Journal of International Technology and Information Management

Volume 26 | Issue 2 Article 2

6-1-2017

The Chief Information Security Officer: An Exploratory Study

Erastus Karanja
North Carolina Central University, ekaranja@nccu.edu

Mark A. Rosso
North Carolina Central University, mrosso@nccu.edu

THE CHIEF INFORMATION SECURITY OFFICER: AN EXPLORATORY STUDY

Erastus Karanja
ekaranja@nccu.edu

Mark A. Rosso
mrosso@nccu.edu

Department of Computer Information Systems
School of Business
North Carolina Central University
USA

ABSTRACT

The proliferation and embeddedness of Information Technology (IT) resources into many organizations' business processes continues unabated. The security of these IT resources is essential to operational and strategic business continuity. However, as the large number of recent security breaches at various organizations illustrate, there is more that needs to be done in securing IT resources. Firms, through organizational structures, usually delegate the management and control of IT security activities and policies to the Chief Information Security Officer (CISO). Nevertheless, there seem to be a number of firms without a CISO and for the ones that do, there is little consensus regarding who the CISO should be reporting to. This exploratory study investigates the organizational security reporting structures using a dataset of all the firms that hired a CISO between 2010 and 2014. The results suggest that the number of firms hiring CISOs is increasing and that the hired CISOs are predominantly coming from outside the firm. Also, CISOs who are hired to fill newly created positions tend to report to the CEO whereas replacement hires for existing positions tend to report to the CIO. These findings have implications for both academics and practitioners.

KEYWORDS: Chief Information Security Officer, CISO, Certifications, Reporting Structure, IT strategy, Security Breaches, IT Resources

ISSN: 1941-6679-On-line Copy

INTRODUCTION

While organizations continue to heavily invest in Information Technology (IT) resources in order to create and sustain competitive advantage, IT security breaches, and their costly disruption of relationships with customers and other stakeholders, are almost becoming the norm. Thus, the use of IT[1] is proving to be a double-edged sword. Despite the increasing urgency for firms to find ways to better protect their IT and related resources, there is a little academic research on an executive specifically hired to be in charge of the IT security function, often called the Chief Information Security Officer (CISO[2]). At the same time, the practitioner literature illustrates a lack of consensus on the CISO position in terms of attributes such as membership in the Top Management Team (TMT), and their place in the corporate governance hierarchy, and, thus, their level of culpability for data breaches.

This exploratory study seeks to investigate the recent CISO hiring's and provide some clarity around how organizations view the CISO role. The results suggest that CISO hiring is increasing, that the CISO positions are being mostly filled with talent from outside of the hiring organization, and that the newly-created CISO positions tend to report directly to the CEO. These observations have important implications for both scholars and the industry practitioners, as will be discussed. The rest of the study is organized as follows. The following section contains background on how IT security impacts business processes followed by a review of the academic and practitioner IT security literature. Following that are the research questions, methods and results, and discussion, with suggestions for industry and future research.

BACKGROUND

In many organizations, most of the business processes are either associated with, or fully embedded in, sophisticated IT infrastructures. As such, many firms continue to innovatively invest in IT infrastructures because of the competitive advantages accruing from the IT and IT-enabled resources (Lin & Ravichandran, 2008; Luftman & Ben-Zvi, 2010). The IT-driven competitive advantages are manifested by new IT-led products and services, efficient business processes, new

[1] IT is hereafter used to refer to both Information Technology (IT) and Information Systems (IS)
[2] CISO is a common title for the senior IT security person in the organization and is used hereafter to represent other titles such as the Chief Security officer, Enterprise Information Security Officer, Vice President of Global Security, Director of IT Security, etc.

ISSN: 1941-6679-On-line Copy

business models, innovative revenue streams, improved partners' and suppliers' collaboration, and improved customers' experiences (Barua & Lee, 1997; Lin & Mithas, 2008). Taken together, the aforementioned strategies yield above-normal performance differentials due to the abilities of IT individuals to prioritize, organize, and use IT resources to efficiently and effectively manage, control and coordinate internal and external value-creating business processes.

In many firms, the IT management capabilities are geared towards ensuring that IT resources are reliable and available (Mithas, Ramasubbu, & Sambamurthy, 2011). However, the management and security deficiencies of IT resources has been highlighted by an increasing number of incidents in which a number of firms have experienced massive data breaches leading to the disruption of business processes, enormous financial losses, and the erosion of customers' and other stakeholders' trust and loyalty (e.g., Eisenstein, 2008). A number of these IT security breaches and their resultant effects on businesses are briefly highlighted next.

Sony servers were breached and the intruders were able to access personal information of 100 million users. The company reported a loss of $170 million associated with this data breach but security analysts argued that the cost associated with the security breach could be as high as $250 million (Williams, 2011). Target was a victim of malware infection which infected the point-of-sale registers and facilitated the stealing of over 40 million credit and debit card data as well as 70 million customers' personal data. The hackers also set-up a control server within Target's internal network to store the stolen data. The company reported that it spent $148 million in combating the security breach. The company shares also slipped after the breach was made public and the CIO and the CEO resigned shortly thereafter. Target also hired its first CISO to prevent another data breach (Steinhafel, 2013). Neiman Marcus, a luxury retailer, experienced a server breach whereby malware was installed on the point-of-sale terminals allowing hackers to access the payment information of the customers who visited the stores. The server breach resulted in 350,000 credit cards being stolen. The company reported $4.1 million in legal fees, investigations, customer communications, and credit card monitoring costs and eventually reported a $68 million year-end loss compared to a $40 million profit the previous year. Following the security breach, the company also hired its first CISO (Katz, 2014). J.P. Morgan's network server was hacked and malicious programs installed that siphoned gigabytes of customers' data (76 million households and 8 million small businesses) that included names, email addresses, phone numbers and addresses. In response to the breach, JP Morgan pledged to spend $250 million on cyber security (Glazier, 2014).

