Defining the Strategic Role of the Chief Information Security Officer

Sean B Maynard
School of Computing and Information Systems,
University of Melbourne, Australia
sean.maynard@unimelb.edu.au

Mazino Onibere
School of Computing and Information Systems,
University of Melbourne, Australia
mazino.onibere@unimelb.edu.au

Atif Ahmad
School of Computing and Information Systems,
University of Melbourne, Australia
atif@unimelb.edu.au

Abstract

The level of sophistication and dynamism of the security threat environment requires modern organizations to develop novel security strategies. The responsibility to strategize falls to the Chief Information Security Officer (CISO). A review of the security literature shows there has been little emphasis on understanding the role of the CISO as a strategist. In this research, we conduct a systematic literature review from the disciplines of information security and strategic management to identify specific attributes required by CISOs to become effective strategists. We discuss these attributes in the context of Information Security Management and argue that CISOs with these attributes or capabilities are better positioned to overcome the existing strategic security challenges facing organizations.

Keywords: Information Security; Information Security Strategy

Citation: Maynard, S. B., Onibere, M. and Ahmad, A. (2018). " Defining the Strategic Role of the Chief Information Security Officer, " *Pacific Asia Journal of the Association for Information Systems, 10*(3), pp. 61-86.
ISSN 1943-7536(print) / ISSN 1943-7544(online)
Copyright © Association for Information Systems.
DOI: 10.17705/1PAIS.10303

Introduction

Recent Advanced Persistent Threat (APT) and ransomware attacks suggests the modern information security threat environment continues to evolve at an alarming rate. The shifting landscape represents greater risk exposure to the information infrastructure of organizations that translates to interruption or destruction of IT networks and systems, loss of revenue and competitive advantage, disclosure of sensitive information, reputational damage, and other costs arising from breaches of confidentiality agreements and loss of productivity (Ahmad et al. 2014a). The risks to organizations have thus become significantly heightened and require novel information security strategies that recognise the complexity of the prevailing threat environment. As a result, organisations are increasingly hiring chief information security officers (CISOs) (Karanja and Rosso 2017). The CISO is gaining a presence in the boardroom, is rising to the level of other C-level executives and has greater input into strategy than ever before (Alexander and Cummings 2016; Dawson et al. 2010).

The CISOs primary objective is to develop organizational-level security strategies that are flexible, adaptable and readily modifiable in commensuration with the dynamic and volatile risk environment, while at the same time aligning with the business strategy. A strategist develops and drives the implementation of strategies that enable organizations to achieve their goals and objectives (Dillen et al. 2018).

A review of the security literature, however, reveals: (1) that the field of information security management has little strategic perspective; (2) that organisations face a number of strategic challenges around the ISM function; and (3) that a dearth of research exists focusing on security leaders functioning at the strategic level. Additionally, there is a lack of consensus on the need for the CISO position in terms of their strategic role in the organization which may explain why CISOs struggle to gain credibility amongst their peers in the C-level executive (Karanja 2017; Karanja and Rosso 2017). We believe that these flaws point to the need for a stronger case to be made justifying the strategic role of the CISO in organizations. We therefore ask the following research question:

What capabilities are required by the chief information security officer to effectively function as a strategist?

Consequently, we have identified five requisite dimensions to the strategic role of the CISO. We argue that with these five dimensions the CISO will be able to overcome the existing strategic challenges facing ISM in organizations.

The paper is organized as follows. First, we discuss the missing strategic perspective of ISM and the resulting ISM strategic challenges. Next, we identify and develop the five dimensions of the strategist based on thematic analysis of characteristics and qualities of strategists extracted from strategic management literature. We then discuss how CISOs exhibiting the competencies defined within the five dimensions will be able to overcome the ISM strategic challenges. Finally, we conclude the paper with contributions and directions for future research.

Information Security Management Strategic Challenges

Information Security Management (ISM) is responsible for the lifecycle of the information security function within an organization. This includes identification of relevant information assets, determination of possible and probable threats, selection of appropriate safeguards, and ensuring the effective and efficient implementation of selected safeguards. Our review of security literature reveals a grouping of activities that make up the lifecycle of the information security function within organizations into practice areas such as security policy management, security risk management, and security education and training (Alshaikh et al. 2014; Alshaikh et al. 2018). While the focus of this paper is

DOI: 10.17705/1pais.10303

on strategic competencies of the CISO, existing ISM practice areas only focus on operational responsibilities of the CISO, revealing an apparent lack of strategic perspective.

The following are challenges currently faced by ISM within organizations because of the missing strategic perspective of the ISM function. We have put together these challenges based a number of key themes brought up by several authors. The strategic nature of these challenges has in part motivated the need for CISOs with strategic perspective.

Evolving Threat Landscape Requires an Innovative Strategy

Traditionally, information security involved identifying information assets, and applying corresponding preventative security measures which were contingent on clearly distinguishable boundaries and perimeter (Durbin 2011). However, advancements in Information Technology (IT) have led to the rise of boundary spanning technologies and trends, which have blurred the lines of boundary around company information assets. Thus exacerbating the risk of leakage of sensitive information (Ahmad et al. 2014a).

