Business Horizons (2016) xxx, xxx—xxx

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

The emerging role of the CISO

Val Hooper *, Jeremy McKissack

Victoria University of Wellington, P.O. Box 600, Wellington 6014, New Zealand

KEYWORDS
CISO;
Cybersecurity;
CISO job/role;
CISO attributes;
Organization concerns

Abstract Against a background of board-level concern for cybersecurity, organizations are seeking to ensure the protection of their information assets and minimize the risk of a cybersecurity attack. These objectives place two particular demands on organizations: to appoint a suitable official to head up their information security operations, a CISO; and to ensure that the executive and board are appropriately informed of the organization's security status. In exploring the challenges that confront organizations in selecting a CISO, we drew on data from the U.S., Canada, and New Zealand. Two main issues were addressed. First, the organization has to be very clear on what it wants in terms of the job the CISO is expected to perform and the corresponding attributes that such an incumbent would need to possess. The CISO is a senior-level executive and rather than being a specialized technical expert, the CISO should be an excellent communicator. This will help address the second issue, which is how effectively the CISO can communicate with the board. Some suggestions are provided that serve to aid both effectiveness and efficiency. However, organizations need to embrace their concern about cybersecurity and build it into their selection criteria for board members.

1. Heightened awareness of cybersecurity breaches

Over the past 10 years, cybersecurity breaches—of which hacking is by far the most common—have cost public and business sectors worldwide billions of dollars. While the data from the different countries is not all equally accessible, that which is reported predominantly from the U.S. and the U.K. indicate the most targeted are the financial, healthcare, and government sectors. More recently, the latter two sectors have been the recipients of an ever-increasing number of attacks. Although the retail sector has been the recipient of many attacks, technology-based or focused organizations—such as eBay, Adobe Systems, AOL, and Sony Interactive Entertainment's PlayStation Network—have suffered the heaviest losses. These breaches have been widely reported in the media and have served to raise public awareness of the potential damage of security breaches.

* Corresponding author
E-mail addresses: val.hooper@vuw.ac.nz (V. Hooper), jeremy.mckissack@vuw.ac.nz (J. McKissack)

0007-6813/$ — see front matter
http://dx.doi.org/10.1016/j.bushor.2016.07.004

Another reason for the heightened public awareness of security breaches is that a number of them have been linked to high-profile celebrities. Security and privacy breaches have become a very profitable topic for the media to cover. Three of the most notable leaks have fueled the publicity in recent years: Edward Snowden spoke out against the mass surveillance that was being conducted by the U.S. National Security Agency; like Snowden, Chelsea Manning (born Bradley Manning) breached the U.S. Espionage Act of 1917 with disclosures of U.S. Army activities in Iraq and Afghanistan; and Julian Assange published secret information and news leaks from anonymous sources, including the Manning files, on WikiLeaks, the website he founded. Breaches of this sort have resulted in divided loyalties in terms of support—even between countries such that Assange is currently enjoying asylum in the Ecuadorian embassy in London.

As the public worldwide operates more and more online, there has been an increased public emphasis on security, as well as privacy. This has been driven by media reports of e-commerce incidents and breaches caused by fraud and identity theft. Social media, too, has opened up a plethora of privacy and security breach possibilities. Similarly, the introduction of e-government in many countries has raised privacy and security concerns, especially pertaining to identity theft. In terms of security and privacy, governments are responsible for their nation's well-being. With the threat of IT warfare and international hacking into government security and systems, government departments are much more aware of the importance of security.

It is against this background of increased opportunity for information security breaches and heightened awareness of the repercussions of such breaches that organizations are seeking to protect the security of their information and minimize the risk of possible damage from a breach. Technological disruption and cybersecurity are now top issues in boardrooms across the world (Paredes, 2016). These objectives place two particular demands on organizations: to appoint a suitable official to guide the organization along a well-protected path which ensures its security, and to ensure that the executive and board are informed appropriately of the organization's security status so they are able to make optimal security-related decisions. We sought to determine how best to address these demands via interviews with senior security officials in public and private organizations in the U.S., Canada, and New Zealand, as well as those in security consulting firms. We also conducted a survey of Chief Information Security Officer (CISO) advertisements. Our findings are reported below.