ISSN: 1941-6679-On-line Copy

Although the aforementioned cases of IT security breaches are not exhaustive, they serve to illustrate the enormity and direct negative repercussions that firms experience when the security of IT infrastructures is compromised. The negative repercussions brought about by IT security breaches are amplified by the fact that many organizational stakeholders namely employees, customers, business partners, shareholders, and government entities are dependent on IT resources. IT security breaches are almost becoming ubiquitous with IT infrastructures and for many firms, it is not if - but when - their IT resources will be breached. For example, a 2015 report by the US Government Accountability Office (GAO) indicated that the number of cyber security incidents reported by federal agencies to the US Computer Emergency Readiness Team (US-CERT) rose from 5,503 in 2006 to 67,168 in 2014, an overwhelming 1,121 percent increase (GAO, 2015).

In addition to the firm's internal reasons for minimizing the negative deficiencies associated with IT security breaches, external factors such as the government legislation, such as the Sarbanes-Oxley Act (Sarbanes, 2002), the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rules (HIPAA, 1996), and the industry standards such as the Payment Card Industry Data Security Standards (PCI DSS, 2015), require firms to guarantee the confidentiality, integrity, reliability and availability of their IT infrastructures (Elliott, Swartz, & Herbane, 2010; Karanja & Zaveri, 2014). There are significant penalties for firms that flout these laws and regulations. For example, Wellpoint Inc. (now Anthem Inc.), one of the largest US insurance companies, was fined $1.7 million by the US Department of Health and Human Services for violating HIPAA Privacy Rules (HHS, 2013). Thus for many firms, the ability to guarantee ***C***onfidentiality, ***I***ntegrity, and ***A***vailability – the ***CIA*** model triad (Russell & Gangemi, 1991) - of the IT resources should be part of the core of their strategy. As such, firms have to expedite or re-orient their IT strategies to mitigate against the security breaches as well as respond appropriately when they experience IT security breaches (Zhang & Li, 2006).

LITERATURE REVIEW

There is little academic research literature on the CISO, the position, and their place in corporate IT security governance. However, a number of researchers have explored some issues related to the CISO position. For example, Johnson and Goetz (2007) conducted a study that involved collecting data from field research and workshops with IT and security executives in large firms (including more than thirty Fortune 500 level companies). The study found that most of their

sample's organizations' CISOs reported directly or indirectly to the CIO. Whitten (2008) created a list of CISO duties by aggregating data from interviews with seven IT security executives and a review of thirty-three online CISO job listings. The study reported that the most mentioned job duties included: oversee IT security policy; management; IT security education; maintain currency; vendor relations; disaster recovery planning; and security breach investigations. Whitten found that business strategy and problem solving skills or experience were underemphasized in both the results obtained from the CISO interviews and job listings. He concluded 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." (Whitten, 2008, p. 17).

Elsewhere, Kayworth and Whitten (2010) interviewed twenty-one information security executives from eleven organizations and found out that each firm's security organization was part of the corporate IT function, with the CISO reporting at most two levels from the CIO. In order to investigate CISOs' ability to act as change agents, Ashenden and Sasse (2013) interviewed five CISOs from global organizations. They found that CISOs struggle to gain credibility in their organizations due to a perceived lack of power, confusion about their role identity, and their inability to engage effectively with company employees. Reece and Stahl (2015) investigated the professionalization of IT security management as the CISO position evolves, due at least in part, to "functional and cultural tensions between those engaged in policy forming and those in technology enforcement" (Ashenden & Sasse, 2013, p. 193). Specialties involved in a potential struggle for control of the IT security management profession include technology, audit, physical security, and business law.

From the practitioner literature, Williams (2007) asserted that CISO reporting is transitioning from the CIO to the CEO, for two main reasons: namely the scope of IT security is expanding from an IT-level concern to a business-level concern, and the need to minimize the potential conflicting priorities arising from the IT security unit reporting to the head of IT unit. These findings are consistent with those reported by Reece and Stahl (2015). Many firms continue to struggle with IT security management issues. For instance, according to a 2014 PwC survey report on the state of US information security practices, many firms that responded to the survey indicated that they had cyber security programs. However, on further review, the cyber security programs at these firms were found to be inadequate and only 28% of the companies had a CISO (PwC, 2014). Proper IT security management policies, practices, and reporting structures guarantee the confidentiality, integrity and availability of IT resources which are becoming more and more important in enabling business continuity.

ISSN: 1941-6679-On-line Copy

IT security issues are also compounded by the fact that, in many organizations and across industries, there is no consensus on who should be in-charge of IT security and also who the individual(s) should be reporting to. For instance, from a survey data published by the Security Magazine (Security, 2015) there is a lack of consensus on the security reporting structure. The inconsistency in the unit in charge of IT security, the officer in charge of IT security, and the office into which the IT security officer reports is illustrated in Table 1. The results in table show that IT security position in the organizational reporting structure varies not only across industries, but *within* industries as well. In only two of the twelve industries shown in Table 1 is there more than 60% agreement on where security reports. In the Agriculture/Farming/Food manufacturing industry, the security docket reports to the Human Resources or Chief Risk or Legal Officer/Risk/Legal/General Counsel. On the other hand, in the Energy & Utilities and the Healthcare/Hospital/Medical Center industries, security reports to the COO/Operations. Finally, in the Industrial Manufacturing, Information Technology/Communications/Media, and the Transportation/Logistics/Supply Chain/Distribution/Warehousing industries, security reports to the Chief Risk or Legal Officer/Risk/Legal/General Counsel.

