UPENDING TRADITION: **MODELING TOMORROW'S CYBERSECURITY ORGANIZATION**

As CEOs and boards seek executives who can help their companies meet the increasing range of cyberthreats, they should be sure they are starting with the right questions and develop their own unique model.

For a multitude of reasons, the role of the chief information security officer (CISO) has never been more important or more ubiquitous. The prevalence of distributed technologies such as cloud computing and the Internet of Things has created new opportunities to breach systems and access data—including in traditionally nontech industries that have never before been meaningfully exposed online. Increased regulatory scrutiny, such as the General Data Protection Regulation (GDPR), has added further nuance to a CISO's duties. And continued rapid developments in technology and regulation portend even more complexity in the years to come.

As these complexities tend to be highly variable across industries and company sizes, so are the reach and responsibilities of the CISO. No single approach to structuring the role has crystallized. Furthermore, in most cases, it is highly unlikely that a single person could even manage every aspect of information security.

So how should corporate leaders begin defining a CISO role? First, they should carefully examine and understand their own current and future information security needs and threat landscape. Second, they should study CISO roles others have put in place to get a sense of what's possible, including understanding the mix of skill sets and expertise among potential information security leaders. Third, they will need to create a role—or, more likely, roles—that meet the complex demands of the business and are capable of attracting the best talent.

The reach and responsibilities of the CISO tend to be highly variable across industries and company sizes.

Start with a comprehensive approach to security

CISOs used to be focused on network security, firewalls, security policies, and governance—and so, traditionally, they have worked comfortably within the IT organization. Today, however, CISOs often have to contend with many areas outside of traditional IT: security architecture, thousands of security products and services, fielded and connected devices, product security, manufacturing security, safety and trust, data protection and governance, identity and access management, artificial intelligence and machine learning, risk management, privacy, investigations, and physical security. And the list goes on. At one large technology company, the CISO was hired in the early 2000s to manage a team of 20 and now, as the company has invested in a more robust cyber function, manages a team of 800. His security organization has grown with the changing business landscape and today encompasses security operations, security engineering, data privacy, and government and federal cyber matters.

One leader took this organization through that evolution, but this is extremely rare; other similar companies have had four to six different CISOs, and sometimes more, during that same timeframe. Indeed, many companies are splitting up the function among multiple roles and departments. Titles such as "head of business and cyberresiliency" and "chief product security officer" are now becoming more common.

Given this proliferation, it stands to reason that CISO reporting lines and their place in the overall organization capture a lot of attention. But reporting lines alone distract from the much more important issue of a company's end-to-end approach to security.

Companies seeking to define how their security needs should be met need to look at every angle of those needs—including not just physical security but also product security, privacy, data protection, business continuity, and governance—and match their security organizational structure to the current business, regardless of the changes this might create in their current structure. A bank, for example, has a decidedly different security profile than a company that manufactures implantable insulin pumps. When considering its total security needs, a bank might decide that its chief security officer (CSO) can continue to report to the chief information officer (CIO) and manage all of security, while the medical device maker might decide that its head of information security reports to the right place but it needs to add a second role for product security that reports to a head of compliance, quality, or engineering. The point is, whether it's one role or two or even three, considerations of reporting lines should be subsidiary to considerations of security strategy.

Once a company's leaders define its strategy, it will become clear where security needs align with traditional structures and governance models and where those needs require organizational change. As corporate leaders then begin to define specific roles, they'll benefit from examining some current approaches.

Existing CISO roles

We have seen a few approaches taken in different industries that have worked well enough in order for CEOs and other corporate leaders to benefit from considering their pros and cons.

Financial services

Financial services companies typically seek CISOs with a risk and legal orientation, since they must protect huge amounts of sensitive personal data as well as navigate complex regulatory compliance. (Many healthcare companies share a similar focus.) Most use one of two CISO models.

