viewed security procedures as bureaucracy that slowed them down and hindered their ability to communicate with customers and partners.

What happened next was far more persuasive than any of our initial efforts to forestall potential problems. A few web sites were launched without rigorous quality control. Hackers found the weaknesses in these sites, but they didn't crash the sites or steal information. Instead, they inserted links to porn sites.

When this unfortunate fact was discovered, it provided the leverage we needed to improve security procedures. I realized this was a case where a picture spoke a thousand words. So, to illustrate the impact, I simply showed the links to people within the company. This wasn't fearmongering. It was simply demonstrating the real consequences of their actions on the brand. Everyone could understand the implied question: Do we want our brand to look like this? This ended, once and for all, any discussion about whether we needed to apply rigorous quality control to external web sites.

The CISO's Sixth Sense

In the book *Blink: The Power of Thinking Without Thinking*, author Malcolm Gladwell (Little, Brown & Co. 2005) describes an interesting experiment. Researchers asked subjects to play a game in which they could maximize their winnings by turning over cards from either of two decks. What the subjects didn't know was that the decks were subtly stacked. They could win by selecting from one of the decks, but selecting from the other deck would ultimately lead to disaster. After about 80 cards, the subjects could explain the difference between the decks. But they had a hunch something was wrong much sooner, after only 50 cards. And they began showing signs of stress and changing their behavior even sooner, after only about 10 cards, long before they cognitively understood a difference existed.

As CISOs, we develop a sixth sense about security issues. Often, my instincts suggest a need to act or begin investigating a specific direction long before our group is able to fully understand or explain what is happening. This sixth sense is particularly relevant in the security realm, where our information is almost always imperfect or incomplete. When a threat strikes, we do not have time to conduct extensive research or wait for evidence to accumulate. Therefore, we need to act decisively based on imperfect information.

I think we develop this sixth sense from the diverse experiences and skills we've acquired during our careers. We can also foster this sixth sense by being aware. Some security professionals tend to be inwardly focused, looking only at the data and systems they need to protect. As described in Chapter 4, I have directed my teams to try to be

more open and outward-looking, sharing information and seeking input from a variety of sources, including peers across our company and at other organizations. This can help CISOs spot early warning signals and correlate information to quickly identify threats. Like secret service agents scanning a crowd, our experience helps us spot anomalies, to see the signals and ignore the noise.

By identifying future risks early, we may be able to prevent them entirely, or at least minimize their impact. We may also reduce the overall effort needed to deal with the risk. Early action may avoid the need for emergency response and a potentially major cleanup effort.

Taking Action at the Speed of Trust

A sixth sense is only of value if the organization can act on it quickly. This requires two things. First, we need the courage to take a leap of faith based on what we believe. This courage is rooted in the attributes I discussed earlier in this chapter, such as being centered and credible, with a clear sense of our mission.

The second requirement is that the organization responds quickly when we inform them about a security issue. This rapid response is only possible if we have established trusted relationships with people across the organization. Because of these relationships, the organization can act at the *Speed of Trust*, as Stephen M. R. Covey describes it in the book of the same name (Free Press 2008). Faster, frictionless decisions are possible because people know, from experience, that our information is reliable and that our focus is on enabling rather than spreading fear.

The CISO as a Leader

Above all, 21st century CISOs must become effective leaders who can inspire their teams to enable and protect the organization

Over the years, I've identified three essential themes I try to instill in my team and constantly reinforce in our day-to-day interactions. Our security team members must believe in our mission; they must feel they belong within the security group and the company as a whole; and they must feel they matter.

If I can make people feel that they believe, they belong, and they matter, they will tackle any challenge. As Kouzes and Posner put it in *The Leadership Challenge* (Kouzes and Posner 2012), "leadership is the art of mobilizing others to want to struggle for shared aspirations." If people understand the greater goal, it helps establish an emotional connection that guides their everyday actions. This is a key reason that I have thought so much about defining the mission, and that I have spent so much time helping the teams I have led to see how their jobs are connected to the business's objectives and concerns.

