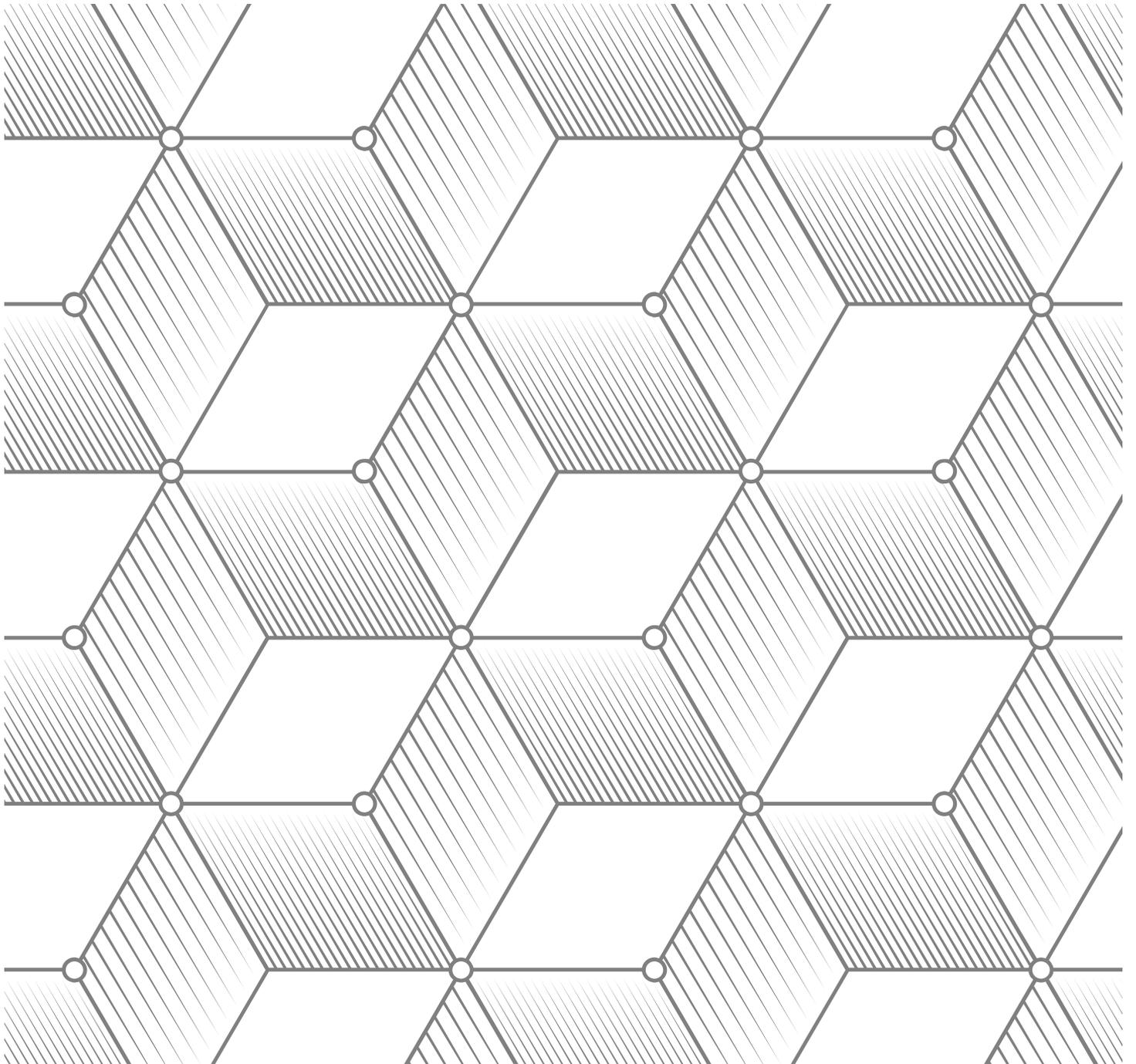


# Blurred Lines

The Evolution of Leadership in  
Information Risk and Cybersecurity



Cyber attacks have emerged as a potential company killer. Cyber threats are more widespread and targeted — and continually evolving. It's not just that the bad guys are getting more “professional” and sophisticated, the very nature of organizations today has opened new fronts of vulnerability. Intrusions occur not just via traditional IT systems and email scams, but also through the ever-growing number of devices and systems connected to a company's network, including shop floor systems, public websites, customer portals and the explosion of data housed in the cloud. The consequences of a security breach can be dire, including regulatory investigations, loss of intellectual property, financial losses from theft or fraudulent transactions and damage to the company's reputation.