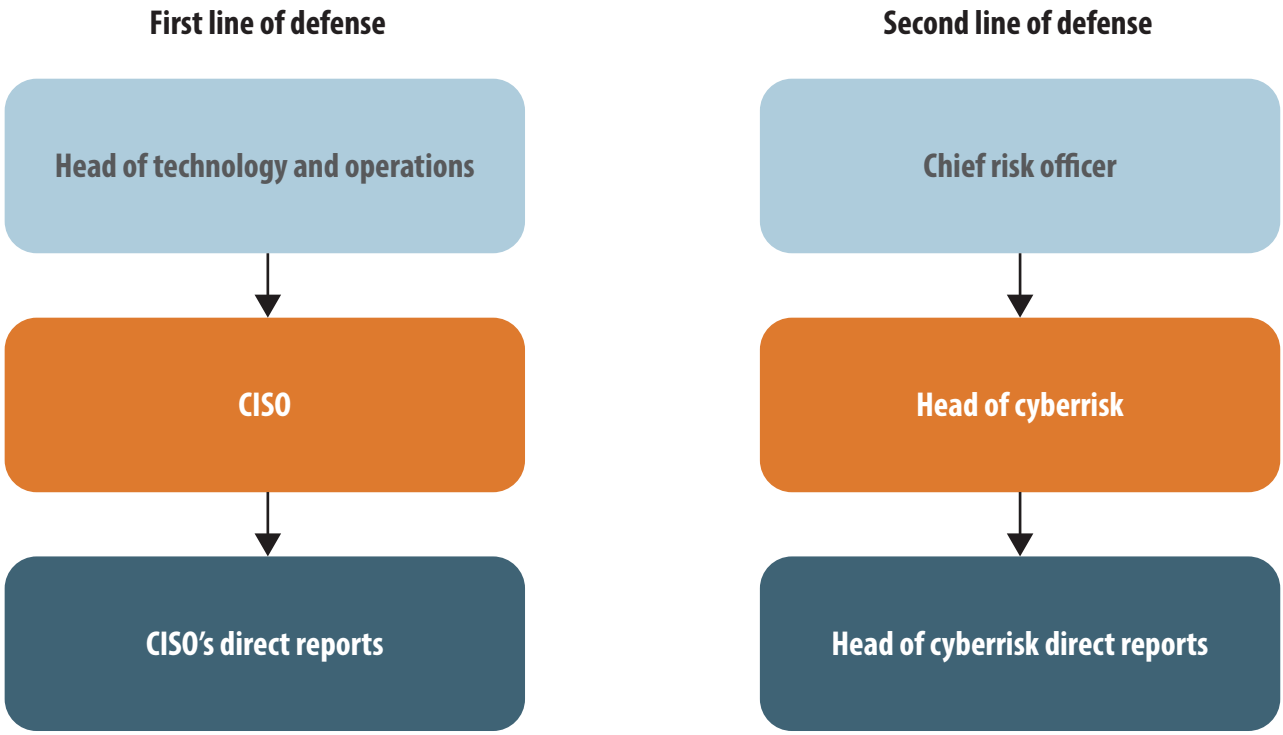
Financial services CISO model 1: A first and second line of defense

Many risk management executives are familiar with the "three lines of defense" model, in which risk management responsibilities are divided into risk owners, including business unit leaders, corporate officers, and IT leaders; various risk control and oversight functions meant to be an independent check of the first line; and internal audit, which is not related to the CISO role (Figure 1).

Of course, every bank has a chief risk officer (CRO), heading the second line of defense; and in many cases, the CRO manages the first line as well. Recently, however, regulators seeking to reduce conflicts of interest have pushed the industry to separate the two, leading to a model in which the risk owners report to a head of business and cyberresiliency, and the control and oversight functions report to the CRO.

While this model does indeed provide better, more independent oversight, the many interdependencies between cybersecurity and information technology can make splitting them apart rather complicated. One CISO at a global payments company, for example, used to lead both the first and second lines—he managed both the people who wrote code and the resources to oversee that code. The company's new CRO, however, took about two dozen members of the CISO's team and moved them to hers, where they were, among other things, writing code to monitor the first line. Suddenly, those team members had to shift gears, spending half of their day coding and the other half making sure that others' code was sound. This transition proved difficult, in part because the CRO knew less about

Figure 1: **Financial services CISO model 1**



coding or managing cyberrisk. The situation settled down after the company created a clear delineation between who wrote code and who reviewed the code.