Furthermore, previously threats were known, predictable, opportunistic and driven by the need for adventure and *bragging rights* by the attackers; however, nowadays, threats have become unpredictable, novel and the motivation behind attacks have shifted to mainly financial gain (Smiraus and Jasek 2011; Sood and Enbody 2013; Tankard 2011). Attackers are no longer youngsters, computer whiz kids or any of the other stereotypes associated with hackers. Rather, they are increasingly organized syndicates and nation states with considerable resources at their disposal, seeking to steal information as part of economic or industrial espionage, and/or covertly sabotage critical infrastructure as part of cyber warfare (Schiavone et al. 2014; Webb et al. 2017). Security strategies that were effective in the past, based on a static selection of preventative safeguards now need to be re-evaluated vis-à-vis the current dynamic environment and sophisticated threat landscape (Baskerville et al. 2014).

Security Strategy Requires a Holistic Organizational View

Despite the increasing recognition of the role of Information Security in protecting an organization's information assets, and the corresponding increase in security spend (Hall et al. 2011), ISM is still seen as a mostly technological problem with many of the standards and best practices being technological in nature. These do not adequately address the human aspects of information security even though strong evidence exists that humans are the weakest link (Karanja 2017). Consequently, the strategic business context within which the organization's information assets are utilised is lost (Kayworth and Whitten 2010). ISM may not have adequate understanding of the business and/or a good background in strategy to appreciate and engage with the business direction, which is essential to an effective security strategy (Sveen et al. 2009). Without this strategic and business context, ISM activities are skewed towards the operational with a systems-view, resulting in a narrow fit. This operations-focused ISM is thus reactive in nature and does not support the long-term orientation of the organization. Further, a system-centric view lacks alignment with the business objectives. However, there are increasingly more calls for ISM to be holistic and to focus on the security throughout the organization (Brooks et al. 2018). *An effective security strategy therefore requires a holistic view of the organization's information assets and a recognition of all organizational capabilities.*

Response to Strategic Change Requires Situational Awareness

As part of operational requirements, ISM responds to security incidents and technological changes within the organization. However, the ISM function has no strategic response requirements.

Strategic response is the ability to recognise changes in the organization's environmental context or to any of the parameters considered during strategy development and to be able to respond accordingly by modifying strategy. In contrast, incident response is operational in nature and has the goal of recovery from incidents, restoration of service and in some cases forensic investigation (Tøndel et al. 2014).

Ahmad et al. (2015) argue that though security incidents and seemingly innocuous anomalies are operational, they may be pointers to new patterns of attacks and threats, which may have strategic implications. If organizations rigorously investigated and learned from these incidents and anomalies, they would acquire situational awareness, which is the quality of being aware of and knowing the immediate and future implications of what is happening around you (Webb et al. 2014). Situational awareness increases ability to detect and identify changes in the environmental context, and thus strengthens the organization's capacity for strategic response.

Unfortunately, as Ahmad et al. (2015) demonstrated in an in-depth case study, even best-practice organizations are not necessarily learning from incidents. Because of poor situational awareness, ISM is not able to respond to changes in the security environmental context within which the organization is operating. This poor situational awareness results in blind spots in security risk management, such that security controls are selected without appropriate reference to the organization's actual context (Franke and Brynielsson 2014; Webb et al. 2014).

Security Strategy Transcends Compliance

Security strategy developed with the sole intent of satisfying compliance requirements does not translate to an effective security posture (Le 2017). ISM becomes a compliance problem in organizations that do not recognise the relevance of security and the role it should play but are rather compelled by regulatory and legal requirements to implement security controls (Shojaie 2018; Tan et al. 2003). Organizations derive security requirements from a number of sources such as operational, legal, contractual, regulatory, and competition requirements. Compliance appears to be compelling due to the known fact that lack of adherence results in clearly understood penalties. Security requirements and risks arising from other sources are left out, consequently, risk management assumes a technological orientation; and risk assessments are performed without appropriate reference to the organization's actual situation (Webb et al. 2014).

When this occurs, the CISOs either may turn to their technological expertise in creating a technologically focused security program or may adopt 'best-practice' international standards and security frameworks such as the ISO 27001 and PCI DSS as part of their security program without a contextual understanding of the organization and the prevailing security threat landscape. This response results in a static security posture that does not take into cognisance any change in environmental context.

Security Strategy Requires Effective Communication

Ashenden (2008) alludes to a communication gap between ISM and senior management or board members of an organization. This gap in turn results in further dissociation of the security function from the business – strengthening the perception that security is a technological subject that should be delegated or relegated to the technical people. Von Solms and Von Solms (2004) argue that one of the ten deadly sins of information security is not realising security is a business issue rather than a technological one.

Furthermore, Alshaikh et al. (2014) identified the ISM practice of intra-organizational liaison which involves communication, collaboration and coordination activities between security management and other functional parts of the organization such as human resources

DOI: 10.17705/1pais.10303

and finance, as a strategic challenge. This practice relates to the case study in Ahmad et al. (2015) where it was observed that members of a particular group or unit tend to focus narrowly on their own objectives and tend to be insular about other units and teams. Further, that teams do not readily disseminate information to one another within the organization often leading to communication breakdown.

Lastly, creating a culture of security and realising desired behavioural change within the organization requires effective communication (Karyda 2017; Ruighaver et al. 2007; Tang and Zhang 2016). Unfortunately, inadequate communication with employees by ISM has been the norm in that security leaders have relied on one-way communication to broadcast security messages to the people with no appropriate means of obtaining relevant feedback (Ashenden and Sasse 2013). Communication sits at the heart of transformation, and if an organization would transform because of its experiences and learnings, then there must be effective communication and collaboration. CISOs need to communicate with senior management, other functional areas and to all employees of the organization. Poor communication within security management affects the security posture of the organization.