2. Security is becoming too important to trust to IT alone

Traditionally, the IT security of an organization fell under the IT security manager, or under the risk manager. Nevertheless, the role and its responsibilities appeared to be an offshoot of IT. It has typically been placed in the IT department, reporting to the CIO or someone holding a similar position. While such an arrangement made sense, the downside was that IT security got diluted in the plethora of other aspects for which IT is responsible—not only in terms of attention or reporting but, because it is largely invisible in the day-to-day operations of an organization, in terms of budget allocation. Consequently, the reporting to the executive/board was also diluted and unless there had been a major breach, security tended to fade into the background in terms of its profile.

The increased general awareness of the significant potential danger of security breaches has triggered organizations that are particularly security conscious, like government departments and banks, to establish a position at a higher level than the IT security manager to be in charge of their security. The CISO position thus came into being. The CISO is a strategic level position, responsible for ensuring that the information assets and IT systems are protected and secure, and that such protection is in line with the strategic direction of the organization.

The question was where to place the CISO. If placed under the CIO or head of IT, the CISO could have the benefit of the CIO's support in many ways rather than having to compete with the CIO, for instance, for financial resources. This sort of configuration provides opportunity for greater efficiencies and better service to the organization. However, it would be difficult for the CISO to blow the whistle on the IT department if the need should arise. Many organizations that are very focused on the integrity of their information, especially in the government sector, seek to preserve the CISO's independence and position the CISO outside the IT department on a level on par with the CIO. This provides independence, but it can also become problematic with regards to the CISO's accountability and reliance on its IT underpinning. A third configuration is a hybrid, with a split between operations and the more strategic level. In this instance, an IT security manager would work under the IT umbrella and be in charge of technical operations. The CISO would operate independently and be responsible for the strategic aspects of security.

Given the heightened awareness of IT security/cybersecurity and the recognition of the importance of safeguarding its information assets, organizations

that have established independent CISO positions usually have the CISO reporting directly to the CEO. This is the case in many government departments where the focus is very much on the need for scrupulous independence and custody of information. Governments thus create an independent CISO position, while organizations, such as banks that are very IT dependent, allow the CISO to fall under the CIO. Small organizations typically don't have a CISO position and security is handled by the CIO. Organizations thus follow any one of these organizational configurations, depending on their business focus and size.

The role descriptions of CISO positions have typically been derived from three sources: the incumbent, a role description from a similar organization used as a template, or an industry standard. Often a combination of two or three sources is used. The first source is more frequent than is commonly believed. Very often, the CISO is someone who has risen through the IT ranks, first becoming an IT security manager and then the CISO. Such CISOs have strong IT knowledge and experience. Alternatively, they might have come up through the risk management ranks, in which case their emphasis would not necessarily be as technical.

3. Are the expectations of CISOs sufficiently well-embodied in their job descriptions?

Many role descriptions have been crafted directly by the incumbent CISO, and one would assume that no one knows better what the role entails and how it serves the organization best. Despite this, we are left with two questions: Do the job/role descriptions actually result in the appointment of someone who is optimal for the requirements of the organization? Do the job/role descriptions correlate? In order to address these questions, we analyzed over 100 advertisements for open CISO positions to identify what was involved in terms of duties and responsibilities and what sort of person was being sought. The evidence indicated that the job descriptions perpetuate what is currently done or advised as best practice, with scant regard for the needs of the organization. Additionally, the attributes of the person desired for the position do not necessarily match the job description.

For our analysis, we accessed the eBizMBA website for the "Top 15 most popular job websites," as well as the JobisJob and Trade Me websites. These were the most frequently visited recruitment sites in the U.S., Canada, and New Zealand. The study proceeded according to themes that were categorized in Xcel spreadsheets. Further analysis of themes and subthemes, and their interrelationships, was conducted with the use of Leximancer Desktop Academic Edition, Version 4. Understandably, not all organizations embraced the same themes and subthemes. This did not mean organizations did not accord those topics due regard, but rather that there were other aspects which they felt were more important to be noted. The findings are reported according to job/role descriptions and requirements of the desired candidate.