As the threats overtake the ability of traditional “castle and moat” defensive approaches, cybersecurity is maturing and, as a result, the profile of the chief information security officer (CISO) role is evolving rapidly. Each company will have a unique set of circumstances influencing its risk profile, yet several macro trends cutting across industries and geographies are spurring shifts in how organizations approach information risk and security:

- From infrastructure to software, as companies increasingly come to rely on third parties for the former (computing, data storage and networks);
- From policy and compliance to hard government connections, as crime increases in sophistication and is available “as a service,” and nation-states fund and direct asymmetric warfare against the private sector of foreign countries;
- From a focus on “securing the perimeter” to securing the data assets themselves as they move in and out of a company's purview;
- From a “black-and-white,” binary, unsecured or secured approach, to one of a sliding scale of security protections and data accessibility depending on data sensitivity and transactional requirements;
- From an inward, corporate focus to client- and “product”-centricity; and
- From a cultural orientation favoring order and safety toward one that prioritizes learning, collaboration and results.

This evolution has important implications for the kinds of information security leaders that organizations need, where they should look for these leaders, how they should assess executives, especially when a lateral hire is required at the top, and how they should develop the leaders of tomorrow from the company's existing talent base. We have observed that the most progressive and successful organizations tend to do the following as they mature in the area of information risk and security:

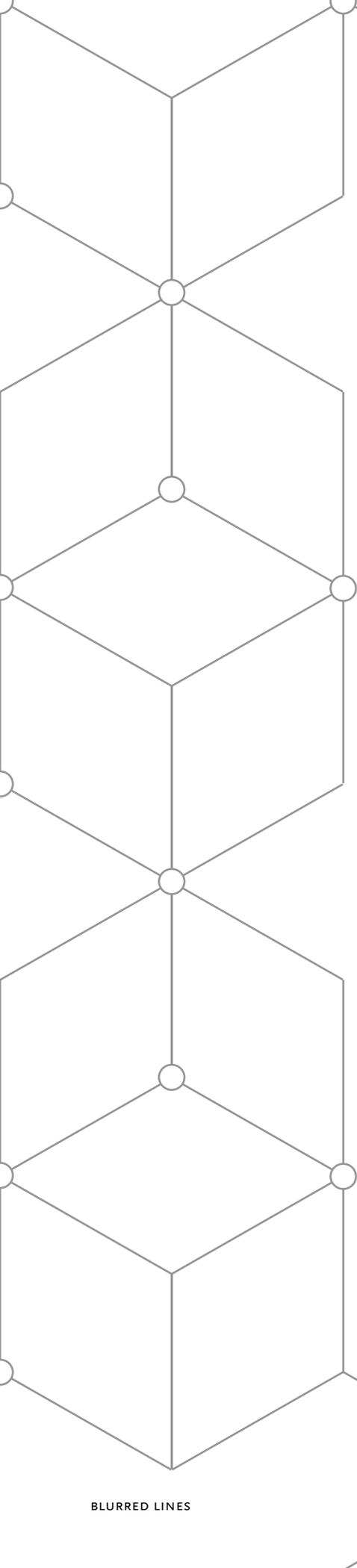
**Leverage analytics and automation to help predict, detect and mitigate risk.**

More mature security organizations are investing in analytics capabilities, artificial intelligence (A.I.) and other automated, intelligent systems to help guide security planning and response. "The single biggest thing we did was create a dedicated threat and vulnerability analytics team whose job it is to understand, both in the moment and over time, how threats and vulnerabilities are unfolding, which help define both how roles are evolving and what we need to be doing strategically for the next couple of years," said Lou Steinberg, chief technology officer for TD Ameritrade. Furthermore, better automation will be important to help offset the security talent shortage over the next several years, according to General (Ret.) Keith Alexander, CEO, IronNet Cybersecurity and former director of the U.S. National Security Agency (NSA). "We'll have a human capital deficiency in this area for the next three to five years. Small and mid-sized companies will have trouble getting IT security people, so we'll need more automation."

