Journal of Computer Science and Information Technology
June 2019, Vol. 7, No. 1, pp. 1-20
ISSN: 2334-2366 (Print), 2334-2374 (Online)

Published by American Research Institute for Policy Development
DOI: 10.15640/jcsit.v6n2a1
URL: https://doi.org/10.15640/jcsit.v6n2a1

An Exploration of the Evolving Reporting Organizational Structure for the Chief Information Security Officer (CISO) Function

Conrad Shayo[1] & Frank Lin[2]

Abstract

The ideal reporting structure for the Chief Information Security Officer (CISO) function is not yet settled. Should the CISO report to the Chief Information Officer, Chief Operations Officer, Chief Financial Officer, Chief Internal Auditor, General Counsel, or Chief Executive Officer? Although existing literature provides recommended reporting structures of the CISO position, most practitioners and researchers discourage the adoption of a "one size fits all". This study borrows from Complexity Theory and Interaction Theory to shed light on "Why" we may have so many different reporting CISO structures even for companies of the same size in the same industry faced with the same information security risks. Using Complexity Theory, we posit that although the initial CISO reporting structure is unpredictable; organizations as open systems have an inbuilt capacity to self-organize, self-motivate, and learn to adapt the CISO reporting structure to their own work environment. Using Interaction Theory, we posit that the emerging reporting structure is created by the interaction between factors inherent in decision makers of the organization and factors inherent in the CISO function. This implies that ideal reporting structures of the information security organization will inevitably vary according to the organization's industry, mission, maturity, culture, risk exposure, resources, capabilities, and prevailing decision making and governance infrastructure. Using a case study research method, we relied on numerous CISO interviews available on open source and our own interviews of two seasoned CISOs. The study recommends best practices for evolving an effective reporting structure for the CISO function.

Keywords: CISO Reporting Structure, Chief Information Security Officer, Cyber security Governance, CISO Function

1. Background

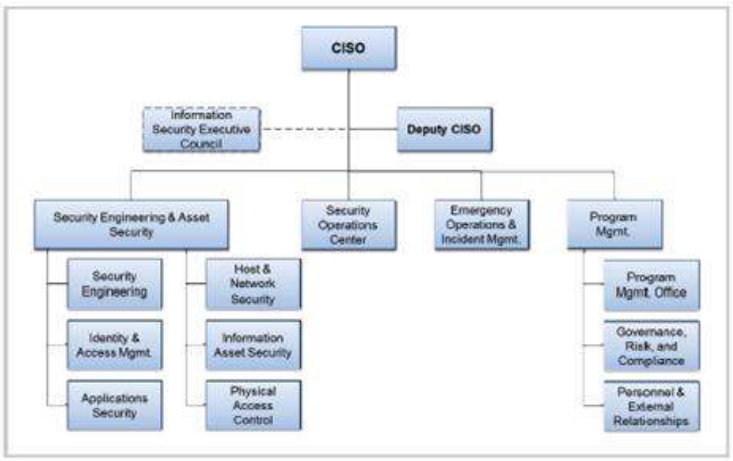
No one knows how many organizations are already being compromised (or will be compromised) by cyber security criminals due to a poor reporting structure of their information security function. Top management in organizations with digital assets coveted by cyber criminals (notably in the financial, retail, and healthcare industries) know that cybercriminals may already be inside their systems waiting to pounce at the right moment. Spectacular hacks looking for customer data and intellectual property are now rampant, with no end in sight. Recently, information security scholars and professionals have advocated the need for a Chief Information Security Officer (CISO) function that directly reports to the Chief Executive Officer (CEO) or the Board of Directors (BoDs), and/or an Information Security Steering Committee (ISSC). There is a clarion call to extend the operational nature of the CISO function to include a strategic leadership role (Aguas, Kark & Francois, 2016),and the CISO should be seen as a technologist, guardian, strategist, and advisor, having a seat at the table of the top management team (TMT) also called the C-Suite (Gesser et al., 2017). And cyber security within organizations needs to be everyone's business – including the board's (Rothrock et al., 2018).

[1] Information and Decision Sciences, California State University, San Bernardino, cshayo@csusb.edu
[2] Information and Decision Sciences, California State University, San Bernardino, flin@csusb.edu

Despite such calls, recent surveys of CISOs and Chief Information Officers (CIOs) by various professional organizations have found that multiple reporting structures still exist for the CISO function (Sales, 2016; Villegas, 2016; Grossman, 2016,; Sparapani, 2017; Vertos, 2018).For example, the Ponemon Institute (2017) found that although 60% of CISOs have a direct channel to the CEO, only 4% of them reported to the CEO. Fifty percent (50%) reported to the CIO, 9% to the Chief Technology Officer, 9% to the Chief Financial Officer (CFO), and 6% to the Chief Operating Officer (COO). The main question asked in the survey related to the reporting structure is: "**Who** do you report to?" The "**Why**" and "**How**" questions have yet to be asked.

Several researchers at the Carnegie Mellon University Software Engineering Institute developed a recommended template structure for the CISO function for use in large organizations (Allen et al. 2015). This recommended structure is shown in Figure 1 below.

Figure 1: Recommended CISO Organizational Structure



The researchers first identified four main functions for the CISO: (1) **Protect**, Shield, Defend, and Prevent, (2) **Monitor**, Detect, and Hunt, (3) **Respond**, Recover, Sustain, (4) **Govern**, Manage, Comply, Educate, and Manage Risk. Second, they identified sub-functions and activities that could be grouped under the four functions before grouping them into proposed departments. Third, they developed the organizational structure shown in Figure 1. The researchers recommended that organizations should use this template to allocate work role duties and responsibilities based on the organizational size, cyber security maturity level, information security requirements, and priorities. What they did not recommend was how to determine to whom the CISO should report. The researchers supported their proposed organizational structure by borrowing from the National Infrastructure for Cyber security Education (NICE) Workforce Framework (National Institute of Science and Technology), The Cyber security Capability Maturity Model (Department of Energy); the National Institute of Science and Technology (NIST) Cyber security Framework, The Computer Emergency Readiness Team (CERT) Risk Management Model, and the Sys Admin, Audit, Network, Security (SANS) Institute Top 20 Critical Security Controls.

This paper is organized as follows. First, we provide a brief review of the CISO literature. Second, we present the research design and discussion of existing theories from social science that help explore how organizations determine the position of the CISO and why. Third, we analyze interviews of thirty seven (37) CISOs and three (3) CEOs obtained from an open source on the Internet, as well as our own interviews of two seasoned CISOs. Lastly, we discuss the findings and provide suggestions for further similar exploratory or confirmatory case study research that could shed more light on our research question.

2. Literature Review

A few academic studies have researched the CISO reporting structure: Karanja & Rosso (2017), Beatty, Arnett & Liu (2005); Johnson & Goetz (2007), Kayworth & Whitten (2010), Ashenden & Sasse (2013) and Allen et al. (2015), Whitten (2008), Kwon, Ulmer, & Wang (2013). Karanja & Rosso (2017) conducted an exploratory study of the CISO reporting structure of firms that hired a CISO between 2010 and 2014. The job data was extracted from LexisNexis Academic Database. They found that new CISO hires tended to report to the CEO, while replacement hires tended to report to the CIO.

They also found that 80% of the firms hired CISOs from outside the organization, with only 20% groomed from within. Of the 80% hired from outside, 49% reported to the CEO, 29% reported to the CIO, and 22% reported to others. Of those who reported to the CEO, 77% occupied a newly created CISO position, and 23% occupied an old position. Of those who reported to the CIO, 37% occupied a newly created CISO position, while 63% occupied an old position.

Two earlier studies found that the CISO position was mostly two levels below the C-Suite (Johnson & Goetz, 2007), and lacked credibility and power (Kayworth & Whitten 2010). Ashenden & Sasse (2013) found that the Audit, Physical Security, and General Counsel functions, in addition to the Information Technology (IT) function, were among the ones yearning to control the Information Security Management function. According to Whitten (2008), the CIO who reports to the CEO is the one who has traditionally been responsible for IT security and the CISO position was created to take over this responsibility because of the current danger of cyber-criminal activities. Some practitioners have argued that since the CIO is already a member of the Top Management Team (TMT) and understands both the technical security and business languages, s/he is the best person to preside over the CISO function. However, other researchers have argued otherwise. A study by Beatty, Arnett & Liu (2005) found that putting the information security role under the CIO maybe too overwhelming for a single person.