Financial services CISO model 2: The chief security officer tops the chart

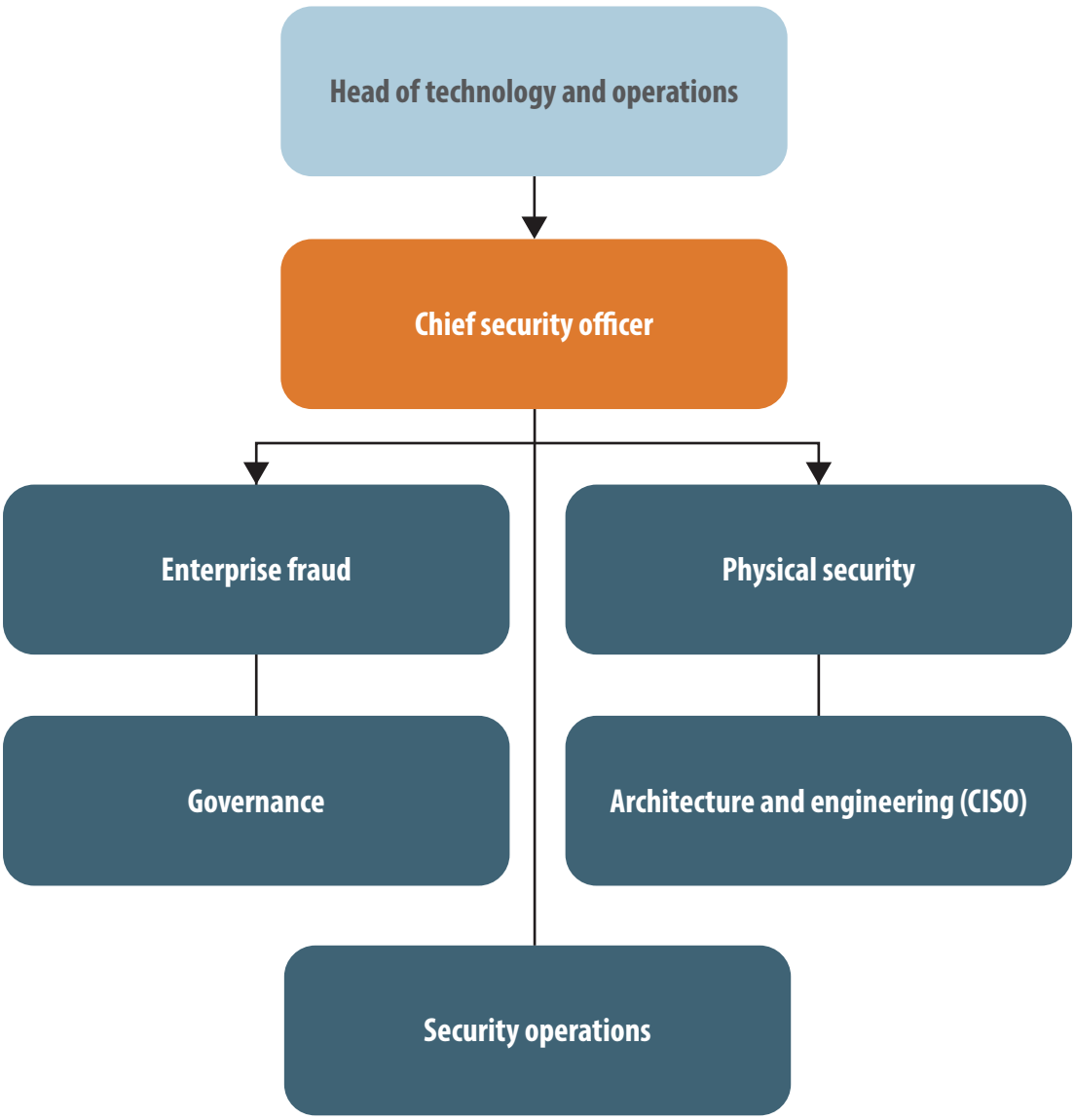
In this emerging arrangement, three groups—enterprise fraud, physical security, and information security—report to a chief security officer (Figure 2). Sometimes, that person in turn reports to a joint head of technology and operations. This latter role is not common yet, but as technology becomes more pervasive, more companies are considering such a role, particularly those that offer services or software. In this scenario, there is still a risk organization and someone reporting into that CRO who has oversight over cybersecurity. In a consumer bank, for example, both physical and systemic security (that is, safeguards for the bank's systems, mostly having to do with identity and access management) are often involved in a breach, and so it makes sense to align these roles.

The main benefit of this model is having a single point of accountability for everything related to security. The biggest challenge lies in succession planning, since the leader of each silo has a specific skill set that doesn't easily translate into the top role.