For example, a typical operational goal might be to patch all systems within a week of a new software release. This goal is more meaningful if we establish the links to the business using the *I believe, I belong, and I matter* mantra: "I believe in the mission of Protect to Enable. If I'm not protecting to enable, the other employees at the organization I belong to cannot do their jobs effectively. The company doesn't achieve its results, and the company doesn't execute its vision. Patching systems quickly matters because it helps our users do their jobs, which in turn helps the business achieve its goals."

Learning from Other Business Leaders

As leaders, we can learn a lot from how other business leaders work. Today, managers are moving away from command-and-control to a more collaborative approach that takes advantage of the diversity of employee ideas and strengths. I'm not talking about a consensus process, which can lead to endless debate and indecision. Rather, a leader's goal is to ensure alignment to a common mission and accelerate decisions. Within this framework, differing viewpoints and debate spark creativity, generating new ideas and a productive tension that can drive results.

Because security can be frustrating, even daunting, it's vital to find ways to help employees stay motivated. It's important to help employees feel they are making progress, not just when they achieve major milestones, but in solving the smaller problems they face every day. A key study found that even small wins boost motivation, productivity, and creativity. In the *Harvard Business Review* article describing the study, authors Teresa Amabile and Steven Kramer (2011) determined that the feeling of making progress is the most important contributor to an employee's emotions, motivations, and perceptions.

Opportunities to lead occur continually, in every interaction with our teams, with other people in IT, and with business partners. The question we need to ask ourselves is whether we are seizing these opportunities to reinforce our mission and ultimately to help the organization achieve success.

In highly technical jobs and organizations, we have a tendency to focus on technical challenges while overlooking the "people factor." I think it's important to remember the need for personal connections, which foster the sense of belonging. When we know a little more about each other, we care more as a result. I think about this in my day-to-day interactions. If a team member is making a presentation, are we paying attention and asking thought-provoking questions, or are we distracted? And if so, do we think they will feel they belong?

When we meet with a team member to discuss their struggles with a project, are we helping them think through the issues and come up with solutions? Are we helping them believe they can overcome the challenges and that the results will matter to the company and to us? Or are we just taking them to task? Each interaction is an opportunity for coaching and helping employees improve their performance.

A final requirement of effective leadership is the ability to develop other leaders within the security group. Otherwise, the group's strengths in managing risk for the business will last only as long as the current CISO's tenure. By building competence in depth, the CISO can ensure that the organization delivers sustained performance over time. We will discuss this in more depth in the next chapter.

Table 10-1 shows research by executive-search firm Korn Ferry suggesting that cybersecurity leaders need a unique set of attributes, including the ability to think outside the box, dig deeply into issues, exercise judgment at board level, and be a credible business partner (Alexander and Cummings 2016).

Table 10-1. *Attributes of Cybersecurity Leaders(Alexander and Cummings 2016)*

Key Attributes for Cybersecurity Executives			
Competence	**Experience**	**Traits**	**Drivers**
Strategic, global thinker (sees big picture)	Depth of technical experience	Learning agile (can adapt to the new and different)	Seeks high visibility and accountability roles
Thinks outside the box	Understands the evolving legal and regulatory environment	Flexible	Strives to be agent of change (not agent of "no")
Analytical (digs deeply into issues)	Has successfully handled security incidents in the past	Tolerance for ambiguity	Must "thread the needle to balance driving change with managing enterprise risk"
Possesses business savvy (understands how information is used in daily operations)		Intellectually curious	Pursues close engagement with business leaders (works to add business value)
Balances competing priorities		Bias for action	
Communicates and influences broadly (board, senior management)			
Attracts, builds, and leverages talent			

Voicing Our Values

Obviously leadership means taking responsibility. Yet some CISOs seem to forget this, at least occasionally. A typical situation goes something like this. The CISO warned of a security issue but couldn't obtain the budget or resources to address it. So the CISO abdicated responsibility because someone else had made the decision not to fund a solution. I take a different view. I believe even if we disagree with the decision, we should do our best to voice our values. We need to articulate the potential impact to the organization, to our customers, and to society, as I discussed in Chapter 9.

