NGS GLOBAL

PERSPECTIVES ON EXECUTIVE LEADERSHIP

Pathway to Protection: The New Skill Sets Required of Chief Information Security Officers

Robert (Bob) Kobayashi, *Managing Partner*
David Nosal, *Managing Partner*

September 2012

As the number of headlines around hacking and security breaches grows, many organizations are turning to their Chief Information Security Officers for answers. We recently spoke with a number of leading security executives to better understand their approach to risk management in mission-critical situations and the key attributes of today's best-in-class security officers. Our conversations revealed a talent pool scrambling to keep pace with rapidly changing requirements.

Evolution of Threats

The role of the Chief Information Security Officer (CISO) has evolved from technical troubleshooter to that of a strategic business partner. In the formative years of information security, the CISO position was fairly simple: The CISO knew where attacks were coming from, what they looked like, and could therefore proactively identify and protect the company against threats. As the Chief Security Officer at a leading network services company recounts, “We had lead time for threats. We were notified about vulnerabilities before exploits were in the wild, and we were able to prevent things before anything disastrous happened.”

The nature of the CISO role changed around the time Operation Aurora hit the media. The 2009 security breach, dubbed Operation Aurora, was a widely publicized cyber attack focused on exploiting dozens of organizations, including Adobe Systems and Google. The hackers responsible for this attack sent tailored messages via email or instant message to individuals at targeted companies hoping that they would open a link to a web page. Once the web page was opened, the intruders were able to exploit a weakness in Microsoft’s Internet Explorer and connect the target’s system to a remote server in Taiwan.[1] That connection enabled the attackers to have complete control of the internal system and steal valuable intellectual property and user information. According to the CSO at a leading network services company, “Aurora was a game changer for security. It showed us that preventing known attacks and putting all of our eggs in one basket doesn’t cut it.”

> “...Preventing known attacks and putting all of our eggs in one basket doesn’t cut it.”
>
> —Chief Security Officer at a leading network services company

Security systems function in much the same way as flu shots: the vaccine prevents against a few of the season’s most common threats, but it is impossible to protect against every strain. Correspondingly, CISOs cannot expect antivirus or antimalware software solutions to protect against all threats. Operation Aurora opened the eyes of many of the world’s leading technology companies to the fact that today’s hackers are incredibly resourceful and can circumvent the preventative measures that have been in place for years.

From this unfortunate event, companies realized that preventing attacks is just one part of the security function.

With so many unknown threats in the wild, an organization might go hours, days, or even weeks without knowing “they’ve been hit.” The ability to detect ensures a more effective response and greater damage mitigation.

The information security program of the past has evolved into a more blended, three-pronged structure that includes the components prevent, detect, and respond. Executives must obtain funding to implement new security measures as the scope of their position expands. Considering the current economic landscape, CISOs must be more strategic and closely aligned with business goals to find mutually beneficial, cross-functional solutions. Companies are more likely to adopt new forms of security if doing so helps to solve issues in other business units. The trends around information security requires a different type of leader; specifically, a strategic business partner.

Technical Innovation

The role of the CISO is evolving in large part due to technological innovations, and the accelerating rate of such innovations. With the increasing availability of cell phones, tablets and laptops, many employees have the option to work from home, across the country, and during irregular hours. A large enterprise might have 50 different applications with various levels of access for each user. The issue for security executives is how to ascertain who should be granted access, where, in what form, and to what degree. Add to that the increasingly mobile nature of jobs – not just in security, but across an organization – and access and identity management becomes even more complex. For example, if an executive from a U.S.-based company is stationed in China, he or she will need access to the company’s applications and databases. The CISO must plan for a system to control access and protect against potential foreign threats.

The CISO and Vice President, Enterprise Information Security at a $20B+ leading mobile service provider believes that domestic operations are not necessarily more secure than foreign sites. He states that "security is not a function of geography – it is a function of people, process and technology." Security breaches can occur anywhere in the world if the proper measures are not in place. However, organizations with international operations should consider recruiting security executives with global experience. Each region has different governing rules around privacy, security and compliance, and familiarity with these variations – and at times, local law enforcement organizations – will aid executives in their efforts to build a cohesive security system.

Managing Risk

Security and risk are indirectly proportional to each other, meaning that more security precautions and systems yield less risk. The CISO at a commercial financing and leasing company states, "We don't have a good language for understanding the risk appetite a business is willing to deal with. If we did, we could build a risk profile that equals the risk appetite." Without a baseline of how much risk a company is willing to tolerate, it is up to the security officer to make judgments and prioritize projects based on previous experience. CISOs should be comfortable making recommendations without a blueprint to guide them.

