THE CHIEF INFORMATION SECURITY OFFICER: AN ANALYSIS OF THE SKILLS REQUIRED FOR SUCCESS

DWAYNE WHITTEN
Texas A&M University
College Station, TX 77843

ABSTRACT

The aim of this study is to determine a set of skills needed for a Chief Information Security Officer (CISO) in a competitive business today. To this end, a review of the literature and IT security executive interviews were conducted to identify a set of relevant skills. This list was then compared to a set of job listings for CISOs. Ultimately, a set of skills were developed that organizations can use when defining the CISO position and seeking new CISOs.

Keywords: Chief Information Security Officer, security, governance, IT managementThe Chief Information Security Officer: An Analysis of the Skills Required For Success

INTRODUCTION

Business environments today have become increasingly more severe, complex, and interdependent at the domestic and global level. As this has happened, Information technology (IT) security has taken an increased role in companies in recent years. As evidence supporting the need for increased security, consider the costs of security breaches. According to a study conducted by Ponemon Institute LLC for PGP Corp., a security software vendor in Palo Alto, Calif, security breaches cost $14 million per incident last year. These costs included the direct costs such as attorney fees, as well as indirect costs such as opportunity costs and lost productivity. It was also reported that companies lost 2.6% of their customers as a result of these breaches [4].

In addition to existing security concerns that IT management deals with, newer technologies that are being implemented are adding additional risks as well. As an example, 62% of companies expect to implement converged IP networks in the next three years even though 63% of respondents thought it would increase the risk of security breaches [7].

Established in 1988, the CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. Total vulnerabilities reported by CERT in 1995 were 171, increasing to 1,090 in 2000, and around 6,000 in 2005. Thus, it can easily be seen how the number of incidents has dramatically increased.

Other statistics are just as concerning. The FBI reports that companies have a 90% chance of having a network or computer security breach within the next year, 80% chance of a financial loss due to a security breach, and 44% chance the loss will exceed $4 million (fbi.gov).

These statistics show the increasing number of security concerns that must be addressed by organizations. In order to address these concerns, the right security governance must be in place [15]. Thus, organizations are placing a Chief Information Security Officer (CISO) in charge of corporate information security. Since this position is relatively new, it raises questions about the requisite background and experience of CISOs that is needed. Similar to other IT positions, an analysis of the required skill is necessary [10]. In order to research these questions, a review of the extant literature and executive interviews were performed. From this analysis, the profile of a typical CISO emerged. This was compared to a set of CISO job listings to determine if companies today are actually searching for the "right" type of person for the CISO job.

LITERATURE REVIEW

The academic literature related to CISOs is scarce. Thus, the review of the literature consists mostly of articles in the practitioner press. This literature provides some information, but nothing that empirically investigates the CISO job.

Recent publications have suggested that CISOs should first think of themselves as business professionals and secondly as security specialists [5]. With a focus on the business dimension of their role, they should be evaluating ways to increase value to the organization and integrate security needs with the business goals and objectives. This goes far beyond simply safeguarding the assets they are charged with protecting. In addition, they should understand the organization they are in and the broader industry in which they belong.

The job of CISO has been described as primarily a business professional that can integrate security skills [9]. The business skills are needed to understand the business environment the organization is within so that the CISO can understand how security can be integrated into the business processes and strategies.

It is also suggested that CISOs partake in continuing security education for themselves. This education should include not only security management, but also business content as well. They should be responsible for extending training to the organization as well because information security is not just the responsibility of the CISO, but of the entire organization, especially the other c-level positions [9]. Another suggestion is to send security personnel to professional group meetings such as ASIS and ISACA to increase awareness and networking [1]. Today, more CISOs understand the need to be proactive in offering advice and helping to educate business units throughout the organization as this can add value and decrease risks [1]. Together, they must ensure that security is integrated into risk assessment, business continuity planning, and business strategy.

Soft skills are another important area in which CISOs should be well adept. Because of their executive responsibilities, they should be able to make effective presentations, communicate verbally and in writing, speak well in public, be a good leader [5]

and have strong interpersonal and political skills [9]. These soft skills can be more difficult to acquire and develop, but due to their importance they should not be overlooked.

Developing a flexible problem solving approach becomes critical also. Due to the broad range of security issues that arise, they must be able to have good problem-solving skills that can be used to prevent, detect, and mitigate security threats. The individual in this position should have the ability to calmly facilitate the appropriate resolution to challenging ethical and crisis situations. This problem-solving attribute should also entail investigative skills that aid in tracking a security issue trail.

An understanding of information systems security issues is vital [8]. Ultimately, the CISO is defined by the security they provide to the organization. Thus, a firm understanding of the security threats and risks associated with those threats is essential.