As partners in the organization's strategy, we should commit to the decision and share full accountability and responsibility with our peers. Having said that, we also need to clearly express our personal values and stay true to our principles. Adhering to our values may mean taking career risks, as discussed in Chapter 9. Therefore it is critical that we take the time to reflect on what our principles and values really are. This personal

journey, which we all need to take, adds another dimension to the Z-shaped individual, a dimension of values (Figure 10-2). As Mary Gentile, the author of *Giving Voice to Values (2010)*, puts it, "We are more likely to voice our values if we have decided that the costs of not doing so, and the benefits of trying, are important enough to us that we would pursue them even though we cannot be certain of success in advance. In order to get to this place of clarity, we need to spend serious time thinking about our own identity, our personal and professional purpose, and our own definition of success and failure."

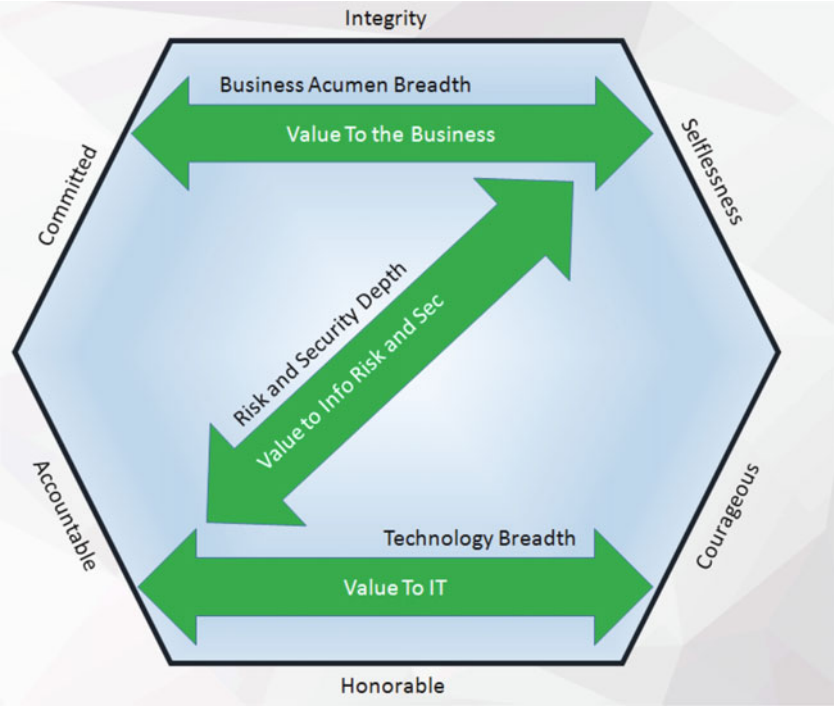

Figure 10-2. *Another dimension of the Z-shaped individual: the personal values that guide our actions*

Discussing Information Risk at Board Level

Clearly, corporate discussions of any topics that have such far-reaching potential impact on society should include participation by the executive board. Board awareness of security has increased somewhat due to the spate of well-publicized breaches. Yet surveys show that the majority of boards are still not aware of major security and privacy issues. A recent study found that only 32% of boards review security and privacy risks, and only 45% have any involvement in security strategy (PWC 2015).

In contrast, a significant number of security professionals believe that the CEO and executive boards are responsible to society for the sometimes disastrous impact of security and privacy issues. In another recent survey, one sixth of security professionals

said they advocate arrest and a prison sentence for the CEO or board members after a breach (Websense 2015). That seems to indicate that they feel their management is not taking the problem seriously enough, or perhaps even chooses to look the other way, and that they are concerned about the broader consequences to society.