The return on investment for security is also difficult to communicate. The Executive Director of Information Risk Management and Compliance at a Fortune 100 pharmaceutical manufacturing company put it simply when he said, "There is not a lot of solid ROI data for risk management. We don't have tables that say if you invest X dollars in information security, you reduce your risk by X%."

The return on investment in information security is hard to define or quantify; a "win" for security is simply the prevention of an attack. It is often difficult for executives outside the realm of information security to understand the need for programs based solely on "what ifs."

> "Security is not a function of geography – it is a function of people, process and technology."
>
> — CISO & Vice President, Enterprise Information Security at a leading mobile service provider

Communicating Risk

Security executives can streamline communication between senior management and security personnel by using a common language. Eliminating technical jargon from the conversation ensures that concerns and objectives are correctly understood by all parties, thus synchronizing the company's strategic initiatives with its security systems.

Many security executives get advanced degrees in business or finance to help them understand the language and priorities of non-security executives. According to the CISO at the commercial financing and leasing company, who received a Masters degree in Finance, "It doesn't matter the size of the corporation, the most commonly used language at the top is finance. The more you understand the language at the top, the better equipped you are to translate between information security and senior business leaders."

The same Executive Director of Information Risk Management and Compliance at a Fortune 100 pharmaceutical manufacturing company took an inverted approach to communicating risk across the organization. He first focused on identifying major strategic initiatives that were well-understood throughout different business areas, and then linked those initiatives to specific risks that would impede their success. The security expert elaborated on this notion: "What we saw was that information risk had a lot of intersection between strategic comparatives. When the executive committee saw that, they became more open to investing in security because of its impact on the company's major strategic themes."

Executives outside the field of security are concerned with how proposed changes will affect their operations. Security officers should therefore have enough business knowledge to put security in terms others can understand and appreciate.

Integration with Business Strategy

Many CISOs are taking a more business-centered approach to security. An independent security consultant and former CISO at a leading travel website states, “It’s best if people in the profession keep in mind the reason why the position exists – to help the business achieve and deliver their goals and enable the organization to be more successful and efficient.” Security is now a strategic position that adds value and competitive advantage to a company. The CSO at a leading network services company adds, “When your products are more reputable, consumers will trust you to hold their information. We are no longer a purely technical role; we’re business partners who can add tremendous value to the company.”

To further illustrate this point, consider Amazon.com, the top Internet retailer with revenues in excess of $48 billion in 2011.[2] Without a secure system, users would not trust Amazon.com to hold their payment and personal information. Amazon.com’s level of trustworthiness as perceived by consumers is directly correlated to the company’s revenue stream. With stakes so high, a single security breach could easily destroy customer loyalty, brand reputation and ultimately shareholder value. It is critical for senior security executives to realize how a simple security update or new system can impact all facets of an organization.

CISOs must also fully understand the strategic initiatives of their organization in order to be effective decision-makers. The CISO at a leading entertainment and media company further explains this concept: “Anyone can take a million dollars and start installing new products. The key to a successful security practice is establishing whether or not that security initiative will have a positive impact on business strategy at their specific company.” Each organization has a unique security fingerprint that requires different levels and modes of security. Understanding business goals helps security executives identify the most valued company assets so that they can prioritize and distribute security resources appropriately.

This added emphasis on business strategy does not mean that technical skills are no longer necessary. The CSO at a leading network services company describes the technical requirements by saying, “You have to know what to look for and how to defend against it. You don’t have to be a reverse code engineer or a hacker, but you should have an understanding of what those things are because you are often asked to explain what it is and why others should care about it.” Without a basic understanding of the technical elements of security, it is even more difficult to align communication between the security team and senior management.

“Anyone can take a million dollars and start installing new products. The key to a successful security practice is establishing whether or not that security initiative will have a positive impact on business strategy at their specific company.”

— CISO at a leading entertainment and media company

Brands of Security Management

The network services company’s CSO feels that there are four types of risk and security managers: the purely technical leader, the business savvy executive, the legal partner and the government administrator. The technical leader, while fully qualified to make decisions about preventative installations, might miss the risks associated with the big strategic picture of the company. For example, if a business decides to extend operations overseas, the security officer should have the business acumen to highlight potential issues and help develop a plan to mitigate risk.

Conversely, a business savvy executive with little technical expertise could potentially weaken a leader’s ability to link the day-to-day operations of the security function to the C-suite.