3.1. Job/role descriptions

Although the vast majority of the positions were titled CISO, in some instances the position was named director of information security. Many of the advertisements did not indicate to whom the CISO reported and those that did seemed to be equally split between reporting to the CIO and reporting to the CEO/ President, or CEO and board of directors. The role was frequently described as an expert advisor to senior management and a strategic enabler. Clearly it was envisioned as a key leadership role, entailing more strategic-level responsibilities.

However, many of the job descriptions consisted of a lengthy list of tasks which the CISO would be required to perform or for which they would be responsible. These lists consisted of a mixture of strategic and operational tasks and, given the interspersion of the types of tasks in the lists, it was often not apparent whether the compilers of the advertisements themselves could distinguish clearly between the different strategic and operational levels of tasks.

The focus of the responsibilities fell very much on risk—in fact, more so on risk than security. Protection against risks was paramount, and ensuring business continuity, speedy incident response, and disaster recovery were close seconds in the priorities. Also, according to many advertisements, the CISO was responsible for monitoring the external environment and keeping abreast of the latest developments in the information security and cybersecurity arenas.

At a senior, strategic level, the CISOs were required generally to manage the whole security operation. In most instances, they were required to devise an enterprise-wide security plan and implement it, coordinating all the relevant activities and staff involved. The success of the plan should be monitored regularly and the CISO was responsible for developing metrics and frameworks for regular reporting. The CISO was also responsible to developing and adhering to a security budget, although

this was often not the case if the CISO reported to the CIO. In a number of instances, the CISO was responsible for the development of appropriate IT security governance mechanisms. Another important aspect of the CISO's responsibilities appeared to be to liaise and communicate with important internal and external stakeholders. These included the IT and risk departments internally but also all IT users, legislative and regulatory bodies, suppliers, and customers externally. Additionally, the CISO in many organizations would be tasked, to a greater or lesser extent, with the development of ongoing training and mentoring programs for staff to create an environment of security awareness and vigilance.

Although the strategic level tasks certainly did feature in the job descriptions, the overwhelming majority of the job descriptions contained lengthy lists of operational-level tasks. Sometimes over 30 tasks and responsibilities were listed. Occasionally, they would be introduced by such phrases as "oversees daily security activities," or responsibility for "all ongoing day-to-day activities." While it would be necessary for the position to be industry specific, one job description of the CISO in an average-type business industry even included that the job may contain "occasional bending, stooping, lifting and climbing."

3.2. What organizations are seeking

Given the responsibilities of the CISO, the requirements for the candidate organizations were seeking reflected some interesting trends. Considerable experience was required: usually at least 10 years in IT, 5—10 years in security, and 5—10 years in risk, of which at least five years should have been in a senior management/leadership role. However, only one or two organizations required evidence of successful accomplishments in those specific fields. In addition, the CISO should be knowledgeable about the business environment, although not all advertisements specified this. For organizations in the health sector particularly, knowledge of that specific industry was required.

With regard to education, a degree in computer science or related fields such as IT was usually required. Often a master's degree indicating either further specialization or, occasionally, more of a business focus as manifested in an MBA was recommended. However, an overwhelming list of industry qualifications, such as CISSP, CSSLP, CCFP, CISA, and CISM were usually required. For instance, one job required experience with vulnerability scanning tools, web application vulnerability scanning tools, static analysis tools, and current security certifications such as CISSP, CSSLP, CCFP, GSSP-JAVA, and GSSP-NET. In addition, knowledge of ethical hacking tools was sometimes included. Knowledge of specific systems was usually required, including auditing systems like the ISO/IEC 2700 suite; frameworks like CoBIT, COSO, and ITL; as well as international standards and regulations, such as those promoted by NIST, SOX, and HIPAA.

While some advertisements focused on strong technical skills, such as programming experience with Java and expertise in cryptography, other jobs sought a CISO who was proficient in PC use and Microsoft Windows. This range is surprising, particularly for someone heading up an information security department. Often, experience with Microsoft Windows is assumed in a similar way the ability to read is. On the other hand, the overwhelming focus on technical qualifications and expertise is understandable, but in many instances it was in disregard for the need for business knowledge and the ability to be able to communicate with the rest of the organization and the board.