"Fielded product"–focused companies

Companies that sell connected products such as medical devices, automobiles, pumps, valves, or engines value CISOs who can concentrate on the security of those products, as the trust customers have in

Figure 2: **Financial services CISO model 2**



their brand depends on the security and integrity of their products. CISOs in fielded product–focused companies must also be able to grasp the life cycle of a product to understand whether normal wear and tear or planned obsolescence will create any security risks. For example, older versions of software used by customers can create vulnerabilities, and even software updates themselves, if not done properly, can create unwanted entry points. Good communication skills are also paramount, since product CISOs more frequently need to explain complex technical topics to nontechnical colleagues.

Fielded product–focused CISO model 1: The chief product security officer reports to compliance and safety

In an enterprise with thousands, or possibly hundreds of thousands, of IoT and fielded devices, security needs to encompass manufacturing as well as remediating devices in the event of a breach. Therefore, one such company created a CISO model in which a CISO and chief product security officer work in tight partnership and under the CIO and legal and compliance functions.

In this model, the CISO is responsible for system-access and -security architecture as well as policy compliance, while the chief product security officer defines the overall security program for devices and ensures that the hardware is compliant and that any partners involved in the products' functionality are secure (Figure 3).

As IoT technologies continue to proliferate and enter the mainstream, we anticipate more companies will adopt this type of structure.

Fielded product–focused CISO model 2: The chief cybersecurity officer manages subordinate CISO roles

This model, adopted by a Fortune 50 global automotive manufacturer, accounts for the unique security needs of a large and

Figure 3: **Fielded product–focused CISO model 1**

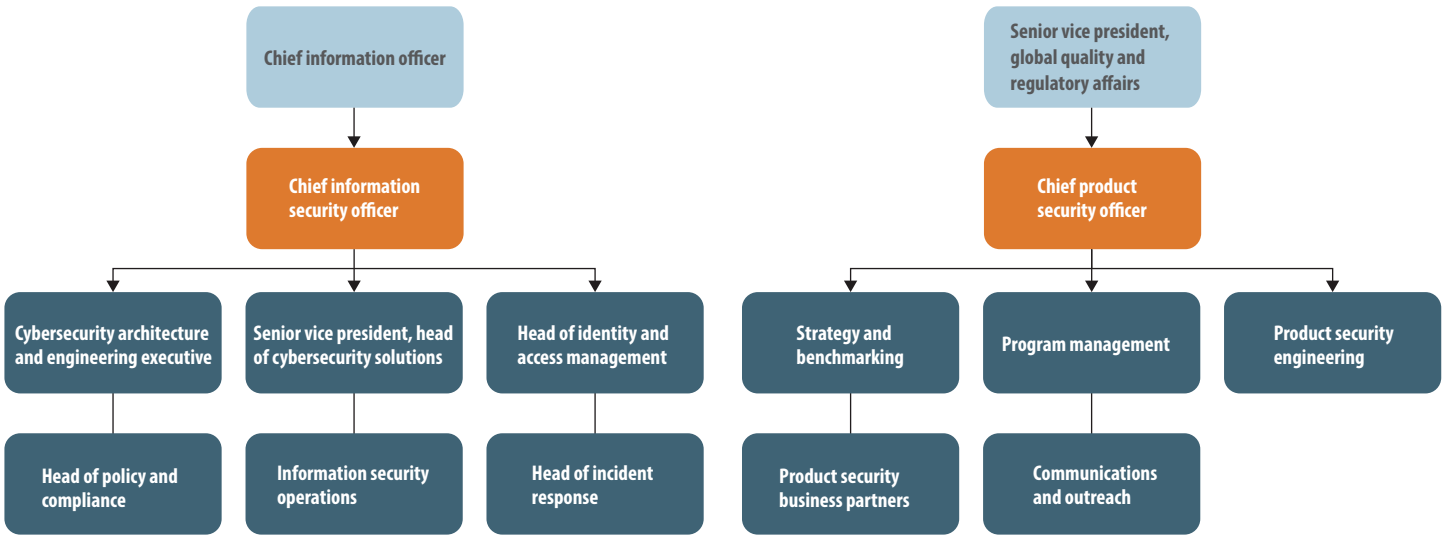
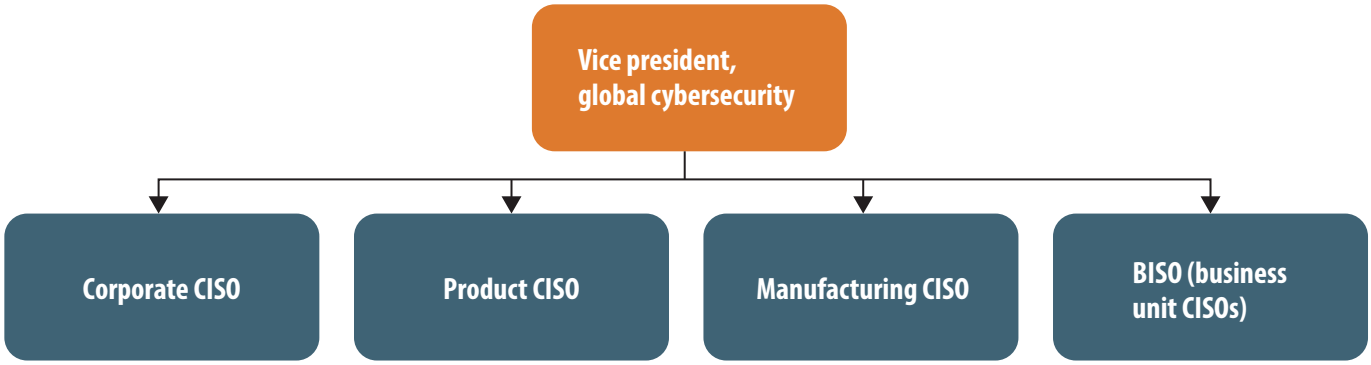