Methodology

In this research study, we assessed publications from both security literature and strategic management literature using the systematic literature review technique (based on Mathiassen et al. 2007). We used the Scopus online database to search for the relevant terms, because of its overall coverage of academic journals and conferences, including those in information systems, management and security. We initially performed a search in the information security management literature to identify the role of the information security manager. Table 1 summarises the search steps and results (see column "A – Information Security"). We were only able to find 15 articles that had some information about the information security manager's role as a strategist, even after broadening our search criteria.

Table 1: Summary of search process

Selection Step	**A - Information Security**	**B - Strategic Management**
Step 1: Broad search of Scopus	**A1:** Keywords: ("*information security manager"* AND "*strategist")* (0 articles)*;* "*role"* AND ("*information security manager")* (84 articles) and ("r*ole"* AND "*CISO")* (30 articles after removing duplicates from previous search) – **Total security articles: 115**	**B1:** Keywords: "*role"* AND "*strategist"* (**188 strategic management articles**)
Step 2: Selection of appropriate articles	**A2:** Identify papers from step A1 that discuss the roles of the security manager via reading the abstracts and skimming the papers (**13** / 115 articles selected)	**B2:** Identify papers from step 1 that discuss the role of the strategist vie reading the abstracts and skimming the papers (**42** / 188 **strategic management articles identified**)

Step 3: Search for additional papers	**A3:** Keywords: ("IT Security manager" OR "CISO" OR "information security manager") AND ("*role" OR "functions")* (4 additional articles were found)	
Step 4 Selection of appropriate articles	**A4:** Identify papers from step A3 that discuss the roles of the security manager via reading the abstracts and skimming the papers (3 / 4 selected) – **Total security articles: 16** / 119	
Step 5 Forward and Backward Chaining	**A5:** Using forward and backward chaining we did not find any articles that were not already in our result set.	**B5:** Using backward and forward chaining, we identified, by title, a further **27** articles
Step 6 Selection of appropriate articles		**B6**: Identify papers from step B5 that discuss the role of the strategist via reading the abstracts and skimming the papers (16 / 27 selected) – **Total strategic management articles: 56** / 215
Step 7: Final selection of articles	**A7:** Fully read all articles (from step A2 and A4) and select relevant ones based on the discussion of the role of CISO"s (identified SS articles) – **Total security articles: 15** / 16	**B7:** Fully read articles (from step B2 and B6) and select ones relevant to the characteristics of a strategist (**Total strategic management articles: 35 /** 56)

Subsequently, the Strategic Management literature was used to determine the role of the strategist in business. Column "B – Strategic Management" in Table 1 summarises the search in the strategic management literature. We identified 35 articles that describe the role of a strategist in organisations.

Step 1 of each search was a keyword search of the Scopus database, searching all fields in the articles. Step 2 was to skim the titles and abstracts of each article to determine its fit within this study. Step 3 and 4 were a further search and selection using broader search terms in information security management, as the initial search did not return large numbers of articles. Steps 5 and 6 used backward and forward chaining to identify any articles that were valid, that we did not have in our result set. In the information security literature, we were unable to find more articles that were not in our result set, however in the strategic management literature we identified a further 16. The final step, step 7, was a thorough read of the articles where we determined the validity of each article in full. At the end of our article search and selection process, we identified 15 information security management articles that discuss of the role of CISO's, and 35 Strategic Management articles that focus of characteristics of a strategist. A complete list of the articles used in this review can be seen in Appendix 1.

We extracted relevant *words, phrases and sentences* describing the roles of security leaders from each security literature article. These were used in a thematic analysis to create a concept matrix (see Webster and Watson (2002, p. 17). As we analysed each article, themes were developed and placed in a concept matrix in order to better group and present the key concepts uncovered (see Appendix 2 for the

DOI: 10.17705/1pais.10303

concept matrix of the security literature). The analysis of the extracted texts revealed that the discourse on security management roles is predominantly from a functional or 'practice' point of view, rather than in terms of competencies. We found no practice area for strategizing or development of security strategy. Similarly, we extracted relevant *words, phrases and sentences* describing characteristics of strategists from each strategic management literature article. We analysed the extracted texts using the same thematic analysis technique as above. Subsequent to the analysis we were able to group the strategic management articles into five categories. We named these categories of similar macro competencies as the *five dimensions of the strategist*.

Findings

This section presents the synthesised findings from the literature review. The first section presents findings from security literature; and the second section, findings from management literature.

Role of the Chief Information Security Officer

Security leaders are required to understand the organization and industry they are in (Johnson and Goetz 2007; Whitten 2008) for them to be successful in the ISM practice areas. By this understanding, they are able to appropriately identify the assets that require protection, can determine to a reasonable extent the threat landscape and thus can attempt to create value through security for the organization. Security executives are required to maintain a focus on the business objectives and continually seek ways to better integrate security needs into business processes and objectives, aligning security strategy with business goals (Alexander and Cummings 2016; Ashenden 2008; Ashenden and Sasse 2013; Dawson et al. 2010; Lindup 1996; Moon et al. 2018; Whitten 2008).

The CISO has the responsibility for designing, implementing and managing security safeguards and countermeasures based on risk management. Thus the CISO, as any other management function, is required to optimally configure and allocate available security resources for effective and efficient security function Alexander and Cummings (2016); (Ashenden 2008; Ashenden and Sasse 2013; Dawson et al. 2010; Karanja 2017; Karanja and Rosso 2017; Williams 2007). They must also be able to deploy a number of differing security strategies (Ahmad et al. 2014b; Johnson and Goetz 2007) and have the power to put these into practice (Steinbart et al. 2018).