“The legal partner,” according to the above-mentioned CSO, “has a tendency to drive the company to zero risk because of the compliance, privacy and litigation components of security.” It is impossible to reach zero risk in an organization because threats, such as viruses, are always evolving to find the weakest point of entry. Additionally, today’s Darwinian marketplace demands constant innovation. With innovation, however, comes an extended network of risk and unknown variables. In their attempts to reduce risk, CISOs will inevitably impede organizations’ operating abilities and potential for innovation, thus blocking their ability to adapt to market demands.

> "I'm a big believer that diversity makes the world go round."
>
> — CISO, commercial financing and leasing company

Finally, government or military administrators often move into the field of security because they are typically well-versed in war tactics and espionage and therefore bring a unique perspective on cyber terrorism and hacking. However, executives who have only worked in government may not be familiar with how their decisions around security might impact other functional areas. For example, when conducting a security investigation, executives should consider how actions will affect brand reputation and public image. Appropriate courses of action in the private-sector are not black and white, legal or illegal, right or wrong; rather, options and potential outcomes are carefully weighed to make the smartest decision for the entire corporate entity. The CISO and Vice President, Enterprise Information Security at a $20B+ leading mobile service provider adds to this idea by saying, "There is a lot of gloom and doom from security officers who came up through the government. When a government security officer comes into a company, they say, 'turn off the Internet! I've seen things you wouldn't believe.'" The CISO, a government-trained security officer himself, claims, "Government security officers are very well-qualified, but often find it difficult to overcome their blind spots and transition into the private sector." Government-raised security officers must understand that the real challenge is how to acquire, filter and prioritize limited resources to help drive company value.

An ideal security officer would have qualities from all four archetypes; however, merely possessing these attributes is not a recipe for guaranteed success. Security officers will gravitate towards industries and companies that play to their individual strengths and leadership styles. The key to being an effective CISO lies in finding balance and resisting the urge to lean toward one end of the managing spectrum.

Building a World-Class Team

As a way to develop business-minded security professionals, many CISOs are loaning out their team members to other functional areas – such as sales, marketing, finance and human resources – to give them broader exposure to the parts of the organization that security affects. The Executive Director of Information Risk Management and Compliance at a Fortune 100 pharmaceutical manufacturing company, for example, develops business savvy security professionals by putting them into various operating segments to act as liaisons between the risk management function and business unit.

A security team should consist of a diverse group of individuals with varying degrees of technical, business and strategic knowledge. The CISO of the commercial financing and leasing company reveals, "I don't want to hire strictly information security practitioners. While I still need a few technically trained individuals on the team, I also want people who have come up from the operating side, network side, software development, etc. I'm a big believer that diversity makes the world go round."

The CSO at a leading network services company builds on the commercial financing and leasing company CISO's approach by organizing his security team into distinct verticals for each division of security, such as compliance, engineering and privacy. In this system, each operating arm acts as a piece of an ecosystem, as opposed to independent silos. Organizations can collect data and provide more insight and situational awareness when they pull people together from different functional areas to work on specific projects.

By creating a diverse, cross-functional team, CISOs can create pipelines to maintain a balance between each of the four types of CISOs; namely, the technical, business, legal and government security executive. Strong talent pipelines help CISOs identify gaps in leadership, which ultimately adds to the longevity of the function.

Qualities of Tomorrow's CISO

As security and risk become more crucial functions in an organization, the CISO must adopt the role of salesperson. He or she must have the communication and presentation skills to effectively articulate the need for security to board members, the executive committee and employees. Additionally, executives must be able to brand the security team in a way that eases skepticism by others. According to the independent security consultant and former CISO at a leading travel website, people are often resistant to change. A simple firewall installation might be received with hostility and questioned by employees. It is up to the security official to communicate and demonstrate how changes add to the efficiency of the organization.

The field of information security revolves around unknown variables: What will happen if we don't invest in this new security measure? What should we do if there is a security breach? What if the company wants to move operations overseas? According to the CISO of the commercial financing and leasing company, "Security executives often act like Chicken Little and approach things as if the sky were falling. People have a tendency to say 'don't do that' because it might put the company at risk. Instead, 'just say yes,' is my tagline. We should take more risk in a known fashion to help us beat our competition."

CISOs should examine how risk affects their company's competitive advantage and work with the C-suite to ensure that security efforts are consistently working toward the goals of the organization.

CISOs who are comfortable with risk, ambiguity and uncertainty will be better positioned to quickly respond to impending threats. The independent security consultant and former CISO at a leading travel website elaborates on this notion: "With a massive security breach, CISOs must keep emotion at an even keel, keep fear out of the decision-making process, and be able to quickly create a factual report." The ability to rely on experience and intuition will better prepare CISOs for worst-case scenarios.

