The Rise of the Chief Information Security Officer

By Aileen Alexander and Jamey Cummings

Although the defenses against enemies that humans have been building for centuries have evolved and become more sophisticated, there still remains a common weakness: the reliance on humans to be effective. The Great Wall of China is an example of an impressive accomplishment on a massive scale. Several walls were built beginning in the 7th century and were later reinforced and joined to create The Great Wall that spans the length of more than 13,000 miles. Similar to many modern corporations of today, it is comprised of several systems bound and connected together over time. However, because humans are enterprising and creative and, well, human, one of the ways to penetrate this defense is to bribe someone to open the door.

In today's world, if you're thinking you can build a modern-day "moat" to keep the bad guys out, consider that the 2014 U.S. State of Cybercrime Survey found that almost one-third of respondents said insider crimes are more costly or damaging than incidents perpetrated by outsiders.

To further support this, an April 2015 report from the data security company Vormetric found that 92 percent of information technology (IT) decision makers working in health care think their organization is vulnerable to insider threats. Some 62 percent highlighted privileged users as the most dangerous type of insider.

In a virtual ecosystem that increasingly includes Bring Your Own Device (BYOD) and the Internet of Things (IoT), traditional firewalls do not ensure protection, and even well-meaning employees can bring down an organization as the lines between physical security and cybersecurity become increasingly blurred.

An Insidious Threat

Cybersecurity breaches, whether perpetrated by insiders or others, are an insidious threat, all the more so because those breaches, including the most disastrous ones, often are not detected until the damage is done. One specialist firm

recently estimated that close to three quarters of security breaches go undetected. No management team can afford to become complacent.

"Company leaders are beyond the mindset of thinking that it's a matter of 'if' their organization will face a cyber-attack; they know it's more a matter of 'when,'" said Rocco Grillo, a managing director and global leader of incident response and forensics at Protiviti, a global consulting firm specializing in risk, advisory, and transaction services. "Many C-level executives and boards now recognize that it is inevitable that they will be attacked if it hasn't happened already."

As we've seen in recent years, information security threats have come from everywhere. This includes intentional and unintentional breaches from a company's own employees, criminals stealing credit card data from retailers, nation states sponsoring hacks into confidential corporate files, and "hacktivists" trying to prove political or social points.

Because of these events, cybersecurity has expanded well beyond the confines of IT and has emerged as a concern at the highest enterprise level. It's now clear to see the potentially devastating effects on shareholder value, market share, reputation, and even long-term survival. Cybersecurity is an issue that crosses all organizational silos and boundaries, top to bottom, encompassing people, culture, and risk management and must bridge security, technology, privacy, and compliance.

"The whole concept of the Internet is that it is uncurated; it was created to connect, not to protect. No one is in charge of it," says Dr. Ronald Sugar, former CEO of Northrop Grumman, who currently serves on several corporate boards. "There's no magic bullet that will solve the security problem, but it helps to have a team of smart people in your company and to build layered defenses."

High Security, High Visibility

Korn Ferry has seen an explosion in the number of companies across a spectrum of industries that are beefing up their information security teams. Its cybersecurity practice saw a doubling in the number of executive searches from 2014 to 2015, with many of those senior information security positions being newly created.

Increasingly, executives who take on the Chief Information Security Officer (CISO) role must be prepared for a laser focus on themselves and their teams.

In the summer of 2015, Korn Ferry researchers analyzed data from a "work analysis" exercise given to executives, which asked them to rate the nature of their jobs. The results showed that 80 percent of CISO respondents said their jobs have a very high profile visibility/accountability orientation—nearly double the percentage of other same-level managers surveyed.

Korn Ferry is also seeing a shift in reporting relationships. While many continue to report to a CIO, many more CISOs are reporting to the head of risk management, a general counsel, the company's president, or the COO instead of the CIO, and some would say for good reason.

"A CISO-CIO reporting relationship could potentially make the enterprise less secure," says Melissa Hathaway, private sector expert and former cybersecurity "czar" under Presidents George W. Bush and Barack Obama, "The CISO is responsible for keeping the enterprise safe and the CIO is responsible for keeping the enterprise running 24/7, so there can be an inherent conflict. It should be a shared decision in the C-suite with the CEO playing a key role."