Communication lies at the heart of a number of activities required by the ISM practice areas. CISOs are required to have good communication, collaboration and influential skills, such that they are able to work with other business leaders and secure support from senior management and/or board when required and also influence employee behaviour (Alexander and Cummings 2016; Ashenden 2008; Ashenden and Sasse 2013; Choi 2016; Fitzgerald 2007; Johnson and Goetz 2007; Karanja and Rosso 2017; Whitten 2008; Williams 2007).

Gap in Security Literature on the CISO as Strategist

Though scholars referred to security strategy and aligning security strategy with business strategy, we found no formal recognition of security strategy as a security management practice area. Furthermore, very little has been mentioned about the role of the CISO as a strategist and security strategizing activities; and very little has been mentioned about CISO competencies required for effective development and execution of security strategies.

The concept of strategy and the role of the strategist in strategy formulation and execution is an established and well-articulated subject in strategic management literature. Hence, we turned to strategic management literature to examine the characteristics required for a good strategist and related these to the security executive.

Strategic Management Literature Perspective of a Strategist

Our review of strategic management literature revealed a number of characteristics and qualities of a strategist, which we have synthesised and condensed into the five dimensions of the strategist.

The Dimension of Thought

A strategist is a visionary who sees a world others are unable to see, is a ground breaker, and builds great organizations (Dillen et al. 2018; Hinterhuber and Popp 1992; Hunsicker 1980; Mintzberg 1996; Ringland 2003; Rohrbeck and Gemünden 2011). Strategists are required to use their creativity and imagination to develop strategies and also shape contexts that underpin decision making structures for strategy formulation and implementation processes (Austen Johnson 2007; Grazzini 2013). Strategists are not only great conceptualisers in that they are capable of generating ideas (Dew 2007; Fortino 2008; Kets De Vries 2007), they are also masters of the creative art of synthesising different ideas into one strategy (Mintzberg 1994), often through the process of abduction (Dew 2007). Strategists are innovation catalysts (Barry et al. 1997; Rohrbeck and Gemünden 2011; Smaltz et al. 2006); and their actions precipitate the creation of new possibilities for the organization (Carter et al. 2011). They never stop trying to understand the evolving environment (Critelli 2005). The strategist is a person with the capacity to think laterally and abstractly (Kets De Vries 2007). While lateral thinking allows the strategist to adopt novel approaches in solving problems, with abstract thinking they are able to see beyond the obvious and identify patterns that signify bigger and less apparent issues. The strategist reaches beyond the boundaries of the normal, thinking out-of-the-box (Hautz 2017; Kets De Vries et al. 2010), to break new ground and generate value and growth for the organization (Kets De Vries 2007). They also have the ability or realise and reflect on ethical situations (Behnam and Rasche 2009). Table 2 shows a summary of the Dimension of Thought.

Table 2: Capabilities of the Dimension of Thought

First-Order Capabilities of a Strategist	References
Ability to conceptualise	Critelli (2005); Dew (2007); Fortino (2008); Kets De Vries (2007); Mintzberg (1994)
Ability to think creatively	Austen Johnson (2007); Grazzini (2013)
Ability to think imaginatively	Hautz (2017); Kets De Vries et al. (2010); Kets De Vries (2007)
Ability to think abstractly and laterally	Kets De Vries (2007)
Ability to think to think and devise new solutions without having all facts	Barry et al. (1997); Carter et al. (2011); Dillen et al. (2018); Hinterhuber and Popp (1992); Hunsicker (1980); Mintzberg (1996); Ringland (2003); Rohrbeck and Gemünden (2011); Smaltz et al. (2006)
Ability to realise and reflect on ethical situations	Behnam and Rasche (2009)

DOI: 10.17705/1pais.10303

The Dimension of Contextualisation

The strategist must be able to place strategy in context (Fortino 2008). They must juxtapose their dreams and visions of the future with the prevailing environmental context while keeping the long-term objectives in sight (Hinterhuber and Popp 1992). Effective strategists are those who by reason of being immersed in the day to day activities have acquired sufficient awareness of the organization's operational environment and are able to abstract strategic information therefrom (Mintzberg 1994). They have achieved contextual awareness, which is valuable in crafting and refining strategy. The effective strategist is one who is able to shift easily between different levels of analysis, from the level of details to the level of big picture and vice versa, as required; and be able to identify patterns and recognise causal relationships within the environmental context of the organization (La Paz 2017; Watkins 2012). In the same vein, the strategists must maintain keen awareness of the environment in which the organization is operating, which allows them to be poised and ready to identify any strategic changes that may present a new opportunity or threaten existing position (Barry et al. 1997; Hinterhuber and Popp 1992; Montgomery 2008). They are required to identify strategic changes that occur in the environment such as introduction of new technologies or adoption of new practices by the competition, and be able to determine the corresponding effects on the organization's strategy (Carter et al. 2011; Cattani et al. 2017; Dragoni 2011; Gavetti 2011). Table 3 shows a summary of the Dimension of Contextualisation.