A study by Kwon, Ulmer, & Wang (2013) found that firms with CISOs with a seat in the C-Suite and who are able to brief the board, have a low probability of security incidents. Another study found that CISO participation in the C-Suite led to superior organizational IT capability (Lim, Stratopoulos, &Wirjanto 2012). But a recent practitioner study by the Cyentia Institute reported in Dark Reading by Vijayan (2017) that interviewed fifty (50) CISOs, twenty five (25) Corporate Board Members, and ten (10) subject matter experts found that CISOs and C-Suite/Board Members have divergent views on the value of cyber security, how to measure and evaluate risk, and how to assess the effectiveness of information security projects.

Whereas C-Suite directors regarded brand and data protection as the main value of the CISO function to the organization, CISOs regarded their mission as "guiding and enabling the business and ensuring loss avoidance," (Vijayan, 2017; Gaillard, 2015).The same study reported that, whereas 46% of CISOs felt high confidence in their security controls, only 5% of board members expressed a similar feeling. In addition, when it comes to making a business case for the effectiveness of information security projects, CISOs tended to present technical jargon instead of business language. C-Suite and BoD members are left with the impression that it does not matter how much money is spent, the company will still get hacked. The failure of CISOs to communicate clearly to the C-Suite members and BoD has been widely reported. As noted in the Sans 2017 Survey:

> "The ability to communicate threats and security posture, [Cyber Threat Intelligence] CTI reporting and data interpretation will need to improve, including the ability to understand and map vulnerabilities to the threat indicators, new intelligence sources and more."(p. 8)

Although while most CISOs have strong technical skills, with computer science and computer engineering backgrounds, they have been found to lack business and leadership acumen especially when it comes to increasing visibility into threats, listening to the voice of the end users of business applications, and articulating clearly understood solutions to senior management and the board (Sans 2018 Survey).Conversely, professional blogs have reported that top management does not clearly understand or respect how criminals caneasily enter into their businesses by manipulating employees, abusing applications, or exploiting known and unknown vulnerabilities (Sans Survey, 2018).

3. Research design

This study explores how the CISO organization position is determined and why. According to Yin (2009), the "**How**" and "**Why**" questions are more effectively explored using either Experiment, History or Case Study research methods. For example: Why do some organizations have their CISO report to the General Counsel and not to the CEO? Or to the CIO and not the COO? How can we explain this organizational behavior?

Table 1 shows the relevant situations for different research methods based on the research question being asked (Yin, 2009). Selection of the applicable Experimental Research Method for the relevant question(s) is based on the researcher's ability to manipulate the behavioral events or on whether the study focuses on contemporary events. If one is asking a "how" and "why" question but does not have manipulative control, then one would consider using the Case Study Research method.

According to Yin (2009), the components of case study research design are the study's:

1. Questions
2. Propositions or Justification (for Exploratory Study)
3. Unit(s) of analysis
4. Logic linking the data to the research question
5. Criteria for interpreting the findings

3.1. Study's Questions

As mentioned earlier, the purpose of this study is to explore the questions: **How** is the CISO organization position determined and **Why**? To our knowledge, these questions have not been formally addressed before

Table 1: Relevant Situations for Different Research Methods

Research Method	Form of Research Question	Requires Control of Behavioral Events	Focuses on Contemporary Events
Experiment	How, Why?	Yes	Yes
Survey	Who, what, where, how many, how much?	No	Yes
Archival Analysis	Who, what, where, how many, how much?	No	Yes/No
History	How? Why?	No	No
Case Study	How, Why?	No	Yes

3.2. Research Justification

In this exploratory study, we provide justification for the study instead of research propositions as recommended by Yin (2009, p. 22),Gephart, (2004), and Eisenhardt & Graebner, (2007). Although we have found several theories that are helpful in justifying exploring why the reporting CISO function is not settled, we will only focus on two main theories: 3.2.1Complexity Organizational Theory (Anderson, 1999; Brodbeck, 2002), and 3.2.2 Interaction Theory (Markus, 1983).

3.2.1 Complexity Organizational Theory (Anderson, 1999; Brodbeck, 2002)

Complexity organizational theory posits that although systems are unpredictable, they are subject to certain order-generating rules placed upon them to self-organize, self-motivate, and learn in order to adapt to their own environment. Complexity organizational theory can explain the behavior of organizations faced with cyber threats by predicting that existing organizational structures will engage in a process of self-organization, self-motivation, and self-learning to react to the challenge posed by the operating environment. Therefore, the person the CISO reports to now reflects the current maturity level of the organization, i.e., cyber security maturity, power dynamics of the governance structure, existing trust orientation, and organizational knowledge. According to complexity organizational theory, once the organization's cyber security situation changes, the CISO reporting structure will have to adapt.

1. In May 2011 four months after the data breach at Sony, the company hired Philip Reitinger as the new CISO, who was to report to Shinji Hasejima, Sony's CIO. However, in September 2011, Philip Reitinger was named the Senior Vice President and Chief Information Security Officer, the Corporate Executive in charge of global information security and privacy. This could mean that after self-learning and self-motivation, the top management now found it proper to elevate the CISO position by adjusting the existing structure.

   Similarly, at Equifax, the interim CISO Russ Ayres reported to the interim CIO, Mark Rohrwasser; immediately after the data breach, the newly hired CISO reported to the Chief Counsel. Again, according to complexity organizational theory, we could say that self-learning by the organization (Equifax) led to the subsequent assignment of the new CISO function under the Chief Counsel. It is possible that, if it were not for the data breach at Equifax, the CISO reporting structure could have been the same today, i.e. the CISO reporting to the CIO. According to Brodbeck (2002), "complexity theory does have a place in procedural design as a means of leveraging self-organizing and self-motivating behavior for improved organizational performance." Once an organization learns, it will adapt.

   Nevertheless, how can one explain the fact that the CISOs for Target and Home Depot still report to the CIO and not to the CEO or General Counsel, despite the clarion call by IT industry professionals for CISOs not to report to the CIO due to potential conflict of interest and lack of independence? It seems that contingency theory may have its limits and another theory is needed.

2. In December 2013, Target was hit with a data breach where critical customer data and information of up to 110 million people was compromised.

   "Maiorino joins Target effective June 16 and will be responsible for Target's information security and technology risk strategy helping to ensure that the company, its guests and team members are protected from internal and external information security threats. He will report to Bob DeRodes, executive vice president and chief information officer…" (Target, 2014).

3. In September 2014, Home Depot faced the same fate with its 56 million customers`` data and information. Both companies established a new CISO position that reports directly to the CIO.

   "Home Depot Inc., has hired its first chief information security officer. Jamil Farshchi will manage information security, data protection and vulnerability management, a Home Depot spokesperson told CIO Journal. He will report to Chief Information Officer Matt Carey…" (Security-magazine, 2015).

3.2.2. Interaction Theory (Markus, 1983)

Markus (1983) offers a helpful initial point for examining the myriad of reporting structures for the CISO positon. Although her focus was on why people resist the implementation of new information systems, in this paper we will draw on her insights to explain the CISO reporting situation. We first discuss the three components of interaction theory and then discuss the underlying assumptions shown in Table 2. According to Interaction Theory, the CISO reporting structure could be influenced by:

a) Factors internal to an existing influential organizational decision maker or a group of decision makers
b) Factors inherent in the CISO function
c) The interaction between factors internal to the existing organization deciders, and factors inherent in the CISO function

(a) Factors Internal to the Existing Organization Decision Makers

These internal factors may be common to one influential organizational unit decision maker or a group of influential organizational units' decision makers. The theory states that generally, intuitive decision makers will resist all change to the organizational structure, whereas rational analytic decision makers will embrace all necessary change, the main driver being the individual or group of individuals' beliefs about change. For example, a CIO may resist having a CISO report to her for fear of being fired if a data breach occurs or a vulnerability is missed (Goel, 2017; Drinkwater, 2016). Similarly, the whole C-Suite may want cover by having the CISO report to lower levels of the organization.