Some organizations sought a CISO who possessed excellent communication skills, including verbal, written, or public speaking. Yet others (albeit in the minority) took it further, and were wanting someone with outstanding analytical skills, an uncanny ability to move swiftly to resolution, and an aptitude for providing flexible security solutions. One organization was looking for someone with a strong executive presence. A couple advertisements sought a CISO with strong ethics and understanding of business and information security, as well as an expert level of personal integrity. The latter requirements are interesting because, of all people, someone in charge of security should possess a high level of personal integrity. However, sometimes the obvious needs to be stated and as the examples in the introduction demonstrate, often it is those entrusted with highly confidential material who leak it.

Overall, it seems that both the role/job descriptions and the candidate requirements have a strong technical and security focus and that each of them, while containing some elements of business knowledge and understanding, saw the detailed technical/security expertise as being of primary importance. Given the mixture of strategic and operational tasks in many of the long lists in the job descriptions, the impression is created that, although they know CISOs should play a strategic role in their organization, organizations allocate many operational tasks to the role.

Picking up on the importance of good communication skills and business knowledge listed in some advertisements as requisite attributes, one of the emerging, primary roles of the CISO is to act as a

bridge between the executive and IT security functions. It is imperative for the CISO to work well with people and have a good business understanding. Too much of an emphasis on technical expertise, without a balance of business knowledge and interpersonal skills could be detrimental to the organization. Whitman and Mattord (2010, pp. 388—390) said, "In information security, over-specialization can actually be a drawback. . . The CISO is a business manager first and a technologist second."

4. The importance of the CISO as communicator

One of the biggest challenges that CISOs face is the invisibility of security success. Success usually goes unheralded, while breaches can receive huge attention. Success is not generally perceived as resulting from proactivity. If it is celebrated, it is in response to successful reaction to a breach that has already occurred, where the damage is minimized and business continuity is not too disrupted. More often than not, the response is to blame the security department if the reaction is unsuccessful, rather than celebrate each hurdle addressed or attack thwarted.

While boards worldwide are concerned about their security, the invisibility of much of the positive activity ensuring security makes it difficult for board members to grasp the spectrum of such activities and judge whether what is being done is sufficient. Plus, reporting of security performance is often swamped by any number of more pressing issues. For instance, private organizations would be more concerned about stakeholder wellbeing, share prices, and profits—until the organization is struck by a security attack.

As a communicator, success in the CISO role requires the ability to understand what is important to both business and technical audiences. It is unlikely that the issues faced by members of the executive team are the same as those who are developing and administrating security controls within the organization. Having understood the expectations of all stakeholders, the CISO's role is to explain security concepts in terms that can be understood within the C-suite (e.g., through the use of analogy) and to educate the security team about the business drivers that direct the focus of security investment. In his article, Ragan (2014) quoted Stephen Boyer, the co-founder and CTO of BitSight Technologies:

> In no way should every board member have to act as a security expert. But, in today's world, cyber risks are a major part of managing risk in a business. Therefore board members need to make it known what they see as critical and how to begin those conversations.

Acting as a conduit of security information to the executive and, ultimately, the board, it is essential for the CISO to make sure the security team understands what information is required, how discussions should be framed, and the level of abstraction required by decision makers. Otherwise, the CISO is at risk of having conversations with the business that fail to address the most relevant issues.

Based on an understanding of the organization's business strategy, the CISO will often work with risk practitioners to identify the most significant security risks. The CISO also needs to consider risk in relation to business partners and suppliers. Suppliers can be used as a backdoor to get into a targeted organization. Third-party assurance is a growing focus of security managers as organizations become increasingly connected. Security risk indicators help CISOs assess risk exposure. Such indicators might include the number of monthly attempts to access the corporate network from known sources of cyber espionage, attempted intellectual property theft, or quarterly revenue losses associated with customer data leakage incidents. These primary risk indicators are important to communicate to the board because they help illustrate the strengths and weaknesses of a company's overall security posture. Risk indicators such as these can be used to 'tell a story' to board members and fellow executives. Stories can help business managers understand what specific threats are targeting the organization, what the attacks look like, and what they can do to help avoid a breach.