Industry	Security Reports to	%	Comments
Agriculture/ Farming/ Food Manufactur-ing	Human Resources	29%	In this industry the dominant reporting structure is human resources and the Chief Risk or Legal Officer/Risk/Legal/General Counsel
	Chief Risk or Legal Officer/Risk/Legal/General Counsel	29%	
	CEO/President/Executive Director	14%	
	CFO/Finance	14%	
Business Services/ Consulting	CFO/Finance	29%	The CFO/Finance & Chief Risk or Legal Officer/Risk/Legal/General Counsel are the two main offices into which security reports to
	Chief Risk or Legal Officer/Risk/Legal/General Counsel	29%	
	CIO/Information Technology	14%	
	Other	28%	
Diversified	CAO/Administration	29%	Three main dominant reporting structures
	COO/Operations	29%	
	Chief Risk or Legal Officer/Risk/Legal/General Counsel	29%	
Energy and Utilities (Oil and Petroleum)	COO/Operations	63%	These two industries are oriented towards a COO/Operations security reporting structure
	Chief Risk or Legal Officer/Risk/Legal/General Counsel	25%	
	CIO/Information Technology	12%	
Healthcare/ Hospital/Medical Center	COO/Operations	35%	
	Facilities	19%	
	CAO/Administration	12%	
	GM/Business Unit	67%	Security is reporting to

Industry	Security Reports to	%	Comments
Hospitality/ Casino	COO/Operations	33%	GM/business units
Finance/ Banking/ Insurance	Chief Risk or Legal Officer/Risk/Legal/General Counsel	29%	For most of the firms in these industries, security mostly reports to the Chief Risk or Legal Officer/Risk/Legal/General Counsel
	Facilities	24%	
	Human Resources	14%	
	CAO/Administration	10%	
	CFO/Finance	10%	
Industrial/ Manufactur-ing	Chief Risk or Legal Officer/Risk/Legal/General Counsel	33%	
	COO/Operations	25%	
	Human Resources	13%	
Information Technology/ Communi-cations/ Media	Chief Risk or Legal Officer/Risk/Legal/General Counsel	38%	
	CFO/Finance	23%	
	CAO/Administration	8%	
	CEO/President/Executive management	8%	
	COO/Operations	8%	
Retail, Restaurants/ Conveni-ence Stores/Food Services	Chief Risk or Legal Officer/Risk/Legal/General Counsel	30%	
	CFO/Finance	20%	
	COO/Operations	20%	
	CAO/Administration	10%	
Transporta-tion/ Logistics/ Supply Chain/ Distribution /Warehous-ing	Chief Risk or Legal Officer/Risk/Legal/General Counsel	38%	
	Human Resources	27%	
	CEO/President/Executive Director	16%	
	COO/Operations	16%	

Table 1: Office Which Security Reports to for Various Industries (2015)[3]

The inconsistencies and lack of consensus indicated in the Table 1 are consistent with that of the existing research on the much more established position of the CIO (Al-Taie, Lane, & Cater-Steel, 2014; Peppard, Edwards, & Lambert, 2011; Chun & Mooney, 2009). Overall, the review of the existing literature on the position of CISO reveals a lack of clarity regarding the role of the CISO in the organization, as well as a lack of consensus as to where CISOs in general should report in the organization.

[3] The data in this table is aggregated from various sources and includes information from The Security 500 Benchmarking Survey which aggregates data from various sources and tracks 18 vertical markets (http://www.securitymagazine.com/

RESEARCH QUESTIONS

THE NEED FOR MORE CISOS

Due to the importance of IT resources to organizational business processes, many firms have designated a managerial position in-charge of managing IT resources – CIOs - who have also been incorporated into many firms' TMTs (Preston, Leidner & Chen, 2008). Increasingly, firms are also creating an IT security office and designating an officer in-charge of IT security. Traditionally, in many organizations, IT security has been the responsibility of the CIO or CTO, while in the recent past; the responsibility has been shifting to a CISO (Whitten, 2008). Ashenden and Sasse (2013) argue that for those firms that have a CISO, the CISOs still struggle to gain credibility due to lack of power, confusion about their role identity, and inability to effectively engage employees. Irrespective of these challenges, CISOs are important as organizations continue to face security challenges as well as mandated industry and government legislative compliance requirements.

Security breaches have resulted in the disruptions of business operations, negative stock market reactions, lawsuits, decline in sales due to store and online customer patronage (McCole, Ramsey, & Williams, 2010) leading to deflated profits and hence less staff compensations (shares and monetary incentives) and lower shareholders' payoffs. In the extreme cases, the CEOs may lose their jobs as was the case at Target Inc. (Target, 2014). Also, according to a *PwC 17th Global CEO Survey* (PwC, 2014), 69% of US executives indicated that they were worried about cyber threats impacting growth. As such the CEOs and other top level executives have a vested interest in ensuring that IT resources are secured and are also less prone to security breaches. *Patrick Morley, president and chief executive officer at Bit9+* – a company that provides security to Global 5000 enterprises stated that, *"….the role of the CISO has never been more critical to the success and well-being of an organization than right now. …"* (Bit9, 2015). The role of the CISO is becoming more important as the guardian of the IT infrastructures. Thus, the first research question is:

RQ1: What is the trend in terms of the number of CISOs hired in recent years?

CISOS AS CHANGE AGENTS

A change agent is an individual who undertakes the task of initiating and managing change in an organization and may be internal or external to the organization (Lunenburg, 2010). Given the challenges experienced by firms in managing their IT security (PwC, 2014), and the high direct and indirect costs

associated with IT security breaches, there would seem to be a need in many organizations for changes in IT security practices. The CISO can serve as the agent and champion of change with a mandate to transform the IT security management (Ashenden & Sasse, 2013).

Management of significant change is frequently implemented by hiring an officer from outside the firm (Hofer, 1980). A number of factors have been cited as the driving forces behind the preferences of outsiders as change agents (Lunenburg, 2010). Some of these factors include the fact that external hires are not familiar with the organizational culture, traditions, and politics and are also not beholden to any internal organizational special interests. As such, they can address issues with a renewed perspective without being tied to the status quo or organizational politics.