Figure 4: **Fielded product–focused CISO model 2**



disparate organization by having a global head of cybersecurity managing four separate CISO roles (Figure 4).

This works well for companies with large, stand-alone, process-intensive business units that warrant C-level cyber leaders of their own: the product CISO is focused on software and hardware engineering; the manufacturing CISO makes sure plants and plant equipment (the operations technology, or OT) are safe; the corporate CISO is the most traditional of the group; and the business unit CISO oversees unique needs of individual business units. All have different skill sets and require different expertise. At the same time, the company's most senior leaders have a single point of accountability for security.

One of the challenges of this approach is determining what the overall cybersecurity leader really needs to know, since he or she will need to know enough to effectively manage all four CISOs. Should that person, for example, have an enterprise, cybersecurity, or manufacturing background? Should he or she be particularly focused on legal risk or product regulatory compliance? The answers will depend on the specifics of the products the company makes and the markets in which it operates.

Technology

Similar to the fielded product–focused companies, many product-heavy technology companies also need a CISO who can fully understand and manage the security of the products they sell, which can reflect a wider range of concerns than fielded products.

Technology CISO model 1: The CISO reports to the head of engineering

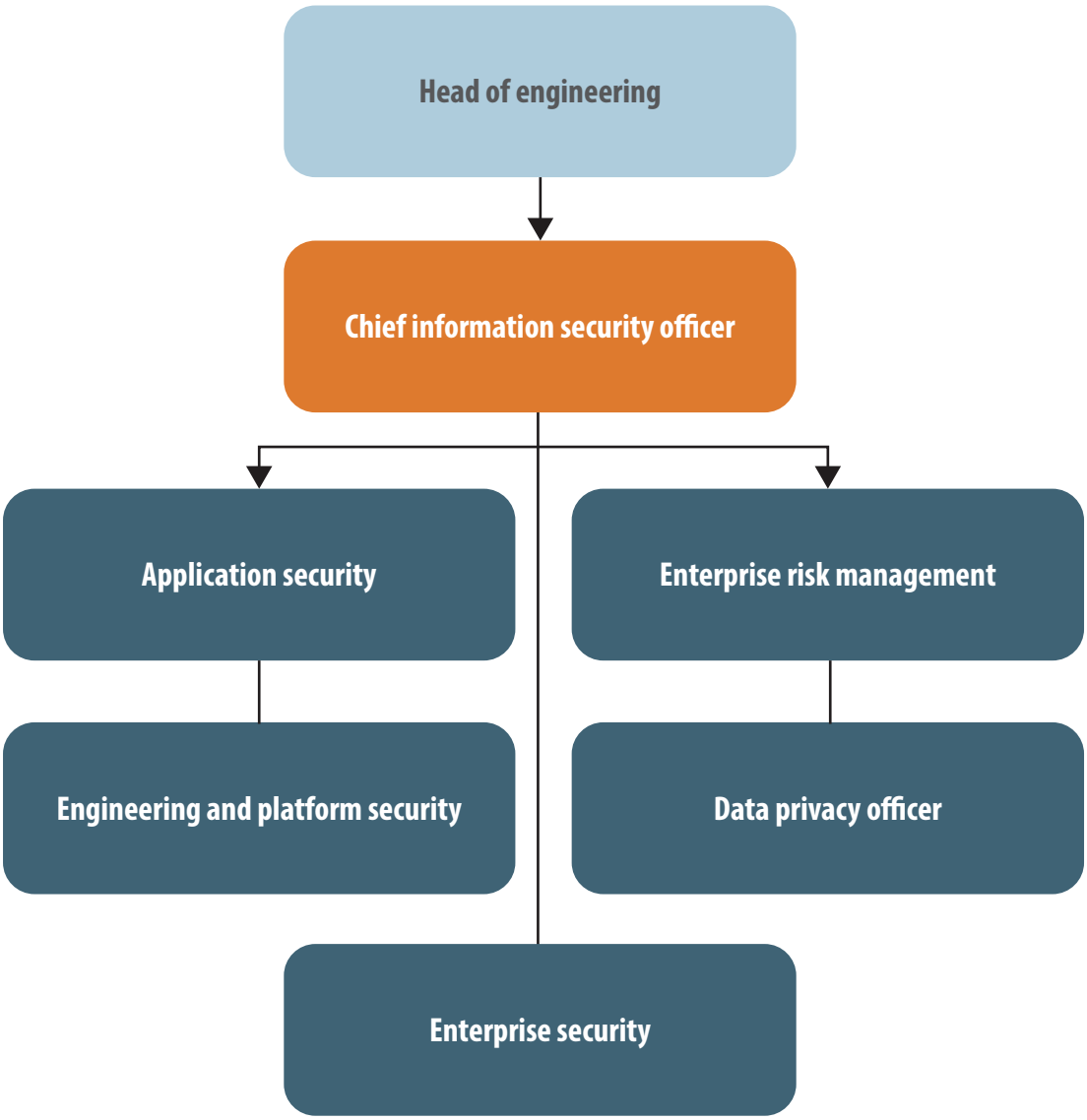
In this model, the CISO acts as both the product and the enterprise CISO. He or she reports to the head of engineering, and other enterprise-level risk management functions, such as app security and privacy, report to the CISO (Figure 5). In this model, the CISO is a "one-stop shop" for corporate and product security; in larger companies, it is also common that each product has its own product CISO reporting in.

With its holistic structure, this organizational structure places significant emphasis on coordinated security. But since this means that no security expertise sits within business functions, there is a risk of engineers and enterprise managers not understanding each other, which can lead to mismatched expectations, project delays, or even occasional security breaches.

Technology CISO model 2: The chief security and trust officer reports to the COO

The leaders of a global maker of network products infused with security determined that their best cybersecurity model was