Due to the importance placed on technology in business today, securing information becomes important for the long-term competitiveness and survival of organizations. CISOs must be able to understand this and not only be able to analyze and understand the value proposition of security initiatives, but also to effectively communicate those to senior executives and Board members (ASIS, 2005). It is very likely then, that the strategic, business, problem solving, and soft skills, along with the continuing education of the CISO will provide more value to the organization and the CISOs career than the technical security skills that may be possessed.

METHODOLOGY AND ANALYSIS

After the review of the extant literature, further information was gathered through interviews with eight executives knowledgeable in the area of IT security governance. Seven executives were responsible for information security in their organizations while one executive was a technology consultant with a firm. In each case, the organizations were large and one of the more successful in their respective industries. The industries represented were IT services, oil and gas, and semiconductors. The interviews were conducted over a two month period between December, 2005 and January, 2006. Six of the interviews were conducted in person, while two were conducted via phone. The interviews averaged one hour in length and were part of a larger research project related to IT security governance

Due to the exploratory nature of the interviews, focused interviews were performed as recommended by Spender [13]. This approach employs unstructured interviews with a loose pattern of agreement with the interviewee about the subject. This method provides the interviewee the ability to provide qualitative input rather than just agreeing or disagreeing with the interviewer. In each case, the interviewee was asked their opinion of the skills that evolved from the prior analysis, about the importance of CISOs, and what makes a good CISO. Detailed discussions followed, providing ample input to confirm the results coming from the job listing analysis.

The executives were basically in agreement that the skills which emerged from the analysis were important. The executives were shown the list of skills derived from the literature review analysis and asked to verify that the list was all inclusive. The CISOs suggested the addition of two items: disaster recovery planning and security breach investigations. Several of them felt that these two areas were important enough to be considered a main job function.

A brief description of each of the skills required in described below.

Management skills include those necessary to "obtain the effective acquisition, allocation, and utilization of human efforts and physical resources to accomplish some goal" [14]. The skills could include planning, assigning tasks, monitoring employees, and leading. IT security education can include education related to new security issues and technologies as well as the education to employees related to these same issues and technologies. In addition, it could include the development of awareness programs related to corporate IT policy.

Soft skills are those skills that include oral and written communication, making effective presentations, as well as other interpersonal skills. Problem solving involves the ability to identify the problem, identify alternative options, identify criteria necessary to evaluate the alternatives, make the decision, and finally evaluate the outcome.

Effective IT security requires a broad category of skills to effectively secure an organization's IT assets. A few examples include intrusion detection, firewalls, anti-virus, and a knowledge of the broad range of standards. Business strategy can be thought of as the company's game plan and as the "set of decisions and actions that result in the formulation and implementation of plans designed to achieve a company's objectives" [12].

Broadly defined, disaster recovery planning entails developing a disaster recovery plan, disseminating this plan to other departments and executives, and coordinating emergency responses as a result of a disaster. Security breach investigation includes managing the investigation and resulting legal actions taken as the result of a security breach. In some cases, it could include coordinating the interrogation of witnesses and suspects.

In order to test whether disconsonance exists between what the literature and practitioners are indicating as important and what organizations are looking for in CISOs, data was collected from a review of 33 recent CISO job listings posted at Chief Security Officer magazine (http://www.CSOonline.com), the leading publication dedicated to this position. These listings represented a broad array of industries. Each listing consisted of job duties and background/experience requirements. All of these were thoroughly analyzed to determine what the CISO would be required to do and also the background requirements expected from the successful candidate. After all listings were analyzed, a large spreadsheet was created with employers as the column headings and the duties and background/experience requirements as the row headings. Next, the row headings were analyzed to determine if they could be consolidated into a smaller number of categories. For example, four duties which were derived from the job listing (work with outside consultants on security audits, evaluate and select vendors, oversee vendors, and work with vendors) were consolidated into a broader category labeled vendor relations.

Once the consolidated categories were created, only those included in at least 25% of listings were retained. In the end, a total of seven duties and five background/experience requirements were found. The seven duties include information security policy, education, management, vendor relations, currency, disaster recovery planning, and security breach investigations (see Table 1). The five required background/experience requirements include communication, IT security, leadership, systems, and investigation skills (see Table 2). More details are included in the Appendix.

Table 1. Frequency of Duties on Job Listings

Duties	Percent of listings included
Oversee IT security policy	70%
Management	58%
IT security education	42%
Maintain currency	39%
Vendor relations	36%
Disaster recovery planning	27%
Security breach investigations	27%

Table 2. Frequency of Background Experience on Job Listings

Background Experience	Percent of listings included
IT security skills	76%
Communication skills	61%
System experience	61%
Leadership skills	39%
Investigative experience	27%

DISCUSSION AND CONCLUSION

Based on a thorough review of the literature and interviews with security executives, a comprehensive list of desired skills were found related to the CISO position. This list was then compared to the results from an analysis of job listings to determine if disconsonance exists between the recommended duties and background requirements and the ones that organizations are actually looking for in their job search.