**Create an organizational culture where information security is everybody's business.**

Even a few years ago, information security was regarded as a back office function in many organizations. That's changed dramatically as companies come to realize that secure software can be a competitive advantage, and that the "ROI" of investing in reputational risk mitigation can be compelling. "Everybody realizes that building trust with clients is not a free lunch. It will cost something to have the increased security," said Barclays chief security officer, Troels Oerting. This recognition has changed the relationship between security and other functions, increasing collaboration on important initiatives. So, no longer is the security review the last stop before a product launch; security is embedded in the development team. "Now we do this development together and build in security by design at the very beginning."

*"Risk professionals in financial services are accountable to the board, whether they report to the CFO or CIO."*



**Assemble diverse, focused security teams with a problem-solving orientation.**

Cyber threats are evolving so quickly that teams that include only people with deep IT security experience can be at a marked disadvantage, as they are more likely to rely on tactics that have worked in the past, even as vulnerabilities and threats change. Facebook, for example, looks for a range of subject matter experts from “the business” who may have an interest in security, and then trains them in the discipline. This increases the intellectual diversity of security teams, as well as their gender and racial diversity. “We build teams with people from engineering, people with investigative backgrounds, people who are subject matter experts, whether it’s fraud or child safety or terrorism, and together they try to break down the problem so that we can leverage a small number of people guiding the activities of A.I.,” said Facebook chief security officer, Alex Stamos. Another CISO whose experience spans the technology, financial services and media sectors likes to build teams with a combination of people who really know the personality and politics of the organization and newcomers from leading-edge security organizations and meld them within a technically passionate, innately curious and smart culture.

**Develop security and risk metrics that are meaningful for the business.** By mapping security investment to measured risk reduction, organizations can assess the return on investment of security spending as it relates to specific vulnerabilities. “And that drives a lot of the decisions we make about where we want to invest and where we want to put our resources,” said Steinberg. “We measure our capability in both driving down the prevalence of the activity we don’t want to see and whether we were successful in mitigating the harm that is caused by the remaining amount of activity.”

**Adopt a default position of transparency and openness, and define a clear response.** The instinct for many organizations in the past was to hide news about a security breach. That’s much harder today given the prevalence of social media, so mature companies have a response plan in place that defines the actions they will take and who is responsible for making decisions. “You cannot keep anything secret in these days. A very small incident could spark into a big issue if we handle it wrongly. People will tweet about it. Journalists and regulators will ask about it,” said Oerting. “The CSO or CISO has a broader role than just to eliminate the threat. It’s also to deal with the crisis and the residual consequences.” Companies also are more likely than in the past to alert one another, even competitors, about breaches so they can collectively learn from one another’s experience, and even collaborate to fend off attacks.

## The changing face of security leadership

A new kind of cybersecurity leader is emerging as the discipline matures: one who is deeply technical, yet highly strategic and knowledgeable about the business, and a skilled communicator.

“As technology has become more critical to companies’ success, CISOs have evolved from a more direct technical role — managing firewalls, managing the security part of the IT portfolio — to having a much broader risk management role that involves understanding the kinds of ways that technology imposes risk on the rest of the company and on the business,” said Stamos.

To do this well, CISOs have to be able to communicate effectively with other senior leaders and the board, earning credibility through the clarity and consistency of their communication, as well as the ability to think on their feet and speak about risk and security issues in business terms.

“More sophisticated CISOs are social butterflies; they’re very collaborative. They’re interested in their peers’ challenges. They’re able to provide a very balanced view when they’re speaking about a problem. Even during a breach, they don’t throw people under a wheel, but they say, ‘Well let’s see, there are systemic problems and here’s some opportunity to fix them,’ focusing much more on what to do about them than how you got there,” said Richard Puckett, vice president for security operations, strategy and architecture at Thomson-Reuters.

The pool of security leaders with these skills is limited today. Given this practical challenge, companies are exploring creative solutions, such as appointing co-CISOs whose skills complement each other, or by appointing an overall leader with accountability for information and technology risk to set the strategy and engage with the board, with a more “hands-on” CISO, focused on cybersecurity, below. Others are appointing

technology leaders from other disciplines — such as CIOs, CTOs and senior engineering leaders — into the top cybersecurity role. PNC Bank, for example, recently moved the CTO for the Pittsburgh-based bank into a chief security officer role. Given the broad remit of these roles today and hyper-competitive market for security leadership talent in certain industries, creative approaches to finding leaders can be effective when the individual has a strong team and right mindset and invests the time to understand security.