Additionally, the CSO at a leading network services company states, "there is a certain leadership and visionary skill that is really needed, because we are always trying to predict the future." CISOs should be comfortable acting in ambiguous situations and preparing themselves for future threats. Success as a CISO depends on one's propensity to adapt to changes in the environment; therefore, the ability to forecast future trends and issues is incredibly valuable.

Recent trends in security breaches have shown that threats are no longer solely cyber-based – hackers are starting to exploit human weakness and emphasize social engineering to gain entry into companies security systems. The CSO adds, "The traditional unwritten law of hacking used to be that you could attack my system, but not my people. People are now accessing employee databases, stealing security badges and hacking into security surveillance cameras. It is a lot easier to walk in through the front door than to get through a firewall." The maturation of this trend will increase the demand for security executives who are fluent in espionage, counterterrorism and human threat protection.

Talent Acquisition Challenges

The broad set of competencies sought in today's security executives has evolved quickly. The main challenge companies encounter when recruiting CISOs is the limited number of technically-oriented executives with sufficiently broad business acumen. Up until Operation Aurora in 2009, most CISOs were technical experts with limited management and operating experience beyond their core area of competency. The attack prompted organizations to seek strategic security leaders with not only a broader strategic perspective, but also experience understanding and partnering with all functional areas of an organization. In the three years since the breach, demand for security executives with the right blend of technical know-how, business acumen, communication skills, and leadership experience has outstripped supply.

As a result, many companies are expanding their search radii to include executives from different industries. Organizations should be mindful of the unique security cultures of each industry before executing their talent acquisition strategies. For example, security experts in the financial services industry tend to share information freely and support other CISOs at competing organizations. CISOs in the consumer industry, however, tend to be highly protective of their security systems. Success or failure in the security function affects industries in different ways. Security failure in the financial services sector could cause national chaos and trouble for all financial institutions. It is therefore important for financial services CISOs to share information in order to protect the health of the industry as a whole. On the other hand, sound security systems in a consumer-driven company could help preserve shareholder and brand value. Consumer industry CISOs are therefore careful to keep their security processes confidential to ensure that other organizations don't steal best-in-class practices to gain competitive advantage. It is important to take into account such differences in culture when recruiting security executives from other industries.

As the field of security and risk management becomes more critical to the value and success of companies, many organizations are offering lucrative stay-on packages to their top security leaders. Because of these robust retention plans, companies find it difficult to buy out executives without draining their talent acquisition resources or limited security budgets.

Closing Thoughts

As data threats have proliferated in recent years, the Chief Information Security Officer's role has become critical to protecting brand and shareholder value for many organizations. Although certain requirements will be specific to the entity, most companies expect world-class senior information security leaders to have the attributes listed below:

Requirements of Today's Best-in-Class Chief Information Security Officers

- Draw on cross-functional experience and business acumen to drive corporate value
- Have strong technical orientation
- Understand international security rules and regulations
- Communicate and influence effectively across the organization
- Maintain composure in times of crisis
- Leverage intuition as well as experience when making tough decisions
- Use predictive analytics to forecast future risks and trends
- Build diverse teams with complementary expertise

It is important for hiring organizations to ensure that — above and beyond technical competencies and soft skills — the organizational upbringing and mindset of prospective information security chiefs support strategic objectives.

REFERENCES

[1] McAfee Labs and McAfee Foundston Professional Services (2010). Protecting your critical assets: Lessons learned from “Operation Aurora.” Retrieved from http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf.

[2] Amazon.com, Inc. (2012). Form 10-K For the Fiscal Year Ended December 31, 2011. Retrieved from http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-SECText&TEXT=aHR0cDovL2lyLmludC53ZXN0bGF3YnVzaW5lc3MuY29tL2RvY3VtZW50L3YxLzAwMDExOTMxMjUtMTItMDMyODQ2L3htbA%3d%3d

NGS GLOBAL

AUTHORS

ROBERT (BOB) KOBAYASHI
Managing Partner for the Global Financial Services Practice

DAVID NOSAL
Managing Partner

ABOUT NGS GLOBAL

With 17 offices across the Americas, Europe and Asia, NGS Global provides the extensive resources of major global executive search firms along with high-touch service, accelerated completion cycles and superior candidate access made possible by a mid-sized platform without external shareholders. Through our commitment to industry expertise, cultural knowledge and partner-led search execution, we deliver exceptional value to our clients.

GLOBAL COVERAGE

AMERICAS

Atlanta
Cleveland
Los Angeles
Milwaukee
Minneapolis
New York
San Diego
San Francisco (Americas HQ)

EUROPE

Frankfurt
Munich

ASIA

Beijing
Hong Kong
Melbourne
Shanghai
Singapore
Sydney
Tokyo