Given the broad and ever-growing importance of security and privacy, boards need be much more involved in than they have been in the past. It is the CISO's responsibility to bring important security and privacy issues to the board, and initiate a debate about the potential impacts of those issues and the right response. Even with the current heightened awareness of security issues, it may not be easy to get the board's attention, because board members have so many other business issues to worry about. It can help to hone in on the handful of risks with the largest potential financial impact or other major implications such as damage to the company's brand. Key areas for boards to consider include

- **Security and privacy strategy**: Is it cohesive and complete?
- **The security and privacy leadership**: Do they act with a level of independence? Do they take ownership of issues, or do they simply manage a risk register?
- **Incident response planning and drills**: Do they occur? Are they integrated across the organization?
- **"Tone from the top**:" Is the executive team engaged? Do their actions match their words?
- **Security and privacy governance**: Does it have the appropriate decision-making structure, including the right level of "tension" between different stakeholders? Is it set up to ask the "high contrast" questions (as discussed in Chapter 2)?

The CISO must take responsibility for determining which issues merit the board's attention. That determination will depend on the potential impact of an exploit conducted against the company's internal systems or technology-based products and services.

C-I-S-O ATTRIBUTES

In this chapter, I have covered a range of abilities and characteristics that the 21st century CISO requires. Many of these probably sound familiar, but it's all too easy to forget them amid the demands of hectic daily schedules. I've found a good way to remind myself of some of the key attributes is simply to look at my job title. The letters in CISO help me remember that we all need Character, Intuition, Skills, and Objectivity. So if you're struggling to remember all the details in this chapter, just remember you're a CISO. You need Character to ensure your actions demonstrate integrity; Intuition to anticipate what's needed and act accordingly, taking risks when necessary; Skills that span business, technology, and a wide variety of risk areas; and Objectivity in order to avoid falling prey to fear-mongering.

Conclusion

As the technology environment continues to evolve, many people believe we're moving toward a future in which organizations outsource much of the delivery of IT services. If this trend continues, what does it mean for the CISO?

In this view of the future, the organization shifts away from IT implementation to procurement and management of suppliers and services, while setting direction and establishing an overall IT architecture.

In addition to this, the organization will need to retain the core competency of the security group: the management of information risk. Essentially, organizations cannot outsource risk. We can hire companies to deliver our business systems, but we're still responsible for compliance with regulations that affect our companies, such as SOX and HIPAA. And if a breach results in theft or leakage of personal information or critical intellectual property, we're still responsible for reporting it. Furthermore, we still suffer the damage to our brand, even if the breach was due a failure of the supplier's systems. As regulations proliferate and more and more personal information is stored in business systems, the risks can only increase.

Therefore the CISO's abilities will remain essential, even if the job title changes. The organization must retain the management of information risk as a core competency. As CISOs, we are poised to continue providing that core competency as long as we can effectively work within this new environment by developing the abilities I've described in this chapter and throughout this book. These abilities enable us to work with others to support the Protect to Enable mission.

I'll close this chapter with an excerpt from a speech by Teddy Roosevelt; the sentiments seem as relevant today as when he made the speech back in 1910. "It is not the critic who counts; not the man who points out how the strong man stumbles, or where the doer of deeds could have done them better. The credit belongs to the man who is actually in the arena, whose face is marred by dust and sweat and blood; who strives valiantly; who errs, who comes short again and again, because there is no effort without error and shortcoming; but who does actually strive to do the deeds; who knows great enthusiasms, the great devotions; who spends himself in a worthy cause; who at the best knows in the end the triumph of high achievement, and who at the worst, if he fails, at least fails while daring greatly, so that his place shall never be with those cold and timid souls who neither know victory nor defeat." (Roosevelt 1910)

We need to be in the arena, and so do our teams. Our mission, as information security and privacy professionals, is a worthy cause. With our efforts to prevent harm to our organizations, our customers, and to society, we can ensure that tomorrow is better than today.