This type of security reporting is primarily old-fashioned and can lead to a reactive response to security incidents. CISOs can reduce the risk of an ad hoc security response by adding context to threat discussions. One method of adding context is through industry and peer benchmarking (Solomon, 2014). The CISO can use peer benchmarking to tell the top management or board where their organization is in relation to their industry and suggest which areas might require improvement. Due to the shared threat of security incidents across industries, it is not uncommon for CISOs to create informal networks for the sharing of information. This level of collaboration between CISOs is not only useful in increasing security for all parties, but it also provides insight into whether an organization is more or less secure than others in the sector. By discussing the expected ranking of an organization within its peer group with top management, the CISO can help

leaders justify strategic changes and investments that can improve security capability.

5. The reporting challenge for CISOs

Having established the risk context and having built security stories, the role of the CISO is then to communicate effectively the security performance and capability of the organization. Executive reports of security assurance and performance metrics, risk and compliance assessments, and ROI measures are often underpinned by a comprehensive set of metrics based on ISO 27001 or other security frameworks.

The challenge with such comprehensive security reporting is that it is generally acknowledged that communicating security information is incredibly difficult, especially with non-technical, disinterested, or time-constrained C-suite executives (Brousell, 2014). Addressing this challenge is not helped by the general trend for security briefings to occur less frequently than the monthly or quarterly briefings with other business disciplines such as finance, HR, or manufacturing. An industry-sponsored survey on the state of risk-based security (Ponemon Institute, 2013) found most senior executives are only asking to hear from their CISOs when breaches have occurred or other security crises hit a need-to-inform crisis level. The focus of the survey was the communication of security metrics. Respondents to the survey were not specifically CISOs but included IT security, operations, and risk management personnel, as well as internal audit and enterprise risk management. A total of 1,321 employees from U.S. and U.K. organizations responded. The survey resulted in these key findings:

- 75% of respondents indicated that metrics were important or very important to a risk-based security program.
- 53% didn't believe or were unsure whether the security metrics used in their organizations were properly aligned with business objectives.
- 51% percent didn't believe or were unsure whether organizations metrics adequately conveyed the effectiveness of security risk management efforts to senior executives.

The report also found that although many organizations rely on metrics for operational improvement in IT, more than half of IT professionals surveyed appeared to be concerned about their ability to use metrics to communicate effectively about security with senior executives. This survey supports a general view that the use of formal assurance techniques, based on comprehensive risk and security metrics, do not always provide an effective communication tool for the CISO.

6. The path ahead

There is a growing trend toward CISOs using cybersecurity control benchmarks, which is viewed as a semi-formal alternative to comprehensive security reporting. One such benchmark that has proven useful within some organizations is the SANS 20 Critical Security Controls (Cain & Couture, 2011; Hardy, 2012). This benchmark is based on a relatively short list of security controls that have proven most useful in combatting cybersecurity incidents. Each of the controls is described in easily understood terms. The current top five from this list (SANS, 2016) are:

1. Inventory of authorized and unauthorized devices;
2. Inventory of authorized and unauthorized software;
3. Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers;
4. Continuous vulnerability assessment and remediation; and
5. Controlled use of administrative privileges.

A comparable cybersecurity control benchmark, the ASD Top 35 is provided by the Australian Department of Defence, Intelligence, and Security (2014). This benchmark is a similarly brief and easily understood list of security controls that have been proven to be effective. The current top four on the ASD list are:

1. Perform application whitelisting of permitted/trusted programs to prevent execution of malicious or unapproved programs, including .DLL files, scripts, and installers.
2. Patch applications (e.g., Java, PDF viewer, Flash, web browsers, and Microsoft Office). Patch/mitigate systems with 'extreme risk' vulnerabilities within two days. Use the latest version of applications.

3. Patch operating system vulnerabilities. Patch/mitigate systems with extreme risk vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.