For instance, following the 2009 security breach, Heartland Payment Systems hired a Chief Security Officer (CSO) from outside the firm. The mandate of the new CISO was to, "…*lead Heartland information security, internal risk assessment programs (protecting sensitive data through risk and threat modeling), and ensures Heartland is compliant with internal, industry and regulatory requirements. Liaison with security professionals in the Financial Services Information Security*….." The CSO was a member of the TMT (Vijayan, 2010). Likewise, after the well published security breach in 2014; Target hired a Senior Vice President and CISO from outside the firm and mandated him to manage Target's information security and technology risk strategy. Target's new CISO job description included being, "…*responsible for managing Target's technology risk strategy and for taking steps to avoid a repeat of the massive data breach at the company last year*…" Specifically, his role was to ensure that the company's stakeholders (company, guests, and team members) are protected from internal and external information security threats. The CISO office holder was a new role for the company (Target, 2014). Capacity, the firm's capability of providing the resources needed for implementing a successful change management, is among the many factors that facilitate the effectiveness of a change agent (Anderson, 2011). When firms hire a CISO, they provide a signal that they have the capacity to implement the IT security changes.

Heartland and Target are just two examples of a CISO hired from outside to act as a change agent. Thus, given that the hiring of a CISO may represent significant change for an organization, we ask:

RQ2: How prevalent are CISOs who are hired from outside the firm?

CISO REPORTING STRUCTURE

Typically, organizational reporting structures are hierarchical, with higher levels in the hierarchy denoting relatively greater power (Brass & Burkhardt, 1993). With the CEO at the top, it is understood that that is where the most power lies. And frequently right below the CEO is the CIO, the individual who is usually in charge of IT resources. Due to the importance of IT to organizational strategy, the CIO often reports directly to the CEO, and in many cases, the CIO is also part of the TMT (Zafar, Ko, & Osei-Bryson, 2015).

Information security has traditionally been the responsibility of the CIO, but now many organizations have created a CISO position to address the increasing importance of information security (Whitten, 2008). However, the issues brought about by compromised IT resources are, not only a concern of the CISO but also, of the whole organization with potential to impact the job status of the holders of the C-level positions (Kubilus, 2004). Thus, IT security should not be an initiative that is left to the IT function but should be an organization- wide initiative that may require the CISO gain the attention of the TMT. Also, the embeddedness of IT resources in the business processes makes the reliability and continuity of IT resources a top priority for the top management teams and calls for stability and clear organizational CISO reporting structure (Elliott, Swartz, & Herbane, 2011). Also, Kwon, Ulmer & Wang (2013) found that firms with an IT executive in TMT have a reduced likelihood of security breaches while Lim et al. (2012) found a positive relationship between the hierarchical power of senior IT executives and the likelihood that the firm will develop superior IT capability.

Given all this, we would expect newly-created CISO positions to be reporting to the CEO rather than the CIO. So, we ask:

RQ3: Where are newly-created CISO positions placed in the reporting hierarchy?

DATA COLLECTION

The dataset for this study was obtained based on the occurrence of an organizational event from LexisNexis Academic. The dataset represented information on firms that hired a CISO (the organizational event) between 2010 and 2014. Organizational events have been adopted in event studies by many researchers to investigate various issues. For example, Chatterjee, Richardson, and Zmud (2001) used an event study method in investigating the market reaction to the hiring of CIOs while Khallaf and Skantz (2011) extended their data and

explored market reactions to the firm's IT expertise. In this study, the organizational event data was plausible based on the fact that many firms issue a press release when they hire senior executives (Fee & Hadlock, 2004). Searches using the keywords "*new*", or "*create*" together with various variations of the CISO or CSO titles and acronyms were done.

To capture as much information as possible about the subject firms, the authors carried out another data search still utilizing LexisNexis Academic (company reports) and organizational charts for each firm. This search involved generating a report for each firm and evaluating the list of the top executives. That way, the authors were able to provide data triangulation about the existence of the CISO position and the reporting relationships.

From the LexisNexis Academic data search, the generated announcements were saved in a Microsoft Word document (refer to the appendix for sample announcements). The methodology used for the data extraction is explained as follows. Each document was reviewed by the authors separately and the extracted data entered into a Microsoft Excel worksheet with the entries for company name, head of security title name, hire date, in or out hire, reporting structure, years of experience, gender and other pertinent information. The information collected was evaluated and in cases of disagreements or ambiguity, the contentious announcements were reviewed together in order to reach a consensus. Eventually, the data were merged into one document before proceeding with the analysis. While this manual process was time consuming, it provided better information than automated data retrieval "bots" which may omit some information and present ethical challenges (Allen, Burk, & Ess, 2008).

RESULTS

Between January 2010 and December 2014, a total of 55 firms hired a CISO and issued a press release following the hiring. Of these 55 firms, 23 were publicly traded firms while 32 were privately held firms. Other studies involving other positions (Chief Information Officers and Chief Risk Officers, for example) have had similar yields in data points per year, but have used longer time frames for data collection as shown in Table 2.

ISSN: 1941-6679-On-line Copy

Study	Position	Time Frame	Years	# of Data Points
Chatterjee, et al., (2001)	Chief Information Officer	1987-1998	12	96
Beasley, et al., (2008)	Chief Risk Officer	1992-2003	12	120
Khallaf & Skantz (2015)	Chief Information Officer	1987-2007	21	118
This study	*CISO*	*2010-2014*	*5*	*55*

Table 2: A Sample of Studies Collecting Executive Hiring Announcements

The sampled firms used various titles to refer to the head of IT security. The titles were Chief Security Officer, Chief Information Security Officer, Vice President and Chief Security Officer, Senior Vice President and Chief Information Security Officer, among others. Of the 55 CISOs hired, only 6 (11%) were females implying that IT security management is a male-dominated domain (89%). From the 55 IT security officers who were hired, there was experience data for 26. The years of experience ranged from a low of 10 years to a high of 40 years and the average years of experience was 22 years.

The major industry security certifications earned by many of the CISOs in this study include Global Information Assurance Certification (GIAC), Certified Penetration Tester (GPEN), Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) among others. The role of a CISO has not been in existence for a long time, when compared to those of CFOs or CIOs, and that may explain why as a measure of skills and knowledge, many of the hired CISOs have industry security certification credentials. Earning security certifications exposes one to the tools and techniques used in IT security as well as serving as a benchmark for knowledge and skills in managing IT security issues and is recommended for anyone aspiring to venture into IT security careers.