Table 3: Capabilities of the Dimension of Contextualisation

First-Order Capabilities of a Strategist	References
Ability to recognise and place strategy in the organisational context	Fortino (2008); Hinterhuber and Popp (1992)
Ability to assume a holistic/big-picture view	La Paz (2017); Mintzberg (1994); Watkins (2012)
Ability to maintain a keen awareness of environment	Carter et al. (2011); Cattani et al. (2017); Dragoni (2011); Gavetti (2011); La Paz (2017); Watkins (2012)

The Dimension of Execution

The work of the strategist does not end with the articulation of vision and high level strategy, rather, the strategist is required to translate the vision and high level strategy into an actionable plan (Angwin et al. 2009; Rohrbeck and Gemünden 2011; Van Rensburg et al. 2014). In this dimension, the strategists are action-oriented and are required to bring into reality the visions of the desired future. They give action to the dimensions of thought and contextualisation.

Not only do they engage in strategic planning plan, they also drive the implementation of the plan, steering the execution and ensuring continued alignment with the vision and overall organizational goals and objectives (Carter et al. 2011; Hinterhuber and Popp 1992; La Paz 2017; MacLean and MacIntosh 2015; Sparrow 2013; Van Rensburg et al. 2014). The strategist as an entrepreneur, initiates transformational change within the organization, effectively and efficiently allocates resources (human, financial, material, and information) required to execute the strategic plan by ensuring the best fit between needs and constraints (Carter et al. 2011; Grazzini 2013; Kets De Vries et al. 2010). The strategist provides clear strategic direction for the organization, ensures the continued alignment of strategy implementation with the business goals and objectives (Beaver 2002; Hoffmann 2012; Kets De Vries 2007). Table 4 shows a summary of the Dimension of Execution.

The Dimension of Response

A change in environmental context may require a commensurate modification or refinement of strategy. Strategy is not static. The strategist is skilful at reading situations (Smaltz et al. 2006) and maintains a keen awareness of the organization's environment - continuously scanning and monitoring the prevailing environmental landscape searching for new opportunities or threats that could affect current strategy (Carter et al. 2011; Hautz 2017). Once the strategist spots a new threat or opportunity, agility is required to determine the effect of the change and refine strategy accordingly. The more agile a strategy is, the easier it is to respond to change in the environment.

Table 4: Capabilities of the Dimension of Execution

First-Order Capabilities of a Strategist	References
Ability to translate vision and strategy into actionable plan	Angwin et al. (2009); Rohrbeck and Gemünden (2011); Van Rensburg et al. (2014)
Ability to execute strategic plan	Carter et al. (2011); Hinterhuber and Popp (1992); La Paz (2017); MacLean and MacIntosh (2015); Sparrow (2013); Van Rensburg et al. (2014)
Ability to ensure alignment of execution with strategic context	Carter et al. (2011); Hinterhuber and Popp (1992); La Paz (2017); MacLean and MacIntosh (2015); Sparrow (2013); Van Rensburg et al. (2014)
Ability to provide clear direction for the organisation to follow	Beaver (2002); Hoffmann (2012); Kets De Vries (2007)
Ability to effectively and efficiently allocate of resources	Carter et al. (2011); Grazzini (2013); Kets De Vries et al. (2010)

The dimension of response requires that the strategist be able to learn and unlearn rapidly as required (Angwin et al. 2009; Kets De Vries et al. 2010; La Paz 2017). Ability to quickly learn what is new in the environment and unlearn what is no longer relevant is instrumental to being effective as a strategist. Inability to unlearn may result in applying knowledge that is no longer relevant to a situation – attempting to solve a new problem using old tricks. Flexibility and adaptability are crucial in an ever-changing environmental context (Van Rensburg et al. 2014). While the strategists are required to be able to develop and commit to long-term plans, making strong choices at the beginning, they are also required to be able to refine and modify action plans with decisiveness and flexibility when so required (Angwin et al. 2009; Dillen et al. 2018; Hinterhuber and Popp 1992). This ability to make quick decisions in the face of changing environmental context (Breene et al. 2007) and to decide which detected changes in the environment to respond to (Beaver 2002), are vital qualities of an effective strategist. Table 5 shows a summary of the Dimension of Response.

The Dimension of Advocacy

Strategies are not developed, executed and operationalised in isolation, rather effective strategies require communication,

DOI: 10.17705/1pais.10303

collaboration, negotiations, motivation and persuasion throughout the lifecycle of the strategy. The strategist is required to be an effective advocate of the strategy from initiation to execution and to institutionalisation (Van Rensburg et al. 2014). The scope of advocacy is strategic and pervasive – from the senior executive level to the operational level within the organization, even extending outside the organization to key stakeholders and strategic alliances. The strategist must be able to influence the decisions and actions of key stakeholders (Hinterhuber and Popp 1992; Watkins 2012).

Table 5: Capabilities of the Dimension of Response

First-Order Capabilities of a Strategist	References
Ability to timely detect changes in the environmental context	Smaltz et al. (2006)
Ability to agilely respond to strategic changes	Carter et al. (2011); Hautz (2017)
Ability to modify or refine strategy as required	Angwin et al. (2009); Dillen et al. (2018); Hinterhuber and Popp (1992); Van Rensburg et al. (2014)
Ability to learn and unlearn rapidly as required	Angwin et al. (2009); Kets De Vries et al. (2010); La Paz (2017)
Ability to be decisive in the face of change	Beaver (2002); Breene et al. (2007)

As strategies are in many cases built on ideas and visions that others cannot grasp or perceive, the strategist must be able to clearly communicate the strategy in clear and understandable terms to convince and secure the buy-in of all relevant stakeholders (Critelli 2005; Fortino 2008; Gavetti 2011; Van Rensburg et al. 2014). The strategists must be able to sell their ideas and ideals. Furthermore, at other times, effective strategies emerge from artfully synthesising ideas from different persons (Mintzberg 1994) by effective communication, collaboration and negotiation skills.