“There are some very good infrastructure managers who would make great CISOs because they have a personality that lends itself to constantly questioning, constantly innovating and understanding the nuances of threat assessment, but there are other infrastructure executives who would fail miserably,” said one CISO. “The challenge is to identify the personality traits that lend themselves to success in those roles.”

Organizations also are exploring various reporting structures for the CISO role. Steinberg favors placing the CISO within the technology organization, reporting to the CIO, so that information security and technology are closely aligned. “The information security space is so deeply technical right now and things are unfolding so rapidly that having any kind of separation between the people doing the execution — designing and developing controls — and those responsible for policy — who identify the need for those controls — is a serious problem. You lose the communication channel, the tight feedback, when you organizationally separate them.”

Others, like Stamos, argue that CISOs shouldn’t always report to the CIO in order to maintain a degree of independence to effectively monitor the IT organization. “There needs to be a natural tension between IT and information security — between the incentive to deliver technology solutions quickly and inexpensively and the need to protect the company and its assets. That natural tension is healthy, and it’s very difficult to maintain

*“There needs to be a natural tension between IT and information security — between the incentive to deliver technology solutions quickly and inexpensively and the need to protect the company and its assets. That natural tension is healthy, and it’s very difficult to maintain if the CSO is reporting to the CIO.”*

if the CSO is reporting to the CIO.” During his time running enterprise security operations and architecture at GE, Richard Puckett was asked to report on a bi-monthly basis directly to the company’s chairman and CEO, Jeff Immelt, as GE recognized the importance of the program, and the need for a communication channel to the board independent of the CIO function.

For others, the question is less about who the CISO should report to than who the CISO is accountable to. Indeed, increasingly, CISOs are also accountable to the board of directors or the board’s audit or risk committee, as well as to their “hard line” executive manager. Said one CISO, “I’m very much a proponent of what financial services organizations do, which is differentiate between the accountability and the reporting. Risk professionals in financial services are accountable to the board, whether they report to the CFO or CIO.”

## Building the next generation of cybersecurity leaders

As CISOs break out of their functional boxes and have impact across a variety of executive functions — engineering, digital, data, risk and even sales, while regularly engaging at board level, there is a “blurring of the lines” in terms of the route up for tomorrow’s leaders. The next generation of CISOs are likely to be more versatile, senior, business- and externally facing than has been the case to date, yet, in many cases still highly technical. “The move to IoT is driving data to live in the cloud, and if data lives in the cloud it needs to be

protected in the cloud. It’s a great example of why a strategist is needed in this space, because all of a sudden you’re being asked to protect data that is outside of your perimeter and that’s a very different problem from building a great castle with a moat and a wall to keep the bad guys out,” said Steinberg.

As they rise, the CISO’s direct staff need to have more exposure to business development, customer communications, business planning and continuity around commercial capabilities, argued Puckett. “Those are the classic areas where there is a deficit among more back-office, IT-centric security teams.”

For many, learning to develop the relationships outside of the function and communicate about cyber risks and solutions at the right altitude for the board and C-level leaders can be the hardest part of the transition into the CISO role. “All of a sudden, you get thrown into a whole new series of relationships,” observed one CISO. “So, as CISOs are building the talent around them, they should make sure they’re getting senior executive exposure on many occasions, so that they’re prepared. If the first time you meet with the executive committee is during a formal, periodic security update, you risk misrepresenting the technical risk and losing the audience in a quagmire of techno-speak and fear.”

## Author

Peter Hodkinson (New York and London)

## ABOUT SPENCER STUART

---

At Spencer Stuart, we know how much leadership matters. We are trusted by organizations around the world to help them make the senior-level leadership decisions that have a lasting impact on their enterprises. Through our executive search, board and leadership advisory services, we help build and enhance high-performing teams for select clients ranging from major multinationals to emerging companies to nonprofit institutions.

Privately held since 1956, we focus on delivering knowledge, insight and results through the collaborative efforts of a team of experts — now spanning 56 offices, 30 countries and more than 50 practice specialties. Boards and leaders consistently turn to Spencer Stuart to help address their evolving leadership needs in areas such as senior-level executive search, board recruitment, board effectiveness, succession planning, in-depth senior management assessment and many other facets of organizational effectiveness.

For more information on Spencer Stuart, please visit [www.spencerstuart.com](http://www.spencerstuart.com).

Social Media @ Spencer Stuart

Stay up to date on the trends and topics that are relevant to your business and career.