RQ1: What is the trend in terms of number of CISOs hired in recent years?

Table 3 shows the annual distributions of the CISOs who were hired between 2010 and 2014. The column labeled "Hired from" denotes whether the security chief was hired from outside the firm or from within the firm (usually a promotion or job rotation). There is a marked increase from 2010 (4) to 2014 (19) in the number of CISOs being hired by firms.

Hired	2010		2011		2012		2013		2014		*Total*	
from	#	*%*	#	%	#	%	#	%	#	%	#	*%*
outside	3	*75.0*	8	77.9	10	83.3	8	72.7	15	78.9	***44***	***80.0***
within	1	*25.0*	1	11.1	2	16.7	3	17.3	4	21.1	***11***	***20.0***
Total	***4***	***100***	***9***	***100***	***12***	***100***	***11***	***100***	***19***	***100***	***55***	***100***

Table 3: Shows the distributions/type of hired CISOs over the years

RQ2: How prevalent are CISOs who are hired from outside the firm?

A Z-test for comparing proportions of the CISOs who were hired from outside the firm to those who were hired from within the firm (outside total=44, within total=11) was conducted (Z=6.293, p=0.001) Based on this dataset, in all the years, firms hired more CISOs from outside the firm than from within the firm.

RQ3: Where are newly created CISO positions placed in the reporting hierarchy?

Table 4 contains data on the reporting relationship. The column labeled "Others" represents those CISOs who reported to neither the CEO nor CIO and included CISOs who reported to executives with titles such as chief marketing officer, chief operating officer, and chief financial officers among others. The column labeled "Not specified" represents those CISOs' who's reporting structures were not explicitly stated in the press releases and could not be verified otherwise. From the table, the proportion of CISOs reporting to the CEO (49%) is higher than those reporting to CIOs (29%), "Others" (16%), and the "Not Specified" groups (6%). To help answer RQ3, Table 4, was regenerated by dropping the row with the "Not specified" data and the two columns with the "Others" and "Not specified" data to yield Table 5, as shown. Subsequently, a 2x2 Chi-square test was carried out and yielded results (χ^2 =6.657, p=0.011) implying that CISOs hired to fill newly-created positions were more likely to report to CEOs, while those CISOs hired to fill old positions were more likely to report to CIOs. A Fisher exact test yielded similar results. On the other hand, a 2x3 Chi-square test with the "Others" column yielded statistically significant results implying that CISOs hired to fill newly- created positions were less likely to report to CIOs.

ISSN: 1941-6679-On-line Copy

Reporting Structure										
Type of position	**CEO**		**CIO**		**Others**		**Not specified**		***Total***	
	#	%	#	%	#	%	#	*%*	*#*	*%*
New position	20	74	6	38	6	67	3	*100*	*35*	***64***
Old position	6	22	10	63	3	33	0	*0*	*19*	***35***
Not specified	1	4	0	0	0	0	0	*0*	*1*	***2***
Total	***27***	***100***	***16***	***100***	***9***	***100***	***3***	***100***	***55***	***100***

Table 4: Distribution of the type of position and the reporting structure

Reporting Structure						
Type of Position	**CEO**		**CIO**		**Total**	
	#	%	#	%	#	**%**
New position	20	77	6	37	26	**62**
Old position	6	23	10	63	16	**38**
Total	***26***	***100***	***16***	***100***	***42***	***100***
χ^2 test results						
$\chi^2 = 6.528$	*Alpha = 0.05*		*Degree of freedom =1*		*Prob.=0.011*	
Fisher's Exact Test Prob. = 0.011						

Table 5: Distribution of the type of position and the reporting structure (CEO and CIO only)

FINDINGS AND DISCUSSION

The fact that firms issue press releases when they hire CISOs is an indicator of the important role that IT security is playing in the organizations. Also, press releases are targeted at the general public and act as a signal that the firm is committed to making structural changes to the management of IT security for the benefit of the stakeholders. The press release data indicate that security is becoming a concern for a number of firms as illustrated by the rising number of hired CISOs. Moreover, in the dataset, the majority of the new CISOs were hired from outside the firm, presumably, either due to lack of talent within the firm or to bring a fresh viewpoint to IT security. Also, most of the CISO hiring in the dataset were for newly-created positions, the existence of which again indicate that firms are beginning to take security more seriously.

Newly-created CISO positions tended to report to the CEO, while replacements for CISO positions tended to report to the CIO. That makes intuitive sense in that creating a new position at a higher level is likely easier politically than changing who a current position reports to. So, even if all hiring companies aimed to

improve the importance of security in the organization, it may be easier politically to increase the rank of the position when creating it anew. The raising of the level of the CISO position in the organization due to an increasing corporate emphasis on security is consistent with agency theory (Eisenhardt, 1989), as this type of restructuring serves to reduce the amount of information asymmetry between the Board/CEO and the CISO. In other research, Kwon, et al. (2013) found that firms with an IT executive in TMT have a reduced likelihood of security breaches. Lim et al. (2012) found a positive relationship between the hierarchical power of senior IT executives and the likelihood that the firm will develop superior IT capability.

Major financial and legal damages have been associated with data breaches. As mentioned earlier, Target's CEO, Gregg Steinhafel, resigned after Target 2014 massive data breach and the company is on track to make $39.4 million settlement with the financial institutions impacted by the data breach On the other hand, Sony Pictures co-chairwoman, Amy Pascal, also resigned following the data breach at the company. Moreover, the CEO of Avid Life Media, parent company of Ashley Madison, resigned and the company shelved plans for an IPO after the company experienced a data breach (Reuters, 2015). High stakes like these can inhibit disclosure of security issues. With the CISO reporting to the CIO, there exists a possible conflict of interest (Allen & Westby, 2007) - the CISO might be less inclined to disclose security flaws that might cast the CIO in a negative light. Also, a lack of direct CISO - CEO reporting structure might mask security vulnerabilities to the top management team, which if exploited, could expose the firm to lawsuits and lost business.