Because the CISO has moved from the back-of-the house operations to a key public-facing figure relied upon heavily by others in the C-suite, gone are the days when someone who is a brilliant technology expert but lacks business and relationship acumen can make it at the top ranks of a cybersecurity role.

> An ideal CISO has to keep up with the breakneck speed of technological change, and also have a Herculean aptitude for leading courageously, moving nimbly, and understanding the right level of risk needed to make an organization safe while still innovating.

What It Takes to Be a CISO

Countless studies show a critical gap in technical skills for finding CISOs and the security team, but those articles are missing a key point. While experience is important, what is really needed are cybersecurity leaders with a different makeup. Korn Ferry's research suggests that these leaders need to possess the ability to think outside the box, dig deeply into issues, exercise seasoned business judgment, exert influence at the board and C-suite levels, and be a credible business partner. Their motivational makeup needs to be different as well because the most effective leaders are those who seek high visibility and accountability and strive to be agents of change.

To illustrate this point further, see the graphic "Key Attributes for Cybersecurity Executives" on page 58.

Adapting to the Pace of Change

The only constant for today's CISO is change. The survey of CISOs mentioned earlier in this article also revealed that nearly 80 percent of respondents say their jobs had a very strong change orientation. By contrast, just over half of all other same-level managers indicated their jobs had a very strong change orientation.

The survey also found that, compared to other same-level managers, CISOs rank their jobs as having a higher requirement for:

- Long-term strategic vision
- Implementing new initiatives

Key Attributes For Cybersecurity Executives

Competencies

- Strategic, global thinker (sees big picture)
- Thinks outside the box
- Analytical (digs deeply into issues)
- Possess business savvy (understands how information is used in daily operations)
- Balances competing priorities
- Communicates and influences broadly (board, senior mgt.)
- Attracts, builds, and leverages talent

Experience

- Depth of technical experiences
- Understands evolving regulatory and legal environment
- Has (successfully) dealt with / handled security incidents in the past

Traits

- Learning agile (can adapt to the new and different)
- Flexible
- Tolerance for ambiguity
- Intellectually curious
- Bias for action

Drivers

- Seeks high visibility and accountability roles
- Strives to be agents of change (not agents of "no")
- Must "thread the needle" to balance driving change with managing enterprise risk
- Pursues close engagement with business leaders (works to add business value)

In essence, an ideal CISO has to keep up with the breakneck speed of technological change, and also have a Herculean aptitude for leading courageously, moving nimbly, and understanding the right level of risk needed to make an organization safe while still innovating.

People with *all* of those attributes are tough to find. That's where HR partners come in to play a key role in helping the CEO and board find not only the CISO, but the full team of cybersecurity experts who collectively have what it takes to keep organizations safe.

> Close to three quarters of security breaches go undetected.

In working with clients across a wide range of industries, Grillo has seen a shift in the makeup of the types of experts on cybersecurity teams. "Many teams were previously comprised of an IT-centric group to respond to breaches," he said. "Today, companies with more incident response programs and ones that have set 'the tone at the top' have incident response plans whose participants include in-house IT experts plus business stakeholders from legal, compliance and specialists in proactive crisis preparedness as well as real-time crisis management. Outside counsel and forensics investigators are also needed."

Grillo believes the key to effective security governance programs is to have a strong internal leader, often a CISO, who partners with legal to guide the organization before, during and after a crisis.

"Being prepared and having a mature, tested incident response program are essential to mitigating the risk of cyberattack and being able to respond quickly to limit the damages of an attack and restore business operations back to normal," said Grillo.

Emerging Archetypes of CISOs

Based on insights gleaned through the identification and assessment of senior information security and risk management executives during several search assignments through the years, Korn Ferry has found three emerging archetypes of leadership backgrounds:

- **Techie turned executive.** A technical master who works well with the CIO, has a hands-on approach during a crisis and is a driver of enterprise security architecture.
- **Enterprise security and risk-focused leader.** A "big picture" leader who aligns information security with corporate business strategy and one who transforms the security function to meet the environment. This person is process and policy driven.
- **Washington/cyber and physical security blend leader.** A mission-driven leader who understands macro geopolitical and threat trends. This person has access to intelligence due to relationships and credibility. While less technical, this person is able to "connect the dots" across security silos and is "Washington" savvy on a regulatory front.