It is interesting to note that total agreement was not found between the research list and the job listings. Both sets did include management skills, information systems security education, a broad array of soft skills, information systems security skills, disaster recovery planning, and security breach investigations. Surprisingly, business strategy skills or experience was not included frequently enough to be included in the job listings categories. It was only mentioned in six of the 33 (18%) of the listings. This is surprising given the fact that it is one of the more critical issues mentioned in the literature and by the executives.

Problem solving was also not included frequently enough in the job listings to be included in the final group. This is surprising due to the significant amount of problem solving that is required to prevent, detect, and control for security issues.

Several skills were included on the job listings that were not mentioned in the literature or by the security executives. These included vendor relations and systems skills. Based on the job listings reviewed, vendor relations consist of evaluating, selecting, and working with vendors. The increased importance of vendor relations has paralleled the increased usage of outsourcing vendors by organizations. A possibility exists for explaining why vendor relations were not included in the original list. It is possible that the authors that were cited and the executives that were interviewed considered vendor relations as the responsibility of another executive. In many organizations, specific individuals are responsible for procurement and/or outsourcing relations.

Systems skills is a broad collection of skills specifically included in each job listing. As seen in the Appendix, this list if fairly large due to the wide variety of technologies, protocols, hardware, and software that organizations use. In most cases, organizations listed specific systems skills in their job listings that correlated to their technology environment. The reason why this may not have been included in the original list is that it is specific to the job. Some jobs require experience in UNIX, C++, TCP/IP, scripting, while others may require experience in a number of other protocols and technologies.

Limitations

Although this research paper has attempted to investigate the role of the CISO in organizations today, still, limitations of this study do exist. One limitation is the relatively low number of job listings that were available. The author does feel that since the number of job listings and industries represented was large enough, that a basic understanding of the duties and background/ experience requirements of CISOs today were found. In addition, with the relative newness of the CISO job, a large number of CISO job listings are not available.

FUTURE DIRECTIONS

Future research in this area could include further investigation of the CISO role utilizing a case study approach whereby the investigator(s) interviewed CISOs and others working with CISOs to get a deeper understanding of their duties, roles, and responsibilities. This investigation could use a framework similar to Mintzberg's [11] that classified managerial work according to ten basic roles. These roles consisted of three interpersonal roles (figurehead, leader, and liaison), three informational roles (monitor, disseminator, and spokesperson), and four decisional roles (entrepreneur, disturbance handler, resource allocator, and negotiator). Many of these appear to be present in the CISO duties included in the job listings utilized for this research. Similar to what has been done with CIOs [3] and Chief Privacy Officers [6], further research could be performed to investigate the extent to which each of these are important in the role of the CISO.

Due to the relative newness of the position in many organizations, the roles, responsibilities, and duties are likely to evolve over time. Thus, a longitudinal study over a span of several years could also provide valuable information as to the evolution of CISO position.

CONCLUSION

Based on a thorough review of the literature, interviews with security executives, and an analysis of job listings, a comprehensive list of duties and background/experience requirements were found related to the CISO position (see Table 3). The most interesting issue that arose from this research is that business strategy did not make the list of most included job duties. Given the high level of importance given to this by the literature and the executives, it is surprising that it was not listed on the job listings surveyed. Thus, it appears that many of the organizations searching for new CISOs during the research period did not fully understand the importance of including the CISO in the business strategy formulation.

It is our hope that organizations currently employing a CISO or are considering the addition of the position will consider the duties and responsibilities included in our results as perfunctory in their position requirements.

Table 3. CISO Skills

CISCO Skills Derived From . . .			
Lit. Review	CISO Interviews	Job Listings	
Management Skills		Management (D) Leadership skills (B / E) Maintain Currency (D)	
IT Security Education		IT Security Education (D) Maintain Currency (D)	
Soft Skills		Communication Skills (B / E)	
IT Security		Oversee IT Security Policy (D) IT Security Skills (B / E)	
Problem Solving			No Match
Business Strategy			No Match
	Disaster Recovery Planning	Disaster Recovery Planning (D)	
	Security Breach Investigations	Security Breach Investigations (D) Investigation Experience (B / E)	
		System Experience (B / E)	No Match
		Vendor Relations (D)	No Match

(D) = Job duties as described in the job listings
(B / E) = Background and / or experience required as described in the job listings

REFERENCES

[1] Datz, T. (2005) How to Manage Security Halfway Around the World. *CISO*, 3(4) pp. 46-48.