For the CISO-CEO reporting relationship to be successful, the CISOs have to speak the business language (Kayworth & Whitten, 2010). This is illustrated in the Neiman Marcus press releases which stated that, *"….the CISO needs to be able to work with executive management in determining acceptable levels of risks for the organization……providing subject matter expertise to executive management on a broad range of information security standards and best practices; and ensuring security programs are in compliance with applicable laws…"* Although the data did not yield enough information on the educational backgrounds of the hired CISOs to make a generalization on the CISOs academic credentials, the available data indicate that majority of the CISOs earned bachelor's degree in engineering and computer science. Also, a number of these CISOs had earned Master's degree in Business Administration (MBA). The bachelor's degrees and the industry certifications give these CISOs the IT technical skills. On the other hand, MBAs enable them to acquire the business skills and knowledge as well as develop their management skills which are

ISSN: 1941-6679-On-line Copy

important when communicating with the top executives. The certifications and MBAs are also important to those CISO who are reporting to the CIOs because they allow the CISOs to bring both business and IT security skills and knowledge to the table during their interactions with the CIOs.

Elevating the CISO in the organization creates more of a demand for business and communication skills that could exacerbate an already existing shortage of CISO candidates, both inside and outside the firm. This should prompt firms to begin developing in-house IT security expertise by, for instance, encouraging IT staff to obtain appropriate IT security industry certifications. Educational institutions can also incorporate IT security programs into their curricula (Sharma, et al., 2013).

LIMITATIONS & FUTURE RESEARCH

Given the sample size in this exploratory study, further research is needed to confirm the general findings. Another avenue to explore is whether hiring CISOs from the outside is primarily triggered by the firm's desire to instill change in the organization, or whether it is because the expertise to tackle and prevent cyber-attacks is simply lacking in the organization. Also, can it be determined that the hiring of a CISO did indeed improve the security of the organization?

This research did not consider firms' existing reporting structure with regard to who the current CIO reported to when the CISO was hired. The literature suggests that strategic positioning of the firm should dictate who the CIO reports to (CEO vs. CFO) (Banker, et al., 2011). Does who the CIO reports to affect who the CISO should report to? We didn't examine that. A look at the governance structure as a whole may be required to fully sort out who the CISO should report to. Another factor to consider is the varied roles of CIOs (Chun & Mooney, 2009). Of the four role types identified in their CIO typology (Landscape Cultivator, Triage Nurse & Firefighter, Innovator & Creator, and Opportunity Seeker), only the Landscape Cultivator maintained a focus on security. Again, the role of the CIO in the organization could affect the decision of who a CISO should report to.

Due to the increasing importance of the topic of corporate security, there is a general need for further research on the CISO, an instrumental figure in corporate security, in order to build on the preliminary research in this area. For example, background characteristics that make CISO's successful, such as type of experience and education, would be helpful in developing the CISOs of the future. Also, are there different types of CISOs whose level of effectiveness depends of certain organizational characteristics? With the promotion of the CISO position,

how does this effect overall corporate governance? An increasing number of corporations have implemented, or are implementing, enterprise risk management, which integrates corporate IT security into risk management for all aspects of the corporation (Pagach & Warr, 2011). This initiative is typically led by a CRO (corporate risk officer, Karanja & Rosso, 2017). How does the CISO position fit into this type of corporate strategy? What is the relationship between the CISO and the CRO?

CONCLUSION

The findings suggest that hiring for CISO positions is on the rise, mostly from outside the firm, and that the trend for new CISO positions is to report to the CEO (rather than to the CIO, or lower in the IT organization). This suggests that companies are moving to improve their security, something that a company's vendors and customers will come to expect, if not demand.

This exploratory study examined the role of the chief information security officer (CISO), relying on publicly-released hiring announcements to provide insight into the position. Similar to the position of the executive in charge of IT, the CIO, there is a lack of consensus regarding the scope of the position, the duties, and its place in the organizational hierarchy. The researchers hope that future studies can build on this research to help clarify the organizational, environmental and personal factors that influence the optimal governance structure for the information security of a given firm.

REFERENCES

Allen, G. N., Burk, D. L., & Ess, C. (2008). Ethical approaches to robotic data gathering in academic research. *International Journal of Internet Research Ethics*, 1(1), 2012-35.

Allen, J. H., & Westby, J. R. (2007). Characteristics of effective security governance, *EDPAC: The EDP Audit, Control, and Security Newsletter, 35*(5), 1-17.

Al-Taie, M., Lane, M., & Cater-Steel, A. (2014). The relationship between organizational strategic IT vision and CIO roles: one size does not fit all. *Australasian Journal of Information Systems*, 18(2), 59-89.

  ISSN: 1941-6679-On-line Copy

Anthem (2015) Statement regarding cyber-attack against Anthem, Press Release, 2015. Retrieved on 6/19/2017 from https://www.anthem.com/health-insurance/about-us/pressreleasedetails/WI/2015/1813/statement-regarding-cyber-attack-against-anthem

Anderson, L. A. (2011). The change leader's roadmap: How to navigate your organization's transformation. New York, NY: Routledge

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers & Security*, 39, 396-405.

Banker, R. D., Hu, N., Pavlou, P. A., & Luftman, J. (2011). CIO reporting structure, strategic positioning, and firm performance. *MIS Quarterly*, 35(2), 487-504.

Barua, A., & Lee, B. (1997). The information technology productivity paradox revisited: A theoretical and empirical investigation in the manufacturing sector. *Internat. J. Flexible Manufacturing Systems*, 9(2), 145–166.

Bit9, (2015). *Bit9 + Carbon Black Appoints Roman Brozyna CISO* [Press Release]. Retrieved on 6/19/2017 from: https://www.carbonblack.com/company/news/press-releases/bit9-carbon-black-appoints-roman-brozyna-ciso/

Brass, D. J., & Burkhardt, M. E. (1993). Potential power and power use: An investigation of structure and behavior. Academy of management journal, 36(3), 441-470.