"Whatever an organization's reporting structure, the bottom line is the same: the responsibility for everything that happens within the organization, positive or negative, ultimately falls on the CEO and the board of directors. This includes data breach responsibility. This has been reflected in the numerous CEO firings (or "resignations") that have followed bad breaches over the past few years, including those at Target [and] Sony Pictures ..." (Lazarus Alliance, 2017)

(b) Factors inherent in the CISO function

Factors inherent in the CISO function could be the inherent bias of the C-Suite that CISOs are technical people with computer science and computer engineering degrees who do not understand the business or that cyber security exposure is something that will always be there, so, "why bother?" Another reason could be the bias that the only thing CISOs are good at is spreading FUD (Drinkwater, 2016). One dismissed CISO had this to say:

"The IT director constantly ignored the advice of information security, thought that he knew better, and while telling the board that we should improve, undermined my position by telling my peers to let me fail, as he just did not like what I did …..This resulted in a complaint to HR against my director, for conduct unbecoming a director and also a breach of our corporate ethics policy.
HR brushed it under the carpet. A month before my two-year employment period, where employment law would have protected me with unfair dismissal, I was dismissed."(Drinkwater, 2016)

(c) The interaction between factors internal to the existing organizations' unit decision maker(s), and factors inherent in the CISO function

An influential decision maker or a group may resist a new organizational CISO structure due to an interaction between the characteristics related to decision makers and the characteristics related to the person in charge of the CISO function. There are two views of this interaction theory: (a) the social-technical view and (b), the political view.

(i) The Social Technical View stipulates that the introduction of a new CISO position with new job roles, division of labor, the subsequent need for coordinating and communicating security behaviors across the organization may be perceived as creating new responsibilities inconsistent with the existing order. There could be fear that the new position "may structure patterns of interaction that are at odds with the prevailing organizational culture" (Markus, 1983, p. 431). The greater the perceived disruption of the old order, the greater the chance that the new CISO will remain reporting to lower than one level away from the C-Suite executives. Similarly, a reverse FUD factor against the CISO will occur if the CISO is seen as unable to communicate clearly with the C-Suite executives on how the organization can increase its security posture and remain profitable.

(ii) The Political View stipulates that the reporting structure of the CISO could be influenced by the perceived interaction between the new CISO position and the prevailing "organizational distribution of power defined objectively in terms of horizontal or vertical power dimensions, or subjectively in terms of symbolism," (Markus, 432). In a crisis, the CISO may have to assume authority to ensure a swift resolution, so working through reporting lines and hierarchies is not always efficient. A security function can only work if connected with the rest of the organization through more than just reporting lines (Berlitch, 2015). A CISO will undoubtedly shake up the way the organization behaves on micro and macro scales. If you don't want your new CISO to recommend and implement real organizational change for the sake of security then wait until your company is prepared (and eager) to put words into action before adding a CISO to your executive team (Terrill, 2016). It may also be the case that a new CISO position is created immediately after a spectacular data breach as a public relations stunt to mitigate the effects of declining market valuation, loss of customers, or legal action. In this case, should any other data breach or missed vulnerability occur, the CISO becomes the fall guy (Drinkwater, 2016). Most likely, if a CISO is hired for political reasons, s/he will be fired for political reasons. The main questions to ask here are: Why is a new CISO position being created? How is the decision made? Who makes the decision? Who has the authority to fire the CISO? Who is going to be the truth teller when an incident occurs?

As eloquently described by a CISO:

"Sometimes firing a CISO...is purely for optics; a company has to show the public they are taking action…termination can take effect even if the data breach was not directly attributable to the CISO"(Violino, 2017).

Both the Social Technical and Political views suggest that different reporting structures could emerge from similar circumstances. Interaction theory has the potential to provide more precise explanations and predictions of the positioning of the CISO reporting structure.

3.2.2.1 The Underlying Assumptions

In order to compare the theories that attempt to shed light on causes (why) of the existing reporting structures for the CISO function, it is important to discuss the underlying assumptions about the nature of the organizational environment in which the CISO function is introduced.

3.2.2.1.1 Assumptions about the Nature of Organizations

Organizations in which a new CISO function is created can be described by:

Structure: functional, divisional, matrix or project based
Culture: power, role, task, person, entrepreneurial
Employment Contracts: Duties, Dismissal, Vicarious Liability, Compensation, Negligence, Human Rights

In our case, the Rational Theory of Management will assume that all employees will share the common goal of securing and protecting the organization's digital assets and will work together to accomplish that goal. The mission of the CISO function is protecting the organizational assets against internal and external threats and providing the organizational stakeholders with a peace of mind if information security incidents occur.The non-rational view will assume that different employees or employee groups in the organization may have different goals depending on their rank in the organizational hierarchy and that, in general, they may try to pursue their personal goals (to look good) rather than the overall organizational goals whenever there are differences (Markus, 1983).

One example could be a CEO avoiding placing the CISO function under his/her direct report because of fear of job security when a data breach occurs. This means that there will be occasions when some organizational members will not adhere to the rational view.

Table 2: Underlying Assumptions of Interaction Theory in the Structuring of the CISO Function

	People Determined	Structurally Determined	Interaction Theory
Causes of CISO reporting structure	Factors inherent in an Organization's Unit Decision Maker or Collective Decision Group • Personality traits Human nature	Factors inherent in the CISO Function • FUD (Fear, Uncertainty, and Doubt) factor • Does not know the business side Just another IT guy	Factors inherent between the characteristics of the organization's decision maker(s) and factors inherent in the CISO function Sociotechnical View: • Interaction between the CISO function with division of labor Political View: • Interaction of the CISO function with distribution of intra-organizational power
Assumptions about the nature of organizations	Organizational information security goals are shared by all participants	Organizational information security goals are shared by all participants	Sociotechnical View: • Goals are conditioned by history Political View: • Goals differ by organizational position; conflict is inevitable
Assumptions about having a CISO function	If the purposes of having a CISO are consistent with the Rational Theory of Management, then we can exclude this from further consideration	If the purposes of having a CISO are consistent with the Rational Theory of Management, then we can exclude this from further consideration	Sociotechnical View: • The purpose of the CISO function maybe to change organizational culture, not just work flow Political View: • The CISO function maybe intended to change the balance of power
Assumptions about the reporting structure of the CISO function	Reporting structure for the CISO is determined by factors inherent in the organizational unit decision maker(s); undesirable	Reporting structure for the CISO is determined by factors inherent in the CISO function as seen by current decision maker(s); undesirable	Reporting structure is a function of the current situation, existing decision maker(s), and industry influences; each of which is neither desirable nor undesirable

3.2.2.1.2. Assumptions about having the CISO Function

Although the Rational Theory of Management will assume that a CISO function is critical given current high profile data breaches and serious information security incidents, the non-rational view could be that top management unjustifiably views CISOs as FUD mongers, and that they are just 'techies' who think they know everything but in reality they do not understand the business side of things.

"And when it came to the skills gap within their security professionals, the weak spot was ability to understand business, cited by 72 percent of respondents, with 42 percent mentioning communication – but just as worrying for a profession that prides itself on technical ability, technical skills were also cited as a weakness by 46 percent of execs. And IT leaders themselves think that more than 29 percent of their teams need to be replaced to drive digital transformation and increase productivity…" (Morbin, 2016)

"CISOs are now expected to understand and articulate the business risk of cyber-threats to a non-tech audience, become educators for both the board and the workforce as a whole, liaise with and reassure compliance officers and be aware of legal and regulatory obligations…So the CEO, the CIO and the rest of the board can't offload all tech risk – but its potential impact is too great, so they need high-level informed advice to aid decision-making and prioritize expenditure." (Morbin, 2016)

3.2.2.1.3. Assumptions about the reporting structure of the CISO Function

Ideally, the CISO reporting structure should be placed where it is most effective in protecting the organization. However, evidently, this is sometimes not the case. As one CISO lamented:

"Often the CISO is put in an organization where there is a conflict of interest, e.g. they may report to a CIO or CTO who has very different incentives." (Morbin, 2016). This may not be intentional, though. It could reflect ignorance on the part of the organizational decision makers on the optimal location of the CISO function, inadequate exposure to the level of cyber security risk the organizational may be exposed to, or even fear of being associated with a function

that has such severe consequences should something go wrong. In this case, the capability maturity level of the organization may be very low. Another assumption is that it is more beneficial to have the CISO report to the CIO because it is more operationally sound, with both speaking the same language. However, as one information security consultant commented, there is the risk of conflicts of interest:

"A common structure is CISO reporting to CIO. This structure has advantages, such as a deep integration into the IT organization, potentially reducing friction with IT service delivery, as the security function is not seen as an outsider. On the other hand, it risks a conflict of interest, if not collusion, as both the security function and IT service delivery are under the same budget and presumably the same goals." (Berlitch, 2015)

Now we turn to the discussion of the unit(s) of analysis, logic linking the data to the research question, and the criteria for interpreting the findings.

3.3. Unit(s) of analysis

The study is designed as a multiple case design with several units of analysis. We use interview data from 36 current and past CISOs and 3 CEOs. Archived data of 37 interviewees was obtained from open sources on the Internet. These include O'Connor, (2018a-g); Info Sec Institute (2010, 2012a-d, 2013, 2017a-d); and Cybereason, (2017), among others. We also conducted two additional CISO interviews of our own. See Appendix 1.