Figure 5: **Technology CISO model 1**

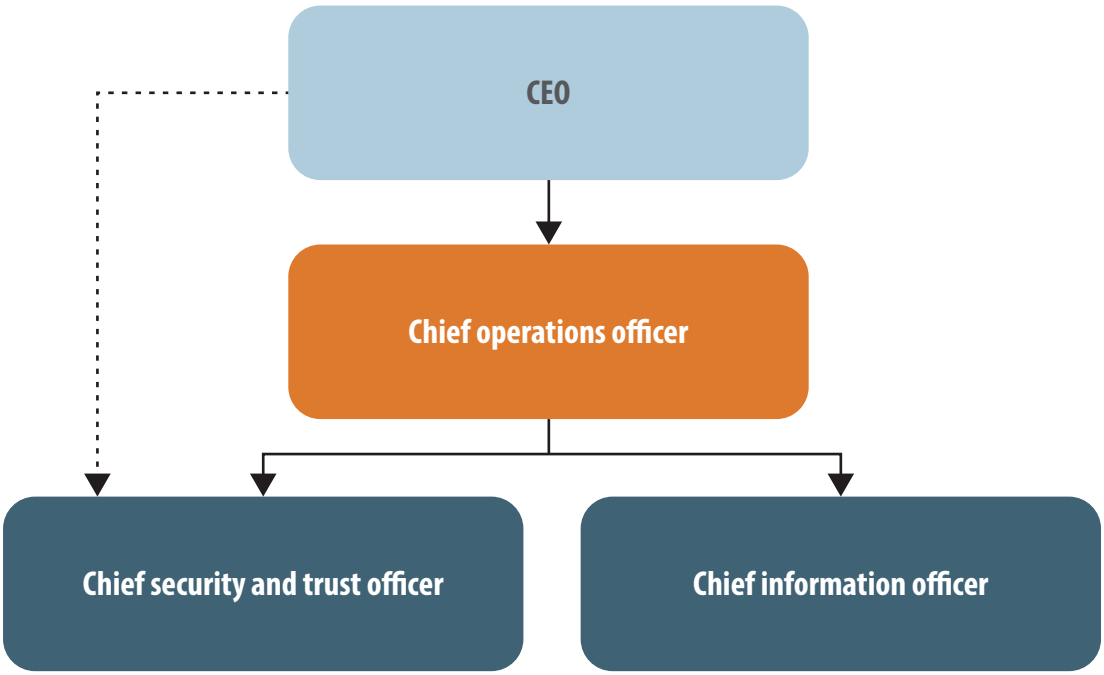


one led by a chief security and trust officer reporting to the COO (Figure 6). This role is on level footing with the CIO and has direct accountability to and regular contact with customers, global governments, and the company CEO and board.

Since security and trust are inextricably intertwined in this company's products, the fact that the chief security and trust officer has a direct line to the company's most senior leaders assigns the ultimate importance to security and ensures that the role has timely access to necessary attention and resources.

The scale of the role is the biggest challenge. The security operation has comprised as many as 2,500 engineers at one point and has expanded and contracted over the years according to business needs. The current 500-person team requires someone who is skilled at corporate security, data security, product/application security, and interactions with governments around the world—not an easy mix to find.

Figure 6: **Technology CISO model 2**



What makes a great CISO?

Even after the CEO and other leaders determine how they want to structure their security leadership, they are unlikely to find a single CISO who can do it all. They must create a role with an adequate pool of qualified candidates—and one that is appealing to those candidates (see sidebar "Constructing a viable role"). They must also make tough choices on which combinations of backgrounds and skills are most important for the CISO—as opposed to the broader cybersecurity team—to possess (Figure 7).

Despite the necessity of trade-offs, in our experience, there are a few skills that differentiate a great CISO from a good CISO. There are also a few misperceptions (see sidebar "Common misperceptions").

Critical skills for CISOs

Most successful product-focused CISOs have a background in engineering or application or software development. This helps them easily adapt to the risks posed by new technologies. CISOs must also be flexible and interested in and able to constantly learn new skills. In addition, successful CISOs have the ability to work across diverse product or business units with variable product development processes to create a comprehensive security organization.