In many cases, a new strategy significantly changes the way the organization operates. The strategist, as the advocate, is required to effectively communicate the strategy to the organization (Behnam and Rasche 2009; Carter et al. 2011; Fortino 2008; Van Rensburg et al. 2014) and to create a shared understanding of the vision and strategy within the organization (Breene et al. 2007; Rooke and Torbert 2005; Van Rensburg et al. 2014). The strategist is skilful in conflict resolution and overcoming people’s resistance to change by employing persuasive, negotiating, influencing and collaborating skills (Angwin et al. 2009; Fortino 2008; Smaltz et al. 2006; Watkins 2012). Table 6 shows a summary of the Dimension of Advocacy.

The Chief Information Security Officer as a Strategist

The competencies and qualities of the strategist described in the previous section are equally relevant to the ISM domain. This section describes how an information security executive exhibiting the competencies defined within each of the five dimensions of the strategist from the management literature will be able to overcome the ISM strategic challenges presented in the background section.

Table 6: Capabilities of the Dimension of Advocacy

First-Order Capabilities of a Strategist	References
Ability to influence and persuade	Hinterhuber and Popp (1992); Watkins (2012)
Ability to collaborate	Mintzberg (1994)
Ability to clearly communicate strategy	Behnam and Rasche (2009); Carter et al. (2011); Fortino (2008); Van Rensburg et al. (2014)
Ability to resolve conflict	Angwin et al. (2009); Fortino (2008); Smaltz et al. (2006); Watkins (2012)
Ability to negotiate and secure buy-in	Critelli (2005); Fortino (2008); Gavetti (2011); Van Rensburg et al. (2014)
Ability to advocate the strategy	Breene et al. (2007); Rooke and Torbert (2005); Van Rensburg et al. (2014)

The CISO and the Dimension of Thought

Organizations currently face a strategic challenge of a highly complex and evolving threat landscape that renders traditional security approaches ineffective (see *Evolving Threat Landscape Requires an Innovative Strategy)*. The unpredictable and novel nature of threats, increasing innovations in ICT and emerging IT trends in organizations require a commensurate novel approach to security strategy.

CISOs functioning as strategists with the competencies of the dimension of thought are required to employ creativity and imaginative thinking to devise effective and relevant strategies. By harnessing the power of abstract and lateral thinking, they are able to construct effective strategies without having all the fact or knowing what kinds of threats to expect.

The Stuxnet attack as described by Choo (2011), is a typical example of a creative and ingenious threat. The target centrifugal environment for the nuclear enrichment process was adequately secured using traditional security. However, not only did Stuxnet inherently employ multiple advanced attack vectors that exploited up to four unknown zero-day vulnerabilities, it also utilised ingenious and unconventional means of achieving initial compromise. Protecting information resources from attacks like this, requires CISOs that can draw on creativity, imagination, and the power of abstract and lateral thinking to craft strategies of commensurate ingenuity.

This paper therefore posits that CISOs must be able to draw on creative, imaginative, abstract, lateral thinking approaches towards developing novel security strategies to address evolving threat landscape in the face of uncertainty.

The CISO and the Dimension of Contextualisation

The strategist's dimension of Contextualisation involves the ability to recognise and place strategy in the organizational context, requires a holistic view and long-term orientation, with an ability to maintain a keen awareness of the environment. Effective strategy must be relevant to the organization for which it is crafted. This requires an understanding of the environment within which the organization operates, an adequate and sufficient understanding of the prevailing threat landscape the organization faces, and awareness of current capabilities the organization possesses. Currently, ISM faces the strategic challenge of compliance culture in which security controls are selected arbitrarily to meet compliance requirements and therefore do not translate to an effective security

DOI: 10.17705/1pais.10303

posture for the organizations (see *Security Strategy Transcends Compliance).*

CISOs functioning as strategists with the competencies of the dimension of contextualisation recognise that security should not be in isolation to the business. They understand the prevailing threat landscape faced by the organization, they also understand the long-term objectives and goals of the organization and are able to measure and/or determine the social context – values, beliefs, behaviours and culture of the organization. Consequently, they are able to create security strategies that are relevant to the organization which in turn translate to effective security posture. An effective security strategy must recognise the organization's contextual environment, which includes the organization's vendors, contractors, customers, competitors and the complex threat landscape.

This paper therefore posits that CISOs must have a keen awareness of the security environment in order to develop long term and holistic security strategies that can be placed in the organizational context.

The CISO and the Dimension of Execution

The strategist's dimension of execution involves the ability to translate vision and strategy into an actionable plan; to initiate and drive transformational change, while ensuring continued alignment with business objectives; and to provide clear strategic direction. CISOs already develop and execute security programs, allocating resources (people, funds, time) accordingly. However, this execution is performed at an operational level without the business context and strategic oversight. Due to the strategic challenge in which security is perceived as an IT problem, security programs have assumed a narrow and system-centric view such that security controls are implemented to solve technical problems with an operational view (see *Security Strategy Requires a Holistic Organizational View).*

CISOs as strategists operating in the execution dimension are required to translate the articulated security vision and strategy into an actionable plan; and continually ensure alignment with organization's business strategy during execution of action plan. They provide clear direction, maintaining the strategic context and guiding execution towards desired future outcomes. Without this strategic oversight during execution, there is the high tendency of misalignment with the business strategy and ultimate derailment, such that implemented solutions no longer represent the intended strategic outcomes. CISOs as strategists therefore provide the strategic steer such that, implementation of security controls can be halted, altered, refined or fast tracked as required based on prevailing strategic context and priorities. Consequently, security controls and counter threat measures are effective and fit for purpose on completion, adding value to the organization as intended.