In the case research design, each organization for which the CISO or CEO worked is a single case study. The unit of analysis is the information provided by the interviewee (CISO or CEO).

3.4. Logic Linking the Data to the Research Question

The authors readall of the interviews' information and identified statements made that focused on:

a) Factors related to Complexity theory [CT]
b) Factors internal to the existing organization Decision Maker(s)[DM]
c) Factors inherent in the CISO function [CISO]
d) The interaction between factors internal to the existing organizations' unit decision maker(s), and factors inherent in the CISO function [INT]

The statements were then coded for each factor. Sometimes one statement covered multiple factors. See Exhibit #3. The frequencies of similar statements repeated by the interviewees were also counted to establish replication and to point to chain of evidence.

3.5. Criteria for Interpreting the Findings

Complexity Theory: If the interviews provide a high frequency of statement related to the need to change the CISO reporting structure based the organization's cyber security continuous maturity, then we will generalize our findings to Complexity Theory.

Interaction Theory: If the interviews provide a high frequency of statement related to factors internal to existing organizational decision makers, the CISO function and the interaction between factors related to the existing organizational decision makers and the CISO function, then we will generalize our findings to Interaction Theory.

Interview data coding: As mentioned above, the units of analysis were thirty seven (37) CISO interviews and three (3) CEO interviews.

The interviews were carefully read, looking for statements that related to the CISO work role, the knowledge skills and abilities they ought to have, perceptions of CEOs about CISOs and vice versa, perceptions of CISOs about CIOs and BoDs, and what all interviewees thought the reporting structure of the cyber security function in the organization ought to be.

Exhibit 1 provides a coded list (A thru AM) of the CISO/CEO interviewees along withtheir current or previous organizational affiliations. It also provides a count of the statements an interviewee deemed critical for the CISO function.

Exhibit 2 provides a list of statements obtained from reading the 40 interviews along with check marks for each statement related to any of the three factors of Interaction Theory [Decision Maker (DM), CISO, and Decision Maker/CISO interaction (INT)] or related to Complexity Theory (CT).

The authors first did the coding in Exhibit 2 independently. The first pass achieved an inter-rater reliability of 80%. After discussions, the second rating achieved a 98% inter-rater reliability. Finally, Exhibit 3 contains the Coded Interviewees (A through AM) and a count of the statements made by each interviewee.

Results and analysis

Complexity Theory (CT). As shown in Exhibit 2, fourteen statements (33% of the 42), are related to CT. These are statements related to how CISOs and CEOs help their organizations to self-organize, self-monitor and learn to cope with their operating cyber environments. The top four (4) out of the 14 statements with highest agreement among the interviewees include having a CISO who:

a) Holds meetings with individuals and focus groups and tells the story of why information security is important to every individual and group in the organization (Statement #4, with 65% interviewee agreement) (henceforth, Statement #4, 65%)
b) Speaks the language of business (Statement #3, 43%)
c) Develops and implements a well-planned, understood and rehearsed incident response plan (Statement #12, 15%) and
d) Develops an accountability and responsibility chart for all key stakeholders on what each one should do in case of a breach (Statement #13, 10%)

Analysis of the 14 statements indicates that effective CISOs should 'have the ability to':

- Understand the organization and its business
- Understand how employees use sensitive data and where the sensitive data is located
- Prepare the organization for quick recovery should a breach incident occur and
- Create a culture of shared responsibility and accountability should a breach occur

Proposition #1: CISOs perceived to have a high ability to help the organization adapt its strategic information security posture to its operating cyber security environment will most certainly be held in high regard and placed at a higher reporting level in the organizational structure.

Interaction Theory (DM, CISO, INT).

DM: As shown in Exhibit 2, five statements (11.9% of the 42), are related to DM. These are statements related to how internal factors relate to an influential organizational decision maker or how a committee may influence the placement of the CISO position in the organization structure. The top four (4) out of the five(5) statements with highest agreement among the interviewees include:

a) The C-Suite and BoDs seeing CISOs as insurance "Political Pawns" to be thrown out when a breach occurs--regardless whether they are at fault or not… (Statement #31, 13%),
b) CEOs having the perception that CISOs do not understand the business (Statement #8, 8%)
c) Perception of the CISO as someone who says "no" automatically to any risky project (Statement #17, 5%), and
d) Perception by CEOs that the CISO is not protecting business processes from harm, rather preventing the business processes from being done (Statement #15, 5%)

Analysis of the five statements using a Text Analyzer from Online-Utility.org indicates that CISOs should:

- Manage the CEO perceptions by demonstrating an understanding of business with credentials/testimonials from referees, mentors and academic training
- Show willingness to engage all stakeholders in the organization including the CEO, the C-Suite and BoDs on the roles they should play in managing cyber risk just as they manage the other risks, be they financial, project, legal, or strategic
- Allay the fears of whistle blowing by committing to transparency and fearless truth telling on cyber security matters
- Be willing to educate the CEO and the C-Suite/BoDs on best cyber security practices and the importance of shared accountability and responsibility during the job interview
- Letting it be known clearly the conditions upon which s/he will be willing to accept the job offering—that s/he is not desperate to get the job

Proposition #2: A CISO who does not manage CEO perceptions (and those of the other influential stakeholders) during the job interview by demonstrating a deep understanding of business and communicating how s/he intends to transparently lead the cyber security function will most certainly be placed at a lower reporting level in the organizational structure.

CISO: As shown in Exhibit 2, twelve statements (28.6% of the 42), are related to CISO. These are statements related to how internal factors related to the CISO function to influence the placement of the CISO position in the organization structure. The top five (5) out of the 12 statements with highest agreement among the interviewees include:

a) The CISO must have the ability to speak the language of business (Statement #3, 43%),
b) CISOs should acquire the necessary knowledge to continuously demonstrate ROI on existing and new security assets-- audit existing security assets to make a case for their continuing usefulness (Statement #21, 18%)
c) CISOs have the perception that CEOs do not understand information security (Statement #8, 8%)
d) CISOs should know where the sensitive data is located and whether money and time is being spent to secure such data and whether it is located internally or in the cloud (Statement #26, 8%)
e) CISOs should demonstrate that Information Security can manage KPIs just as the rest of the business and able to increase (or decrease) spend according to business risks-- BoDs understand numbers, they will focus on them more (Statement #27, 8%)

Analysis of the 12 statements indicates that CISOs should:

- Provide leadership for the cyber security function through a well-articulated evidenced based strategic business vision
- Make a business case for cyber security using business language – e.g. how the Key Performance Indicators (KPIs) aligned with the Critical Success Factors (CSFs) will be impacted by a cyber-breach
- Play the role of an educator, mentor, supporter, enabler and problem solver
- Be a continuous learner from personal mentors, business leaders, and fellow CISOs

Proposition #3: A CISO who does not learn to speak the language of business while at the same time demonstrate technical ability to lead the cyber security function will mostly put under the CIO.

INT: As shown in Exhibit 2, twenty-six statements (61.9% of the 42), are related to INT. These are statements related to the interaction between factors internal to the existing organization decision makers **(DM)**, and factors inherent in the CISO function **(CISO)** coded **INT**. The top five (5) out of the 12 statements with highest agreement among the interviewees include:

a) The CISO holds meetings with individuals and focus groups telling the story of why information security is important to every individual and group in the organization (Statement #4, with 65% interviewee agreement) (henceforth, Statement #4, 65%)
b) The CISO must have an understanding of the voice of the end user-- how end users use systems (Statement #2, 40%)
c) The CISO must have a keen interest in both the operational (perimeter security, secure gateways, remote access services) and the resiliency side of things-- due to lack of appreciation of the capabilities of threat actors (Statement #1, 38%)
d) CISOs should have the ability to demonstrate the evolving information security defense posture-- a cultural, risk and control framework of how current and future threats are identified, isolated and controlled-- How you are going to keep things moving?(Statement #29, 33%)
e) CISOs should help the organization to have a well-developed, understood and rehearsed Incident Response Plan-- BoD, TMT, and all organization employees including the emergency security readiness team should understand it (Statement #12, 15%)
f) CISOs should help develop and articulate an accountability/responsibility chart for all key stakeholders if an incident happens (BoDs, TMT, security team, end users)-- During an attack, only a practiced seriously process can save you (Statement #13, 10%)

Analysis of the 26 statements indicates that CISOs should:

- Not forget that the mission of the CISO function is to provide the organizational stakeholders with peace of mind on cyber riski.e., the knowledge that the organization and its assets (company and customer data, Intellectual Property) are well protected against internal and external threats.