The analysis found that overall the "techie turned executive" was the most common background, with about half of the information security leaders falling into this category (sometimes with additional experience in one of

the other archetypes as well). But increasingly, even if they came up through the traditional technology ranks, these CISOs are required to broaden their approach, according to Art Ehuan, a managing director at Alvarez & Marsal who specializes in cybersecurity.

"Boards and executives are asking why data breaches are still occurring when their companies spend more each year to implement the latest and greatest new information security tools," said Ehuan. "A CISO who is narrowly focused on technology cannot see the broader spectrum of cyber risk. Threat actors constantly change their cyberattack methodologies, so having a CISO who has the ability to look beyond technology and at the corporation and its people, customers, and suppliers holistically has become imperative."

Industry Trends in Security

To dig even deeper into what makes an effective head of a cybersecurity team, Korn Ferry recently completed an in-depth benchmark analysis of the cybersecurity function, by looking at best-in-class company/industry comparisons. When analyzing the backgrounds of the CISOs at 60 of the Fortune 100 companies, interesting trends by industry emerged:

Financial Services

The largest trend in this industry is for the information security executives to have enterprise security/risk focus experience, and also Washington/cyber and physical security backgrounds. Given the sensitive information and compliance issues in this industry, considerable efforts have been put into making the cybersecurity functions here highly focused on risk management. In fact, the financial services sector is where we have more frequently seen a shift in some CISOs now reporting to the chief risk officer (CRO) instead of the CIO.

> "Threat actors constantly change their cyberattack methodologies, so having a CISO who has the ability to look beyond technology and at the corporation and its people, customers, and suppliers holistically has become imperative."

Consumer Products and Retail

All of the information security executives in this category fell into the "techie-turned-executive" category, with a few having both the "techie" and enterprise security and risk-focused background. This is not surprising as consumer, and even more specifically retail companies, have only more recently come under aggressive attack, whereas the financial services sector has already experienced a long history of sustained cyberattacks, and by necessity have had to develop more mature and progressive information security and risk management programs for some time. The retail sector has recently developed its own Retail Information Sharing and Analysis Center (ISAC) to more proactively partner with other organizations to address evolving cyber threats, and we would expect the mix of archetypes within the sector will evolve over time as more and more organizations develop increasingly mature programs and attract more diverse talent.

> Gone are the days when someone who is a brilliant technology expert but lacks business and relationship acumen can make it at the top ranks of a cybersecurity role.

Aerospace and Defense

The largest percentage here is the "techie turned executive" archetype. This may surprise some, but this industry is strongly high-tech oriented. Quite often senior executives have engineering backgrounds, and the businesses themselves are highly engineering driven. As a result, it stands to reason that senior cybersecurity executives would need to have strong technical backgrounds in order to hold their own and establish credibility with other key internal stakeholders.

Creating a Culture of Cybersecurity

As companies work to build out the right mix of people in their cybersecurity teams, it's also critical that the entire enterprise embraces a culture of cybersecurity, and that training and awareness efforts transcend geographical and functional silos. HR can help by working with the cybersecurity team, the entire C-suite and the board to create, communicate and cascade rules and protocols to keep the enterprise safe.

It's up to senior management teams, including HR, to have a cybersecurity strategy, or they simply may be engaged in a game of whack-a-mole, reacting to one threat after another rather than having a comprehensive game plan. That is not to say that cyber threats and breaches can be eliminated—clearly they cannot—but the resulting damage can be greatly minimized with significant planning and quick response protocol. Everyone, at every level of the organization, must understand his or her role in this new era of security defined by the digital age in which we reside.

Aileen Alexander and **Jamey Cummings** are coleaders of Korn Ferry's Cybersecurity Center of Expertise. They can be reached at aileen.alexander@kornferry.com and jamey.cummings@kornferry.com.