This paper therefore argues that CISOs must be able to implement an actionable plan (translated from a clear vision and direction) within the organizational context using efficient and effective allocation of resources.

The CISO and the Dimension of Response

The strategist's dimension of response involves the ability to detect changes in the environmental context in a timely manner and to respond with agility. It also requires the ability to modify or refine strategy as required with decisiveness in the face of constant change, and the ability to learn and unlearn rapidly as required. Currently, organizations are not learning from their security incident response process, and thus are not deriving the appropriate situational awareness, which is key to the detection and identification of changes within the environmental context. Consequently, ability to respond to changes in strategic context is deficient (see *Response to Strategic Change Requires Situational Awareness).*

CISOs as strategists in the dimension of response recognise that the security environment is transient, and that security controls selected today, may become obsolete tomorrow due to evolved threat. With this recognition therefore, emphasis should no longer be placed on the implementation of preventative controls, but rather on the capacity for strategic response. CISOs as strategists must use their ability to learn and unlearn rapidly in an exploratory manner to guide organizational learning from incidents and changes to achieve appropriate situational awareness. In the event of a change or mutation in the threat landscape, lessons learned from previous incidents can be rapidly unlearned as a new threat is discovered – resulting in sustained situational awareness.

The concept of response oriented security strategies exists in security literature. Baskerville et al. (2014) describe a response paradigm in which resources are allocated towards timely detection of incidents and appropriate response capacity. This research therefore extends existing knowledge in security literature by introducing the concept of strategic response in contrast to incident response.

This paper argues that CISOs must be able to detect and respond to strategic changes within the environmental context and decisively modify security strategy as required.

The CISO and the Dimension of Advocacy

The strategist's dimension of advocacy involves the ability to motivate, inspire, influence, persuade, collaborate, communicate clearly, negotiate, and to champion a cause. The strategist in this dimension of advocacy is skilful at conflict resolution and overcoming people's resistance to change. Currently, communication gaps exist between ISM and 1) senior management, 2) other functional parts of the organization; and 3) employees in general. Thus, leading to further dissociation of security from the business and inability to realise desired security behavioural change within the organization (see *Security Strategy Requires Effective Communication*).

Security literature already recognises the CISO as the spokesperson for security and is required to function as advocate for security within the organization (Ashenden 2008; Steinbart et al. 2018). However, evidence from security literature suggests that the extent of this advocacy has been relegated to that of developing and implementing security education training and awareness (SETA) program, which is only a subset of overall security program (Karanja and Rosso 2017). While championing a SETA program is an operational function, championing the Security strategy is strategic.

CISOs operating as strategists within the dimension of advocacy are thus required to possess the communication skills to clearly communicate security strategy in understandable terms to senior management in order to secure buy-in for security initiatives. Serving as advocates of security, they will be able to champion the cause of security at all levels of the organization – from the senior executive level to middle management and non-management levels. Beyond the usual dos and don'ts of security awareness, the CISOs as strategists, are able to breakup currently existing communication gaps, overcome people's resistance to change, and facilitate organizational transformation by inspiring shared vision of security across the organization.

This paper therefore argues that CISOs must be able to clearly communicate strategy in order to motivate and influence relevant stakeholders towards inspiring a shared vision of information security.

Summary

We have combined the first-order capabilities that relate to each dimension into higher second-order capabilities that relate to the strategic dimensions. Table 7 below summarises the Strategic Dimensions and Second-Order Strategic Capabilities of the Chief Information Security Officer.

Table 7: Summary of the Strategic Dimensions and Second-Order Strategic Capabilities of the Chief Information Security Officer

CISO Strategy Dimension	Second Order Capabilities of a CISO
Thought	*CISOs must be able to draw on creative, imaginative, abstract, lateral thinking approaches towards developing novel security strategies to address evolving threat landscape in the face of uncertainty.*
Contextualisation	*CISOs must have a keen awareness of the security environment in order to develop long term and holistic security strategies that can be placed in the organizational context.*
Execution	*CISOs must be able to implement an actionable plan (translated from a clear vision and direction) within the organizational context using efficient and effective allocation of resources.*
Response	*CISOs must be able to detect and respond to strategic changes within the environmental context and decisively modify security strategy as required.*
Advocacy	*CISOs must be able to clearly communicate strategy in order to motivate and influence relevant stakeholders towards inspiring a shared vision of information security*

Conclusion

The highly complex and sophisticated threat landscape has significantly increased the risk to organizational information resources. The increasing magnitude and impact of security incidents have revealed that traditional approaches to security management are no longer sufficient. Today's security strategies must not only be novel, they must also sufficiently dynamic and adaptable to be effective in an unstable security environment (and still maintain alignment with the business goals and objectives).