4. Restrict administrative privileges to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.

The New Zealand government, for instance, used the top four controls from the ASD benchmark as a component of the original New Zealand Cyber Security Strategy. The key stakeholders in the strategy were the CEOs of each of the core government agencies. Each CEO was held accountable for their agency's performance with respect to these four controls. This limited scope made it relatively easy for the CISO (or security manager) within each agency to have conversations about the current state of each control, the associated risks, and mitigation strategies.

This approach to reporting a small number of controls can be used in conjunction with the shortlisting of four to six cyber risks, and reporting the risk indicators that signal the organization's level of exposure to them. A short list of information security risks might include intellectual property theft, a data breach that compromises sensitive customer information, or financial and third-party fraud (Paredes, 2016). The benefit of shortlisting security risks and controls is that they allow the CISO to focus on communicating a relatively small number of significant areas within the larger domain of information security. This more manageable set of controls and corresponding smaller set of metrics is easier to explain to the senior managers. A small number of target controls also provides an opportunity for a CISO to show measureable progress in improving security within an organization.

An ongoing challenge for CISOs is to maintain the momentum gathered by a focused campaign to create an ongoing dialogue with the executive. Another challenge—and one for the organization rather than the CISO to deal with—is to ensure that IT-savvy board members are elected. Better still, such board members should have a good understanding of the basic underpinnings of cybersecurity and the protection of information assets and IT systems.

7. Conclusion

In exploring the challenges that confront organizations in their selection of a suitable CISO, two main issues were addressed. First, the organization has to be very clear on what it wants in terms of the job the CISO is expected to perform and the corresponding attributes such an incumbent would need to possess. The CISO is a senior-level executive and as such should be performing strategic-level tasks rather than daily operational ones. Furthermore, rather than being a specialized technical expert—although we are not denying the importance of technical expertise—the CISO should be an excellent communicator with business knowledge and interpersonal skills. This will help address the second issue, which is how the CISO can fashion communication with the board and the executive in a manner that is most effective and enables the organization to address its cybersecurity challenges. Some suggestions are provided that serve to be both effective and efficient. However, organizations need to embrace their concern about cybersecurity and build it into their selection criteria for board members.

References

Australian Government. Australian Department of Defence, Intelligence, and Security. (2014). *Strategies to mitigate targeted cyber intrusions*. Retrieved from http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf

Brousell, L. (2014). How CSOs can help CIOs talk security to the board. *CIO*. Retrieved from http://www.cio.com/article/2850855/security0/how-csos-can-help-cios-talk-security-to-the-board.html

Cain, C. I., & Couture, E. (2011). *Establishing a security metrics program - Final project report* [White Paper]. Bethesda, MD: SANS Institute.

Hardy, M. G. (2012). *Reducing federal systems risk with the SANS 20 Critical Controls* [White Paper]. Bethesda, MD: SANS Institute.

Paredes, D. (2016). Tech disruption and cybersecurity top boardroom agenda in NZ. *CIO*. Retrieved from http://www.cio.co.nz/article/593402/tech-disruption-cybersecurity-top-boardroom-agenda-nz/

Ponemon Institute. (2013). *The state of risk-based security management*. Retrieved from http://www.tripwire.com/it-resources/the-state-of-risk-based-security-2013-full-report/showMeta/2/?dl=C4FEDC6D-CA1F-B5BC- 8816561E822ACABE

Ragan, S. (2014). Addressing security with the board: Tips for both sides of the table. *CSO*. Retrieved from http://www.csoonline.com/article/2606073/security-leadership/addressing-security-with-the-board-tips-for-both-sides-of-the-table.html

SANS. (2016). *CIS critical security controls*. Retrieved March 20, 2016, from https://www.sans.org/critical-security-controls/

Solomon, H. (2014). Risk management provider now ranks organizations against each other. *IT World Canada*. Retrieved from http://www.itworldcanada.com/article/risk-management-provider-now-ranks-organizations-against-each-other/94859

Whitman, M. E., & Mattord, H. J. (2010). *The management of information security* (3rd ed.). Boston: Cengage Learning.