Chatterjee, D., Richardson, V. J., & Zmud, R. W. (2001). Examining the shareholder wealth effects of announcements of newly created CIO positions. *MIS Quarterly*, 25(1), 43-70.

Chun M, & Mooney J. (2009) CIO roles and responsibilities: Twenty-five years of evolution and change, *Information & Management*, 46(6), pp. 323-34.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review*, *14*(1), 57-74.

Eisenstein, E. M. (2008). Identity theft: An exploratory study with implications for marketers. *Journal of Business Research*, 61(11), 1160-1172.

Elliott, D., Swartz, E., & Herbane, B. (2010). *Business Continuity Management 2e: A Crisis Management Approach*. Routledge.

Fee, C. E. and Hadlock, C.J. (2004). Management turnover across the corporate hierarchy, *Journal of Accounting and Economics*, 37-1, 3-38.

GAO (2015). High Risk Series-Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information. Retrieved on 6/19/2017 from https://www.gao.gov/assets/670/668415.pdf

Glazier, E. (2014). J.P. Morgan's Cyber Attack: How the Bank Responded, October, 3, retrieved on 6/19/2017 from http://blogs.wsj.com/moneybeat/2014/10/03/j-p-morgans-cyber-attack-how-the-bank-responded/

HIPAA (1996). Health Insurance Portability and Accountability Act (HIPAA), P. L. 104–191, 110 Stat 2023 (1996)

HHS Press Office (2013). WellPoint pays HHS $1.7 million for leaving information accessible over Internet, Press Release July 11, 2013. Retrieved on 6/19/2016 from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/wellpoint/index.html

Hofer, C. W. (1980). Turnaround strategies. *Journal of Business Strategy*, 1(1), 19-31.

Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. IEEE Security & Privacy, (3), 16-24.

Karanja, E., & Rosso, M. A. (2017). The Chief Risk Officer: a study of roles and responsibilities. *Risk Management*, 19(2), 103-130.

Karanja, E., & Zaveri, J. (2014). Ramifications of the Sarbanes Oxley (SOX) Act on IT governance. *International Journal of Accounting and Information Management*, *22*(2), 134-145.

Katz, K., (2014). Neiman Marcus/Group, To Our loyal Neiman Marcus Group customers, June 15, 2014, retrieved on 6/19/2017 from http://www.neimanmarcus.com/NM/Security-Info/cat49570732/c.cat?navid=redirect:security&eVar6=data+breach

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, 9(3), 2012-52.

Khallaf, A., & Skantz, T. (2011). Does long term performance improve following the appointment of a CIO? *International Journal of Accounting Information Systems*, 12(1), 57-78.

Kubilus, N. (2004). IT and Security: Converging Roles. *ComputerWorld*. Nov 22, 2004. p. 44

Kwon, J., J. R. Ulmer, & T. Wang. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems*, 27(1), 219-236.

Lin, O., & Mithas, S. (2008). Information Technology and Inventories: Substitutes or Complements?. *ICIS 2008 Proceedings*, 11.

Lim, J. H., Stratopoulos, T. C., & Wirjanto, T. S. (2012). Role of IT executives in the firm's ability to achieve competitive advantage through IT capability. *International Journal of Accounting Information Systems*, 13(1), 21-40.

Luftman, J., and Ben-Zvi, T. (2010). Key Issues for IT Executives 2009: Difficult Economy's Impact on IT, *MIS Quarterly Executive*. 9 (1), 203-213.

Lunenburg, F. C. (2010). Managing change: The role of the change agent. *International Journal of Management, Business and Administration*, 13(1).

McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research*, 63(9), 1018-1024.

Mithas, S., Ramasubbu, N., & Sambamurthy, V. (2011). How information management capability influences firm performance. *MIS Quarterly*, *35*(1), 237-256.

Pagach, D., & Warr, R. (2011). The characteristics of firms that hire chief risk officers. *Journal of Risk and Insurance, 78*(1), 185-211.

PCI DSS (2015) PCI DSS Quick Reference Guide, PCI Security Standards Council, Retrieved on 6/19/2017 from https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf

Peppard, J, Edwards, C & Lambert, R. (2011). Clarifying the ambiguous role of the CIO, *MIS Quarterly Executive*, 10(1), 31-44.

Preston, D. S., Leidner, D. E., & Chen, D. (2008). CIO leadership profiles: implications of matching CIO authority and leadership capability on IT impact. *MIS Quarterly Executive*, *7*(2), 57-69.

PwC (2014). US cybercrime: Rising risks, reduced readiness - Key findings from the 2014 US State of Cybercrime Survey, Retrieved on 6/19/17 from https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

Reuters (2015). Infidelity website Ashley Madison faces 'doomsday scenario' after hack: bankers, July 21, 2015. Retrieved on 6/19/2017 from http://www.reuters.com/article/ashleymadison-hack-ipo-idUSL5N1014B920150721

Reece, R. P., & Stahl, B. C. (2015). The professionalisation of information security: Perspectives of UK practitioners. *Computers & Security*, 48, 182-195.

Russell, D., & Gangemi, G. T. (1991). Computer security basics. "O'Reilly Media, Inc.".

Sarbanes, P. (2002, July). Sarbanes-Oxley act of 2002. In The Public Company Accounting Reform and Investor Protection Act. Washington DC: US Congress.

Security (2015). 2015 Security 500 Sector Reports, Retrieved on 6/19/2017 from http://www.securitymagazine.com/articles/86726-security-500-sector-reports

Sharma, A., Murphy, M. C., Rosso, M., & Grant, D. (2013). Developing an undergraduate information systems security track. *Information Systems Education Journal*, *11*(4), 10-17.