Effective CISOs are also good communicators. They must be conversant in the language of technology because they often have to explain highly technical matters to nontechnical people. They must also be able to build teams and collaborate across the entire company, not just with other IT teams but with leaders of other parts of the business as well. And a skill becoming ever more important, CISOs must be able to succinctly categorize and rank risk at the board and C-suite level.

Last, CISOs succeed most fully when they are customer-facing and can help sell security as a market differentiator. When it comes to the protection of personal data, increasingly the core of the role, a company's reputation is its lifeblood. Reputational damage can be swift, and it can be deadly.

Constructing a viable role

"What's the optimal cyber structure for our company?" is one question. But "Can we find the people we'll need?" is another.

We regularly see companies that create the ideal CISO role or structure for their organization but then can find no one to fill the role. And because the pool of senior cyber talent is still fairly small—and in high demand—it's easy for good CISOs to pass on suboptimal opportunities.

For example, regulators might want a company to hire an executive with a level of seniority that just isn't available among potential candidates. Other issues we've seen are when a CISO is expected to influence the entire enterprise but potential CISOs think the role reports at too low a level, or roles are located in relatively undesirable locations. Sometimes, because of a role's breadth, there are only a handful of people in the world with the necessary skills.

So a critical question for corporate leaders is how to define a CISO role that will attract the broadest talent base possible and thus allow a company to choose the person it wants—and then have that person accept.

For example, say a large financial services firm in a challenging recruiting location wants to hire a chief security officer with broad responsibility over cyber, fraud, and physical security (Financial services CISO model 2). There is an incumbent CSO in the role, and the bank decides to seek someone for a more junior, technical role, hoping to hire a person who will be able to step into the larger role in 12 to 24 months. However, there are only a handful of CSOs with such broad experience at scale, and they all want bigger roles, not lateral moves; anyone interested in that more junior role would more than likely not be ready for the CSO role for another four to five years. The financial services firm must make a choice between redefining the role or lengthening the timeframe for succession.