[2] Gottschalk, P. (2002) The Chief Information Officer: A Study of Managerial Roles in Norway, *Proceedings of the 35th Hawaii International Conference on System Sciences.*

[3] Grover, V., Jeong, S., Kettinger, W.J., and Lee, C.C. (1993) The Chief Information Officer: A Study of Managerial Roles, *Journal of Management Information Systems*, (10)2, pp. 107-130.

[4] Hall, Mark. (2005) Price of Security Breaches, *Computerworld* 39(46) pp. 8.

[5] IOMA. (2005) So You Want to Be a CISO? The Pay's Good-But It's Not Easy. *Security Director's Report.* 5(7) 1,-10.

[6] Kayworth, T., Brocato, L., and Whitten, D. (2005) What is a Chief Privacy Officer? An Analysis Based Upon Mintzberg's Taxonomy of Managerial Roles. *Communications of the AIS* 6(6).

[7] Kirk, Jeremy. (2005) Survey: Execs see security concerns over IP convergence, *Computerworld* http://www.computerworld.com/networkingtopics/networking/story/0,10801,106057,00.html Nov 8, 2005 issue.

[8] Kros, J., Foltz, C., and Metcalf, C. (2004/05) Assessing and Quantifying the Loss of Network Intrusion. *Journal of Computer Information Systems* 45(2), pp. 36-43).

[9] Kubilus, N. (2004) IT and Security: Converging Roles. *ComputerWorld.* Nov 22, 2004. pp. 44.

[10] Lee, C. (2005) Analysis of Skill Requirements For Systems Analysts in Fortune 500 Organizations. *Journal of Computer Information Systems* 45(4) pp. 84-92.

[11] Mintzberg, H. (1971) Managerial Work: Analysis for Observation, *Management Science*, (18)2, pp. 97-110.

[12] Pearce, J. and Robinson, R. (1994) *Formulation, Implementation, and Control of Competitive Strategy.* Boston: Irwin.

[13] Spender. J. (1989) *Industry Recipes: An Enquiry into the Nature and Sources of Managerial Judgement.* Oxford: Basil Blackwell.

[14] Wren, D. (1994) *The Evolution of Management Thought.* New York: John Wiley and Sons, Inc.

[15] Zhang, C. and Li, S. (2006) Secure Information Sharing in Internet-Based Supply Chain Management Systems, *Journal of Computer Information Systems* 46(4) pp. 18-24.

APPENDIX

CISO Duties

Oversee IT security policy	assist with development of infosec strategy, architecture and policies update existing infosec policies review existing infosec policies development of infosec standards, best practices and guidelines documentation of infosec standards, best practices and guidelines coordinate product sec architecture be involved with design, development and deployment phases to ensure security requirements implement and manage physical security
IT security education	policy education mentoring & formal training of personnel on sec awareness develop infosec awareness programs
Management	lead a team of engineers business savvy coordinate effort of various IT depts w/ strategic goals & objectives of sr management make tradeoffs required to meet business objectives multi-tasking between technical, business, strategic, marketing & planning activities day-to-day management issues assign project tasks to team members work w/ software developers to come up w/ reqs monitor status of team member tasks throughout PDLC ensure project is completed on time & w/ high quality participate in all stages of PDLC
Vendor relations	work with outside consultants on security audits evaluate and select vendors oversee vendors work with vendors
Maintain currency	keep current of existing and proposed state and federal legislation related to infosec maintain awareness of threats (virus, hackers, system vulnerabilities) maintain a high level of proficiency in computer security, business continuity and social engineering future vision
Disaster recovery planning	conduct simulations of disaster recovery plans coordinate emergency response team in the case of a disaster participate on a CERT (computer emergency response team) disseminate disaster recovery plan to managers be aware of departmental requirements in the event of disaster develop plans to resume service after a major disaster develop and publish a business continuity plan ensure integrity, availability, & confidentiality
Security breach investigations	oversee investigations of security breaches oversee legal matters related to security breaches interrogating witnesses & suspects Background experience and skills desired
Communication skills	contract and vendor negotiations interacting with CXOs presentation skills documenting skills
IT security skills	intrusion detection systems IDS security models and design security design for systems firewalls risk mgmt vulnerability assessment network vulnerability analysis anti-virus managing infosec standards & practices (FIPS-140, SSL, HTTPS, RSA SecureID, Kerberos, PAM, PKI ...) IT auditing champion of infosec awareness training developing and implementing infosec
Leadership skills	team member development Leadership visionary leader who mentors
System experience	major platforms (C++, Java, Visual Basic) Microsoft software development application development (including web) SDLC on Windows Platform successful Project Life Cycle Scripting (Perl, SED) OO Design & Implementation J2EE apps large enterprise systems Unix OS global systems Network Protocols (TCP/IP, IPX, NetBUI) routed protocols database administration
Investigation experience	data center operations problem-solving skills cyber investigations investigative methods, principles, & technologies interrogation skills computer forensics