- Demonstrate leadership by providing a well-developed, understood and rehearsed framework for Incident Response Plan-- BoD, TMT, and all organization employees including the emergency security readiness team should understand it and practice it periodically.
- Listen to and understand the voice of the users of the organization's digital assets, which includes employees, supply chain partners, competitors, regulators, and even hackers.

Proposition #4: A CISO who demonstrates effective leadership of the cyber security function by providing peace of mind for organizational stakeholders and translating cyber security investment into tangible business outcomes will most certainly be provided a seat at the C-Suite and welcomed to the BoD boardroom.

A further noun-verb analysis of the 42 statements using a Text Analyzer (https://www.online-utility.org/text/analyzer.jsp) from Online-Utility.org reveals that the most repeated verbs are: a CISO **must have** the ability to communicate, listen, speak, perceive, and engage. In addition, s/he should seek, understand, lead, help, provide, protect, and secure. These seem to be the most important attributes CISOs must have in order to perform their rightful craft. The most repeated nouns include information security, CEO, BoD, end users, business, cyber security maturity, security, assets, Top Management Team, data, risk, incident, and customer. These seem to represent the most important mix of ingredients the CISO should work with to deliver security value to the organization.

Discussion

The findings of this study shed light on the unsettled nature of the reporting structure of the CISO position in organizations. The emerging four propositions show that it is possible to generalize the interview statements to the tenets of Complexity Theory and Interaction Theory. These two theories are therefore relevant in exploring how the reporting structure of the CISO function is determined and why. The main drivers of whether the CISO reports to the CEO are: the cyber security maturity of the organization, perceptions of CISOs and CEOs about the nature of cyber risk, the knowledge CISOs have about the business, the knowledge of CEOs have about cyber security, and the respect CISOs and CEOs have for each other and the cyber hackers. The higher the cyber security maturity of the organization, the better the understanding of the CISO and CEO about the nature of cyber risk and the damage cyber hackers can cause to the survival of the organization. However, CISOs must prove that they understand their craft and they belong to the C-Suite:

> "For CISOs the corporate culture is the most important thing to understand, align to and integrate with. They need to understand the business and not fall back on the jargon-laced language of the security department that causes eyes to glaze in the boardroom. To establish themselves as allies and partners to the board, CISOs need to embrace a new set of language and business skills. There is no silver bullet to bridge the culture gap that currently exists between CISOs and the board, and right or wrong, it's not going to happen unless the CISO can prove that he or she is worthy of that respect and authority."(Curry, 2016)

When the C-Suite and the BoDs assume accountability for cyber security, they are most likely to require the CISO to belong to the C-Suite. If the organization does not have a CISO with the required knowledge and skills, they will most certainly hire one externally. The CEO will most likely learn more about cyber risk and the CISO will most likely learn more about the business. Cyber risk becomes just one of the business risks the CEO needs to manage.

Limitations and Suggestions for Further Study

The main limitation of this exploratory study is that the study did not directly interview C-Suite or BoD members who have been directly involved in recruiting and determining the CISO position. This would have allowed us to learn how each company actually determined the reporting structure. The exploration relied mostly on open source CISO and CEO interviews. An argument can be made, however, that before embarking on an explanatory study of how the reporting structure of the CISO is determined and why, it may be beneficial to conduct an exploratory study and develop initial propositions first. Further studies should be done by interviewing CEOs or BoD members directly. Another limitation is that it is extremely difficult to ascribe motivation for a specific reporting CISO structure (Markus, 1983). Although we observe CISOs, CSOs, and sometimes CIOs being the first to be fired or step down when a breach occurs, as was the case with Equifax, it is difficult to know for sure whether the CEO or BoDs, avoided accountability, purposefully to contrive the reporting structure. Nonetheless, one can argue that the claim made by professionals in the information security industry that any CISO 'should be thankful to make it through a year without being a sacrificial lamb' is not without merit. Further studies should be made to confirm this from candid CEOs, even if confidentially.

References

Aguas, T., Kark, K.& François, M. (2016).The new CISO: Leading the Strategic Security Organization. Deloitte Review, Issue 19: 2016. Retrieved from https://www.deloittereview.com.

Allen, J.H., Crabb, G., Curtis, P.D., Fitzpatrick, B., Mehravari, N., Tobar, D. (2015). Structuring the Chief Information Security Officer Organization. CMU Software Engineering Institute, Technical Note CMU/SEI-2015-TN-007. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

Anderson, P. (1999). Complexity Theory and Organization Science. Organization Science. 10(3), pp. 216-232.

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

Beatty, C.R., Arnett, K.P. & Liu, C. (2005). CIO/CTO Job Roles: An Emerging Organizational Model. Communications of the IIMA, 5(2), pp. 1 – 10.

Berlitch, P. (2015). For Security, Organizational Structure May be Overrated. Retrieved from https://www.infosecurity-magazine.com/blogs/organizational-structure-overrated/

Brodbeck, P.W., (2002) Complexity theory and organization procedure design. Business Process Management Journal, 8(4), pp.377-402Retrieved from http://resources.infosecinstitute.com/interview-j-wolfgang-goerlich-cyber-security-strategist-for-creative-breakthrough/

Curry, S. (2016). Bridging the Communications Gap between the CISO and the Board. Retrieved fromhttps://www.scmagazine.com/bridging-the-communications-gap-between-the-ciso-and-the-board/article/578046/

Drinkwater, D. (2016).These CISOs explain why they got fired: Sometimes the chief security officers become the fall guy. Retrieved from https://www.csoonline.com/article/3057243/security/these-cisos-explain-why-they-got-fired.html

Eisenhardt, K. M. & Graebner, M. E. (2007). Theory Building from Cases: Opportunities and Challenges. Academy of Management Journal,50(1), pp. 25–32.

Gaillard, J.C. (2015). Information Security: The Reporting Line of the CISO is Key to Success. Retrieved from https://corixpartners.com/information-security-the-reporting-line-of-the-ciso-is-key-to-success-blog/

Gesser, A., Grinberg, R., Garmon, J. & Tippett, E.A.(October 2017) After Equifax, to Whom Should the CISO Report? David Polk Data Breach Center. Retrieved from https://www.cyberbreachcenter.com/2017/10/after-equifax-to-whom-should-the-ciso-report/

Gephart, R. P. (2004).Qualitative Research and the Academy of Management Journal. Academy of Management Journal, 47(4), pp. 454–462.

Goel, V. (2017).Yahoo's Top Lawyer Resigns and C.E.O. Marissa Mayer Loses Bonus in Wake of Hack. The New York Times. Retrieved from: https://www.nytimes.com/2017/03/01/technology/yahoo-hack-lawyer-resigns-ceo-bonus.html

Grossman, S. (2016). Chief Information Security Officers should be reporting to Chief Risk Officers. Retrieved from: https://www.securityweek.com/chief-information-security-officers-should-be-reporting-chief-risk-officers

Security Magazine(2015).Home Depot Names New CISO. Retrieved from https://www.securitymagazine.com/articles/86248-home-depot-names-new-ciso

InfoSecInstitute. (2010). Interview with Mike Rothman. Retrieved from http://resources.infosecinstitute.com/interview-mike-rothman/

InfoSecInstitute. (2012a).Interview: Jeff Snyder. Retrieved from http://resources.infosecinstitute.com/interview-jeff-snyder/

InfoSecInstitute. (2012b). CISO Series: Richard Bejtlich. Retrieved from http://resources.infosecinstitute.com/ciso-series-bejtlich

InfoSecInstitute (2012c). CISO Interview Series – Michael Peters. Retrieved from http://resources.infosecinstitute.com/ciso-interview-michael-peters/

InfoSecInstitute. (2012d). CISO Interview Series- Doug Steelman: CISO Dell Secure Works. Retrieved from http://resources.infosecinstitute.com/ciso-interview-series-doug-steelman/

InfoSecInstitute. (2013). Retrieved from http://resources.infosecinstitute.com/fortune-500-interview-scotiabanks-greg-thompson-talks-hackers-cyber-terrorists-hacktivists-and-more/

InfoSecInstitute (2017a)Interview: Recruiter and Career Coach Jeff Snyder. Retrieved from. http://resources.infosecinstitute.com/interview-jeff-snyder-2/

InfoSecInstitute (2017b). Interview: Chris Rouland. Retrieved from http://resources.infosecinstitute.com/interview-chris-rouland/

InfoSecInstitute (2017c). Interview: Bob Chaput, CEO of Clearwater Compliance. Retrieved from http://resources.infosecinstitute.com/interview-bob-chaput-ceo-of-clearwater-compliance/

InfoSecInstitute (2017d). Cyber security: An Interview with Chief Information Security Officer, Agnes Kirk. Retrieved from https://watech.wa.gov/about/news-room/news/interview/cybersecurity-interview-chief-information-security-officer-agnes-kirk

InfoSecInstitute (2018). Expert Interview: How to Launch an Effective Security Awareness Training Program. Retrieved from http://resources.infosecinstitute.com/expert-interview-launch-effective-security-awareness-training-program/

InfoSecInstitute (2017e). A CISOs biggest concern? Better alignment between security and business. Retrieved from https://www.cybereason.com/blog/a-cisos-biggest-concern-better-alignment-between-security-and-business.