Figure 7: **Building blocks of the CISO role: Backgrounds and skills**

Main security need	Compliance, risk, and privacy	Deep cyber and technical expertise	IT and infrastructure security	Products and customer-facing technology
Source of expertise and typical experience	Financial services, healthcare, energy, regulators, accounting firms	Former 3-letter agency, Silicon Valley, cyber software, fintech	Fortune 1000, FTSE 250, Nikkei 225, SSE 50	Computer science degree, software development exposure, SaaS, hardware, fintech
Pluses and minuses	Board exposure Polished "Second line" Less technical	In high demand Less well rounded Suspicious of IT "First line"	Board-facing Enough "cyber"? Traditional IT background Less experience in app development	Great with developers Suspicious of IT Enough "enterprise"? Less well rounded

Common misperceptions

Companies seeking a senior security executive will also benefit from *not* following some of the so-called conventional wisdom.

First, it's sometimes true that a CISO who was in charge during a breach is a compromised CISO. But, usually, having overseen a security breach can be quite helpful. There will inevitably be another problem, and having been through a breach is very useful experience. Given the range of threats, from nation states to vendors to connected devices to careless employees, a CISO who was present during a breach may be better able to pick up on warning signs and act swiftly.

Second, for this particular role, short tenures aren't always a bad sign. When CISOs first come on board, many will have a good sense of what they need to do. They spend time learning the business, building communication between teams, starting the right programs—and suddenly there's nowhere to go. As a result, many will leave after being in the role for two to three years. For successful CISOs, this isn't necessarily unusual. CISOs like to solve problems; they don't necessarily want to stay when the project is in "maintenance mode."

And finally, companies don't always need to seek out someone from a three-letter agency. Many firms looking for a new CISO seek people exclusively with experience at the NSA, CIA, or FBI. But some of the most successful CISOs don't come from a regulatory or agency background. While this experience may be useful for highly regulated industries—such as financial services, healthcare, or energy—other types of firms such as technology companies might favor candidates with a broader base of experience in engineering and development, for example. It is important to avoid overemphasizing one qualification to the detriment of others.

Better security is worth upending tradition

There is no single, right CISO answer or organizational structure for every organization, and any answer may not last for long, given both an active, wildly diverse talent marketplace and changing, complex corporate needs. Security needs to "travel at the speed of transformation," and that requires planning, flexibility, and market knowledge. For every single organization, however, it's well worth the time and effort to really think through cybersecurity needs for the next two to four years. CEOs should study how the various roles related to cybersecurity all relate to each other and ensure that they're working together toward a common goal, even if that means upending some existing structures or functions.

By customizing their CISO function to give it the best chance of success, organizations will provide better protection for their customers and better products, as well as make themselves an attractive environment for the experts they need.

About the authors

Matt Aiello
is the leader of Heidrick & Struggles' Global Cybersecurity Practice and is a member of the Global Technology & Services and Information & Technology Officers practices; he is based in the San Francisco office.

maiello@heidrick.com

Scott Thompson
is an engagement manager in the New York office and a member of the Financial Services and Information & Technology Officers practices.

sthompson@heidrick.com

Specialty Practices

Heidrick & Struggles' Specialty Practices provide expertise on emerging technologies.

These practices include:

- Artificial Intelligence, Data, and Analytics
- Blockchain/Distributed Ledger Technology
- Cybersecurity
- Digital Innovation
- Internet of Things

Leader of Heidrick & Struggles' Specialty Practices

Global

Tim Luedke
Managing Partner
tluedke@heidrick.com

Information & Technology Officers Practice

The world is currently experiencing a revolution. With technology constantly advancing, the contemporary business landscape is now defined by rapid innovation. Advances in cloud computing, artificial intelligence, machine learning, and the Internet of Things have enabled companies to become lean, agile, and efficient competitors in the global market. Indeed, the promise of a digital future has convinced organizations across all industry segments to adopt more technology-focused business strategies.

At Heidrick & Struggles, we believe that leadership plays an essential role in this transformation. That is why our Information & Technology Officers Practice is committed to helping our clients find the next-generation technology talent necessary to take their organizations to the next level. Our executive search consultants bring unparalleled experience, having successfully placed more than 1,000 information and technology functional officers with some of the best-known and most-admired companies around the world.

Leaders of Heidrick & Struggles' Information & Technology Officers Practice

Global

Dennis Baden
Co-Managing Partner
dbaden@heidrick.com

Katie Graham Shannon
Co-Managing Partner
kshannon@heidrick.com

WE HELP OUR CLIENTS CHANGE THE WORLD,
ONE LEADERSHIP TEAM AT A TIME®