Steinhafel, G., (2013). A message from CEO Gregg Steinhafel about Target's payment card issues. Retrieved on 6/19/2017 from

https://corporate.target.com/article/2013/12/important-notice-unauthorized-access-to-payment-ca

Target (2014). Target Names Brad Maiorino Senior Vice President, Chief Information Security Officer, Retrieved on 6/19/2017 from http://pressroom.target.com/news/target-names-brad-maiorino-senior-vice-president-chief-information-security-officer

Vijayan, J. (2010). Court gives preliminary OK to $4M consumer settlement in Heartland case, Payment processor agrees to reimburse consumers for costs associated with 2009 breach, *ComputerWorld*, May 7. Retrieved on 6/19/2017 from http://www.computerworld.com/article/2518212/security0/court-gives-preliminary-ok-to--4m-consumer-settlement-in-heartland-case.html

Whitten, D. (2008). The chief information security officer: An analysis of the skills required for success. *Journal of Computer Information Systems*, 48(3), 15-19.

Williams, M., (2011). Sony Apologizes, details PlayStation Network attack, *ComputerWorld*, May 1. Retrieved on 6/19/2017 from http://www.computerworld.com/article/2508384/security0/sony-apologizes--details-playstation-network-attack.html

Williams, P. (2007). Executive and board roles in information security. *Network Security*, 2007(8), 11-14.

Zafar, H., Ko, M. S., & Osei-Bryson, K. M. (2015). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers*, 1-11.

Zhang, C. & Li, S. (2006) Secure information sharing in Internet-based supply chain management systems, *Journal of Computer Information Systems*, 46(4) pp. 18-24.

ISSN: 1941-6679-On-line Copy

APPENDIX

ENP Newswire
June 16, 2010 Wednesday

Sapient Names Curtis Dalton Chief Information Security Officer

LENGTH: 378 words

BOSTON -Sapient (NASDAQ: SAPE) announced today that it has **appointed** Curtis Dalton as **chief information security officer,** a **new** role for the company.

He will be based in Boston and report to Preston Bradford, chief operations officer.

Dalton brings more than 19 years of information security experience with Fortune 1000 companies to the company. Prior to joining Sapient, he was founder and CEO of a Boston-area information security consulting firm that he ran for nearly seven years.

With today's increased pressures in the areas of information security and data protection, Dalton will work internally and externally to ensure that Sapient's sensitive data remains secure. Also, Dalton will evaluate and make specific actionable recommendations to the company's current security policies and practices globally. He will oversee Sapient's Global Security Office (GSO) team.

'The combination of our strategic growth in the SapientNitro, Global Markets and Government Services segments, combined with the ever-changing external environment, has created increased challenges in the areas of information security and data protection,' said Bradford. 'I expect that Curt will establish new best practices to reduce our risk and continue to protect our company as well as our clients as needed.'

Dalton is a Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) and a certified ISO 27001 Lead Implementer and Auditor. He is also a published author of a dozen articles and a popular information security book by Osborne McGraw Hill.

About Sapient

Sapient is a global services company that helps clients transform in the areas of business, marketing, and technology. The company operates three divisions that enable clients to gain a competitive advantage and succeed in an increasingly

ISSN: 1941-6679-On-line Copy

digital world. SapientNitro, Sapient Global Markets and Sapient Government Services fuse insight, creativity and technology to drive innovation and to help clients navigate complex business problems. Our approach is the subject of case studies used by MBA programs at Harvard and Yale. The company has operations in North America, Europe, and Asia-Pacific.

[Editorial queries for this story should be sent to newswire@enpublishing.co.uk]

Governance, Risk & Compliance Monitor Worldwide
November 12, 2014 Wednesday

Neiman Marcus Hires First CISO

LENGTH: 645 words

Luxury retailer Neiman Marcus has **hired** its first **chief information security officer** following its data breach late last year that compromised approximately 350,000 payment cards.

Sarah Hendrickson, who joined the company Nov. 3, will work to develop security and risk management programs, among other responsibilities, company spokesperson Ginger Reeder tells Information Security Media Group. The **new CISO** reports to Michael Kingston, the retailer's CIO, Reeder says.

Hendrickson most recently served as CISO at Children's Medical Center of Dallas.

Security Leadership a Must

The news sends a reminder that, at this point, every major retailer should have a CISO, says Julie Conroy, a security analyst at the consultancy Aite Group. Without question, someone with C-level responsibility for a retailer's cybersecurity strategy is a must, she says. As we have seen, the threat environment is progressing too fast for security to be a siloed effort or an afterthought.

The only reason a company should forego **hiring** a **CISO** is if their CIO is performing the function appropriately in managing the risk for their company assets, says Karen Evans, national director of the U.S. Cyber Challenge, a national cybersecurity workforce initiative, who also served as administrator for e-government and IT in the George W. Bush White House.

Evans says Neiman Marcus' **new CISO** needs to gain a clear understanding of the company's management structure, as well as the relationships between the CIO

and the CEO and the board members. Hendrickson should also understand her technical environment in order to mitigate residual risk from the improvements the company has been making since the breach, Evans says.

With the holiday season fast approaching, and the retail sector being hit hard with payment breaches, it will be critical to have a good, resilient infrastructure and supporting management structure, Evans says.

CISO Role

Neiman Marcus in June launched its search for its first CISO, indicating that the candidate must have eight to 10 years of experience in a significant information security leadership role, according to a job description that was posted to the retailer's website (see: Neiman Marcus Searching for a CISO). In the job posting, Neiman Marcus noted: The CISO will proactively work with business units to implement practices that meet defined policies and standards for information security. The posting also said the CISO needs to be able to work with executive management in determining acceptable levels of risks for the organization (see: Winning Support for Breach Prevention). The security officer's responsibilities will include developing business-relevant metrics to measure the efficiency and effectiveness of the information security program, facilitate appropriate resource allocation and increase the maturity of the program, Neiman Marcus says.

Other duties for the CISO will include: developing and managing information security budgets; creating security and risk management awareness training programs for all employees; providing subject matter expertise to executive management on a broad range of information security standards and best practices; and ensuring security programs are in compliance with applicable laws, regulations and policies.

Breach Details 3

ISSN: 1941-6679-On-line Copy