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 Information Security Officer: An Exploratory Study. Journal of International Technology and Information Management, Vol. 26(2). pp. 23 – 47.

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

Kwon, J., Ulmer, J. R., & Wang, T. (2013). The Association between Top Management Involvement and Compensation and Information Security Breaches. Journal of Information Systems: 27(1), pp. 219-236.

Lazarus Alliance (2017). Data Breach Responsibility: Who Takes the Fall When a Company Gets Hacked? Yahoo Is Trying to Pass the Buck, but Data Breach Responsibility Starts at the Top. Retrieved fromhttps://lazarusalliance.com/data-breach-responsibility/

Lim, J. H., Stratopoulos, T. C., and 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), pp. 21-40.

Markus, M.L. (1983). Power, Politics, and MIS Implementation. Communications of the ACM, Vol. 26(6).

Morbin, T. (2016). The changing role of the CISO. Retrieved from https://www.scmagazineuk.com/the-changing-role-of-the-ciso/article/532261/

O'Connor, F (2017a). Cybereason CISO Interview Series: Taking Acceptable Risk for Acceptable Return. Retrieved from https://www.cybereason.com/blog/blog-cybereason-ciso-interview-series-taking-acceptable-risk-for-acceptable-return

O'Connor, F (2017b). Cybereason CISO Interview Series: The End Of The CISO? Retrieved from https://www.cybereason.com/blog/blog-cybereason-ciso-interview-series-the-end-of-the-ciso

O'Connor, F (2017c). A CISO's biggest concern? Better alignment between security and business. Retrieved from https://www.cybereason.com/blog/a-cisos-biggest-concern-better-alignment-between-security-and-business

O'Connor, F (2017d). Cybereason CISO Interview Series: Security From the Inside Out. Retrieved from https://www.cybereason.com/blog/blog-cybereason-ciso-interview-series-security-from-the-inside-out

O'Connor, F (2017e). Cybereason CISO Interview Series: The CISO as A Business Enabler. Retrieved from https://www.cybereason.com/blog/the-ciso-as-a-business-enabler

O'Connor, F (2017f). Cybereason CISO Interview Series: Why storytelling matters in security. Retrieved from https://www.cybereason.com/blog/blog-stories-from-the-front-lines-of-security-leadershipjohn-knights-information-security-officer-at-wentworth-institute-of-technology

O'Connor, F (2018g). Cybereason CISO Interview Series: Security's Appeal Lies in The Challenge. Retrieved from https://www.cybereason.com/blog/cybereason-ciso-interview-series-jason-callahan-illumina

Penomon Institute Security Report (2017). The Evolving Role of CISOs and their Importance to the Business. Retrieved from: https://f5.com/Portals/1/PDF/labs/Evolving_Role_of_CISOs_Aug2017.pdf?ver=2017-09-18-100218-007

Rothrock, R.A., Kaplan, J. & Van Der Oord, F. (Winter 2018). The Board's Role in Managing Cyber security Risks. MIT Sloan Management Review, 59(2), pp.12-15.

Sales F. (May 2016). MIT CIO: The CISO reporting structure needs to change. Tech Target Network. Retrieved from http://searchcio.techtarget.com/blog/TotalCIO/MIT-CIO-The-CISO-reporting-structure-needs-to-change.

Sans Institute (2017). Cyber Threat Intelligence Uses, Successes and Failures: The SANS 2017 CTI Survey. Retrieved from: https://www.sans.org/reading-room/whitepapers/analyst/cyber-threat-intelligence-uses-successes-failures-2017-cti-survey-37677

Sans Institute (2018). CTI in Security Operations: SANS 2018 Cyber Threat Intelligence. Retrieved from: https://www.sans.org/reading-room/whitepapers/threats/cti-security-operations-2018-cyber-threat-intelligence-survey-38285

Security Magazine (2015). Home Depot Names New CISO. Retrieved from: https://www.securitymagazine.com/articles/86248-home-depot-names-new-ciso

Sparapani,J. (August 2017). Digital security puts CISO reporting structure in corporate glare. Tech Target Network. Retrieved from https://securityintelligence.com/where-the-ciso-should-sit-on-the-security-org-chart-and-why-it-matters/.

Target, (2014). Target Names Brad Maiorino Senior Vice President, Chief Information Security Officer. Retrieved from https://corporate.target.com/press/releases/2014/06/target-names-brad-maiorino-senior-vice-president-c

Terrill, C. (2016). How to Tell When Your Company Should Hire A CISO. Retrieved from Retrieved from https://www.forbes.com/sites/christieterrill/2017/01/19/how-to-tell-when-your-company-should-hire-a-ciso/#74f770831db6

Text Analyzer. Online-Utility.org Retrieved from (https://www.online-utility.org/text/analyzer.jsp)

Veltsos, C. (2018). Where the CISO Should Sit on the Security Org Chart and Why It Matters. Retrieved from https://securityintelligence.com/where-the-ciso-should-sit-on-the-security-org-chart-and-why-it-matters/

Vijayan, J. (2017). CISOs, Board Members Have Widely Divergent Views on Cyber security Retrieved from https://www.darkreading.com/operations/cisos-board-members-have-widely-divergent-views-on-cybersecurity/d/d-id/1328674?

Villegas, M.O. (October, 2016). Breaking down the CISO reporting structure. Retrieved from http://searchsecurity.techtarget.com/tip/Breaking-down-the-CISO-reporting-structure

Violino, B. (2017).5 missteps that could cost CISOs their jobs. Retrieved from https://www.cso.com.au/article/630297/5-missteps-could-cost-cisos-their-jobs/

Whitten, D. (2008). The Chief Information Security Officer: An Analysis of the Skills Required for Success. The journal of computer information systems. 48(3), pp.15-19.

Yin, R. (2009). Case Study Research: Design and Methods, 4th Edition, Sage Publications, California: Thousand Oaks.

Appendix 1: Interview with a ciso
Interview #1

What do you consider the appropriate title for the person performing information security function in an organization?

The title is not important if the person is empowered to do the job; i.e.; safeguarding the organization's information assets. The ideal person should have the technical know-how, politically savvy, and be trusted. No matter what the title is, the information security person should have the responsibility of educating the governance team, including the board of directors, on information security matters. S/he should be a member of the organization's Executive Policy Security Team. There must be an uninterrupted trust between the information security person and top management. Real trust. I know this organization --- and I support it with full commitment to its mission and value proposition.

What do you consider the greatest challenge for an ISO?

Most organizations do not have a strategic information security plan that governs business processes of the organization. If you join such a strategic-less organization, you will be stepping on a land mine. Information security has not truly made sense in most organizations. The ISO must not only keep top management and the Board of Directors and Executive Policy Security Team informed on what the ongoing risks are, but also what breaches have happened and when. They should know about attempted breaches, and how to fend off future offensives. That way, "the team together can make a collective decision on how they respond to those types of things."

How should organizations go about recruiting and retaining ISOs?

Glad you asked this question. I think organization should consider grooming their own ISO internally as part of their strategic succession plan. Anyone coming from without will most certainly have a steep learning curve understanding the culture and creating trusting relationships with management. It really takes time to create a governance structure that truly believes that security is part of the organization's DNA.

- Finding the person from the organization will also not be easy. It takes time to groom the person from inside. It

should be a continuous quest for succession planning. The climate should be such that top management and the support personnel should all want the ISO to succeed. Not only the ISO by the way, but also with each other and for each other.

- On assuming the job, there will be the familiar group dynamics of forming, norming, storming, and fully functioning security aware implementing cohesive organization--- everyone playing their part—very strong support.

What do you consider the ideal ISO?

Somebody with the desire to continuously learn, with high technical and people skills, highly knowledgeable about the security domain and the human condition—why humans behave the way they do. A mentor and teacher. Humble. Someone who values the organization unconditionally. Total belief in the organization they work for…. Total employee <-> organization loyalty, and a feeling of job security. Employable… has merit and can find a job elsewhere when she/he feels compromised. Highest level of integrity and has ability to keep secrets. Ability to empower her/his crew i.e., the working family. Always supporting the information security culture and ownership in the organization.
Educational:

- Desire to educate other people to their level of competence
- Use the Enterprise Information Security Architecture to identify what data needs to be protected and why, how the data should be protected and where, who should protect it and when.
- Oversee Operating System and Application hardening, traffic monitoring, host/network Intrusion Detection, virus protection schemes
- Constantly improve: themselves, organizational culture, team
- Open to the idea that you do not know everything
- A consummate change agent in both theory and practice
- Open to other people's ideas
- Willingness to take calculated risks

What does information security culture and ownership in the organization mean?

It is for the leader in this role to do "Whatever it takes" to profile, secure, protect, monitor the information assets of the organization, "to do right", "be a truth teller" even if it hurts.

In addition, what should be done in times of budget cuts that may affect information security resources?

You must provide the best professional recommendation. You indicate the impact of each of the cuts, and have the governing board (top management) decide where the cuts will be and the risks that come with that. "Sure, if I don't have the money, I will do it cheaper… but top management should support the consequences of the cheaper option…" Every option should be on the table in plain view for the consideration of top management and the Executive Policy Security Team. Find a way to say "Yes" only to empower the organization. Uncompromising when it comes to implement lousy ... cookie cutter solutions… I think Zachman had it right on the need to use his proposed architectural framework to govern risk.

Moreover, there is need for independence… just as an internal auditor is. And it does not matter what the title of the auditor is, or whom they report to exactly, so long as they have the resources to do their job thoroughly, completely, in accordance with company policy, the law, and generally accepted auditing principles.

What additional training you lacked as a CISO and would you recommend for any future CISO?

I should have taken a course on budget management. In this role, a CISO should have 100% Budgetary Transparency—

You need to watch the Science Fiction Movie-- Wing Commander. "You are going to burn out my planes…" You need an organization security leader who is not afraid to play the role of a 'conscientious objector'… One that is respected by her/his independence not by position… One who could say I do not have to have the job I have… One who is frankly ready to tell the truth from the point of view of the organization's mission, vision and values (MVVs); one who will have best solutions (alternatives) on the table for given budgetary resources …

- The organization needs to identify people with those characteristics, groom them, place them, mentor them…

- Character is rarely fully vetted during an interview process
- There must be full unconditional Board and Executive Management support

INTERVIEW #2

How is the CISO position determined and why?

In higher education, there is not consistency. Even within the California State University system 23 campuses about one third (33%) of the CISOs report to the Chief Financial Officer (CFO) and the other two thirds (67%) report to the Chief Information Officer. Here I report to the CIO but I have a dotted line to the President (CEO). In the case of CISOs who report to the CFO, it is possible that they are embedded to another level, the Chief Risk Officer (CRO), who reports to the CFO. Remember, the information security function was a sub-function under the CIO. Therefore, when we had high profile hacks, starting from 2001, the C-suite and BoD started to pay attention and upgrade this function to a higher level.

I report to the President on business matters and to the CIO on the technical aspect. On the technology side is about information security operations—patching, perimeter security, hardening stuff, remote access, etc.). I serve at the pleasure of the President who determined who I should report to. Of course, the President would have had counsel to determine that.

Therefore, what do you think about the future of CISO reporting structure?

I think as the maturity of the information security function in enterprises continues to increase, moving from technical to strategic and compliance CISOs will gradually have independence and not report to the CIO or any other function but directly to the CEO with a dotted line to the BoDs. However, it will take time. If you had asked me this question in the early 2000s, I would not have answered it this way. It will take time for organizations to mature – maybe in the next 10 years or so.

How do you resolve the conflict of interest between the CIO and the CISO?

Conflicts of interest are everywhere. For example, Internal Audit reports to the CFO, the same with the Chief Risk Officer reporting to the CFO. Moreover, it is the CFO and the rest of the C-Suite that has to take risk in order to make money.

The CISO and CIO should talk to each other, but it is a delicate situation when the CIO has self-interest based on how s/he is evaluated. For example, s/he may bring a solution that requires a single sign on (SSO) rather than multifactor authentication. Although the CISO may point out the security risks involved to the CIO, the CIO may be under pressure to get the application. He wants to look good. There is need to cooperate.

Therefore, it seems a CISO must have a strong personality and strong backbone to get his way.

Since the CIO understands the implications of security breaches, the relationship would be less combative. Only the President can fire me. The CIO can only recommend my firing. And if I am fired, I go back to teaching, no problem.

How about accountability in case of a breach?

In the past, it was easy to just fire the CISO when there is a breach, chapter closed. Now things have changed. There is more accountability now. If money was withheld to implement a necessary security project, that will be documented. If I do an audit and recommend to the CIO that specific patches to be done and it turns out hackers got in through the unpatched servers, then the accountability rests with the CIO.

As I said, when a breach happens, even if the CISO is fired, the reputations of the CIO, CFO, and CTO are also tarnished.

What is the future of Cyber security in Higher Education?

Best practices are now emerging. For Example, some campuses are decoupling Security and Privacy governance. Check the University of Berkeley structure—they have Data Privacy and Security Law Compliance separate from Information Security Operations Assessment and Compliance. This I think is the wave of the future. You build governance structures around the areas where failure can occur. See ECAR report from Educause to get more information about CISO reporting structure in higher education.

Exhibit 1. List of Interviewees

Interviewee Name	Organization (Current or Previous)	Position	Code	#*
John Knights	Wentworth Institute of Technology	CISO	A	5
Sue Bergamo	Epserver	CIO/CISO	B	18
Sam Curry	Cybereason	CSO	C	3
Agnes Kirk	State of Washington	CISO	D	3
Doug Steelman	Dell Secure Works/DoD	CIO/NW Defense Director	E	4
Rick Howard	Palo Alto Networks	CSO	F	1
Jeremiah Grossman	WhiteHat Security	CEO	G	1
J. Thompson	Rook Security	CEO	H	2
Kurt Roemer	Citrix	Chief Security Strategist	I	1
Christopher Pierson	Viewpoint	CISO/General Counsel	J	2
Mike Rothman	Securosis	President	K	4
Richard Bejtlich	Mandiant	CSO	L	3
Jeff Snyder	SecurityRecruiter.com	President	M	3
Andrew Rose	The National Air Traffic service- UK	CISO	N	8
Michael Lambert	Ministry of Agriculture--Quebec	CISO	O	2
Jeffrey Guy	Carbon Black	Senior Director	P	2
Tod Fitzgerald	Grant Thornton	CISO	Q	1
Mieke Kooij	Trainline	Security Director	R	3
Becky Pinkard	Pearson	Security Director	S	2
Troels Oerting	Barclays	CSO	T	3
Lee Barnery	Marks & Spenser	Information Security Head	U	3
Elena Kvochko	Barclays Group Security	CIO	V	3
Julie George	Arriva	CISO	W	4
Mark Jones	Heathrow	CISO	X	6
Graham Wright	National Grid	CISO	Y	7
Richard Spearman	Vodafone	Corporate Security Director	Z	5
Xavier Leschaeve	Remy Cointreau	CISO	AA	2
Nic Wells	Arriva	CISO	AB	4
Rod Wallace	Pearson	CISO	AC	1
Julia Harris	Post Office/ex-BBC/Oxfam	CISO	AD	3
Jimmy Bashir	DWP	CISO	AE	3
Drazen Morog	Deutsche Bahn	CISO	AF	4
James Christiansen	Visa/GM/Experian	CISO	AG	5
Todd Bell	Big O Tyres	CISO	AH	4
Ken Deforges	City of Diamond Bar	CISO/CIO	AI	8
Javier Torner	California State University	Information Security Director	AJ	17
Greg Thompson	Scotia Bank	VP Enterprise Security	AK	6
Bob Chaput	Clearwater Compliance	CEO	AL	6
J. Wolfgang Goerlich	Creative Breakthrough Inc.	Cybersecurity Strategist	AM	10

Exhibit 2. Interviewee Statements with Coded Contributing Factors (Decision Maker, CISO, Decision Maker/CISO, Complexity Theory)

Interviewee Statement	DM	CISO	INT	CT
1. The CISO must have a keen interest in both the operational (perimeter security, secure gateways, remote access services) and resiliency side of things-- due to lack of appreciation of the capabilities of threat actors			✓	
2. The CISO must have an understanding of the voice of the end user-- how end users use systems			✓	
3. The CISO must have the ability to speak the language of business-- currently they lack the leadership and communication skills to articulate a coherent information security strategy to the TMT and BoD due to not understanding the business, its purpose, its destination		✓		✓
4. Inability to tell the story of why information security is important to everybody-- tailor the message to each stakeholder group, to their own personal lives, build relationships knowing that each employee, customer, vendor, partner, have the potential for deliberately			✓	✓

or unwittingly harming the organization				
5. The CISO must have the ability to lead the information security function without resorting to the FUD (Fear, Uncertainty and Doubt) factor			✓	
6. CISOs should have visibility and avoid keeping a low profile -- operating behind the scenes			✓	
7. CISOs should seek a mentor, or give back by mentoring and helping others to network		✓		
8. CISOs have the perception that CEOSs do not understand information security and CEOs have the perception that CISOs do not understand business	✓	✓		
9. A CISO should have an understanding that s/he has to enact policies that protect corporate assets but keep them running at the same time-- being open and willing to work with the business areas			✓	
10. CISOs should not place a dividing line between the CIO and the CISO functions when they actually occur simultaneously			✓	
11. CISOs should avoid introducing something that is leading edge, just because it is leading edge			✓	
12. CISOs should help the organization to have a well-developed, understood and rehearsed Incident Response Plan-- BoD, TMT, & all organization employees including the emergency security readiness team should understand it			✓	✓

Legend:

Factors related to Complexity theory [CT]
Factors Internal to the Existing Organization Decision Makers [DM]
Factors inherent in the CISO function [CISO]
The interaction between factors internal to the existing organizations' unit decision maker(s), and factors inherent in the CISO function [INT]

13. CISOs should help develop and articulate an accountability/responsibility chart for all key stakeholders if an incident happens (BoDs, TMT, security team, end users) -- During an attack, only a process practiced seriously can save you...(B)			✓	✓
14. CISOs should listen to the internal customer's business needs-- revenue, cost, employee efficiency, etc. (B)			✓	
15. Perception by CEOs that the CISO is not protecting business processes from harm, rather preventing the business processes from being done	✓			
16. CISOs should be transparent, hold open discussions communicating how he/she can be helpful and supportive-- thus not creating a collaborative atmosphere		✓		
17. Perception of the CISO as someone who says no automatically to any risky project	✓			
18. A perception that CISOs think they have all the answers rather than relying on a broader team		✓		
19. CISOs trying to do it alone (I know it all) rather than getting second opinions and knowing that there are many companies out there that can help a company minimize information risk		✓		✓
20. CISOs perceived as not protecting what matters by knowing where data is, how it should be used, who is using it, and who should use it			✓	
21. CISOs should acquire the necessary knowledge needed to continuously demonstrate ROI on existing and new security assets-- audit existing security assets to make a case for their continuing usefulness		✓		
22. Perception that CISOs lack the understanding what the problem (threat) is, and how to solve the problem using the best means possible		✓		
23. CISOs should have the knowledge of how to patch things up without interrupting the business or getting exploited by an unpatched application			✓	
24. Knowing that the CISO job is a high anxiety job-- leading to high turnover (13 to 18			✓	

months)				
25. CISOs should have the ability to frame things in terms of risk and business enablement to help enable a better conversation with the board		✓		
26.CISOs should have a visibility of where the sensitive data is located and whether money and time is being spent to secure such data whether it is located internally or in the cloud		✓		✓
27. CISOs should demonstrate that Information Security can manage KPIs just as the rest of the business and able to increase (or decrease) spend according to business risks-- BoDs understand numbers, they will focus on them more...(H)		✓		✓
28. CISOs should compartmentalize policy essential for protecting data, networks, devices, sensitive applications, usage and privacy			✓	
29. CISOs should have the ability to demonstrate the evolving information security defense posture-- a cultural, risk and control framework of how current and future threats are identified, isolated and controlled-- How you are going to keep things moving?			✓	✓
30. CISOs should have the ability to have the C-Suite and BoDs acknowledge and accept risk			✓	
31. CISOs seen as insurance "Political Pawns" for the TMT members to get thrown out when a breach occurs-- regardless whether they are at fault or not…	✓			
32. CISOs should consider the size, context, and cybersecurity maturity of the company as factors in the types of information services CISOs should seek-- i.e., every organization handles security differently, based on its needs, maturity and internal structure(K)			✓	✓
33. CISOs should understand that intrusions are inevitable, prevention eventually fails, and the best way to start a real security program is to determine if you are currently compromised			✓	✓
34. TMT and BoD worrying about whistleblowers reporting intrusion to the SEC or the public when boards or TMT fails to report incidents in disclosure documents	✓			
35. Top Management Team & BoD hiring a CISO shortly after a data breach as a way to protect themselves			✓	
36. TMT & BoD members being driven by personal financial and work tenure considerations when deciding on the CISO position-- only 4% of CEOs think they are accountable if a hack occurs compared to 14% of CISOs			✓	
37. It does not really matter who the CISO reports to as long as the organization's information assets are secure-- maybe promote the CISO to the CIO position -- which provides both the technical security and business needs understanding			✓	✓
38. The conflict of interest between the CISO and CIO can affect the effectiveness of the CISO function-- the person responsible for ensuring organizational information security cannot be subordinated to the person responsible for technology selection and implementation-- (a) placing under the CEO is the best option but most expensive, (b) placing in a position within a department where there is no conflict of interest, e.g. Operational Risk Department, (c) placing under the CIO as an additional role has potential for conflict is the cheapest solution for small organizations or ones with lower cybersecurity maturity level			✓	
39. Not realizing that if you only love technology and you are not a good communicator, empathizer, and someone who understands business, then the CISO role is not for you		✓		
40. CISOs should realize that all companies are different, and that once you understand the voice of the internal customer, "go at the pace your company would like to see…"			✓	✓
41. Not realizing that when there is a breach, it is not only the reputation of the CISO that is tarnished even if s/he is fired, but also the entire organization and its leadership (CEO, CIO, CFO, CTO, BoDs)			✓	✓

42. CISOs should create an infrastructure that provides the ability to analyze large amounts of data emanating from the intrusion detection/prevention systems to establish potential patterns			✓	✓
Total	5	12	26	14
Percentage	11.9%	28.6%	61.9%	33.3%

Exhibit 3. Coded Interviewees and Count of Statements Mentioned in Interview (See Exhibit 2)

Code	Statements Mentioned	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
A	**5**	1	1	1	1	1																																					
B	18				1		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1																			
C	3				1																			1	1																	
D	3				1					1			1																													
E	**4**												1										1						1	1												
F	1																					1																				
G	1																										1															
H	2																					1						1														
I	1																												1													
J	2			1	1																																				
K	**4**				1								1																		1	1										
L	3	1																																1	1							
M	3		1	1	1																																					
N	8	1	1	1	1																	1				1			1							1						
O	2																														1					1						
P	2								1																													1				
Q	1																																					1				
R	3		1	1	1																																					
S	2	1		1																																					
T	3																												1		1					1					
U	3	1																											1										1			
V	3	1			1							1																														
W	**4**				1																	1				1			1												
X	6	1		1	1		1							1																	1										
Y	**7**		1	1	1	1																1							1											1		
Z	**5**	1	1		1									1															1												
AA	2	1			1																																				
AB	**4**		1	1	1																	1																			
AC	1													1																												
AD	3				1	1																						1													
AE	3		1	1	1																																					
AF	**4**		1	1	1																								1												
AG	**5**	1	1	1	1																								1												
AH	**4**		1	1	1																																			1		
AI	8	1	1	1	1										1		1												1											1		
AJ	17	1	1		1					1	1	1	1		1	1		1									1		1	1	1	1	1	1						1		
AK	6	1	1	1	1																					1																1
AL	6	1	1	1	1																								1			1										
AM	10	1	1	1	1			1	1	1			1									7				1			1												
Total	**172**	**15**	**16**	**17**	**26**	**3**	**2**	**2**	**3**	**4**	**2**	**3**	**6**	**4**	**3**	**2**	**2**	**2**	**1**	**1**	**1**	**7**	**2**	**1**	**1**	**2**	**3**	**3**	**2**	**13**	**1**	**5**	**3**	**2**	**1**	**1**	**2**	**1**	**1**	**1**	**3**	**1**	**1**
		38%	40%	43%	65%	8%	5%	5%	8%	10%	5%	8%	15%	10%	8%	5%	5%	5%	3%	3%	3%	18%	5%	3%	3%	5%	8%	8%	5%	33%	3%	13%	8%	5%	3%	3%	5%	3%	3%	3%	8%	3%	0.6%