The security campaign requires CISOs to function as 'strategists', capable of crafting security strategies that enable organizations to achieve their goals and objectives. This paper set out to answer the research question: w*hat characteristics are required by the chief information security officer to effectively function as a strategist? We* observed that the security literature lacked a strategic perspective, with no evidence to show that CISOs were required to function as strategists. Furthermore, security management within organizations faces a number of strategic challenges that detract from the overall effective security posture of the organizations. This requires the security function to assume a strategic orientation and develop strategic competencies before it can overcome these challenges.

We subsequently reviewed the management literature, identified a number of characteristics and qualities of the strategist, which we coded using thematic analysis, and condensed into the five dimensions of the strategist. These dimensions have been adapted from the management literature perspective into the security domain and discussed in the context of current security management strategic challenges.

This paper posits that CISOs require the competencies inherent in the five dimensions to function effectively as strategists. We further argue that CISOs with these dimensions are better positioned to address the current strategic challenges faced by security management.

Contributions

The five strategic dimensions of thought, contextualisation, execution, response and advocacy have the potential to transform the role of the CISO to one better suited to the strategic security challenges faced by modern organizations. In this regard, the five dimensions extend guidance in the literature on the role of CISOs.

The CISO must have sufficient formal power derived from the reporting structure in the organization to effectively exercise the five strategic dimensions (see Carter et al. (2011) on CIOs). Similar to the situation with CIOs, if CISOs are effectively seen as middle managers then they will be forced to fall back on their technical credentials and build their reputation on the management of information resources. Whereas if CISOs are seen to be on par with other C*x*Os then they will have the opportunity to create important business relationships and the authority to create security strategy around information resources. It is in the latter situation that the organization benefits the most from the CISO's strategic capability. Subsequently, research reports that increasingly CISOs not only have good skills in IT and information security, but also have undertaken business studies, usually in the form of an MBA (Karanja and Rosso 2017). This is critical as it enables them to utilise both business and information security knowledge, for instance being able to contextualise an incident within the business context.

Further, organizations must be open to *strategizing* on information security. This may not be the case in organizations where it is seen that meeting standards is enough (compliance culture), or where the only security controls deployed are as a result of legal and regulatory imperatives. For example, strategists may be extremely valuable in firms where the primary security concern relates to the protection of Intellectual Property from industrial espionage. In this case, the ability of the organization to protect its IP investment comes down to the effectiveness of its security strategy rather than the amount of compliance with industry standards. This also depends on the CISO's propensity to be able to respond to strategic changes in the organisational internal and external environment to keep the security strategy current, and on their ability to clearly communicate the strategy to their peers and to the rest of the organisation.

Organizations can use the five dimensions as a guide to develop selection criteria to recruit the most appropriate CISO. The dimensions provide specific competencies required to succeed in discharging the strategic responsibilities of a CISO. CISO candidates who exhibit these 5 dimensions should be able to strategize within the organizational context and can be seen as leaders in the organization. The five dimensions can be thus used as criteria to test whether CISO candidates are suited to the CISO role in organizations.

An increasing focus of ISM research is the need to develop new paradigms and models to better explain security strategic response in organizations. However, the literature does not define the capabilities needed by the CISO to generate, apply and evaluate these strategic security paradigms to the organizational context. This paper contributes to theory by identifying the specific characteristics needed in a CISO to apply these paradigms and methods in practice. We now understand that CISOs need specific competencies (see the specific propositions related to the 5 dimensions) to wield successful strategies to protect organizations. An understanding of these competencies further provides scholars insight into the strategic role of CISOs.

Further, this paper draws insights from the management literature (which is well researched and established in the concept of strategy and the role of the strategist) and interprets these into the security domain. It succeeds in establishing a portal to the security literature from the management literature, an approach other researchers in the security strategy field can adopt and utilise in drawing and

DOI: 10.17705/1pais.10303

appropriating insights into the security strategy space.

Limitations and Further Research

This study has the following perceived limitations. Firstly, as this was a conceptual study based on systematic literature review, no data was collected to provide empirical evidence for how CISOs may overcome current strategic ISM challenges, using the competencies of the five dimensions of the strategist.

Furthermore, CISOs with the five dimensions may not be able to overcome all the strategic challenges if their position is not strategically placed within the organizational hierarchy. However, Jarzabkowski et al. (2007) argue that not only top management can be strategists but middle-management and even non-management employees could be important as strategist. This could be investigated in further research to determine if and how CISOs who are not occupying a strategic role within their organizations can still influence and shape organizational-level security strategy using the five dimensions.

Thirdly, it may be difficult to find CISOs with the competencies of a strategist, in this case the onus then falls on higher education institutions to instil and help future CISOs cultivate such competencies at a tertiary level (Ahmad and Maynard 2014).

The following represent additional opportunities for further research. Firstly, as the five dimensions represent different types of skills and competencies that are required at different stages of strategy formulation and strategizing activities. Each dimension and their inherent competencies should be investigated to determine which is most suitable for each stage of the strategy lifecycle. Consequently, organizations can have more refined selection criteria for CISOs depending on where they are in the strategy lifecycle.

Secondly, further research is required in defining and articulating a practice area for security strategy. This should include development, execution, operationalisation, and maintenance activities for security strategy.

Thirdly, further research is required to expand the scope of literature review on the characteristics of strategist to warfare literature to determine and extract the characteristics of a ‘General’ as a strategist. Strategy originated from the military and warfare and as cyberspace has become a battleground for cyber warfare (Denning 1999), characteristics of a general as a strategist, which may not have been relevant to strategic management, may be relevant to security. These characteristics would then be used to expand and enrich the five dimensions presented in this paper.

Finally, each of the five dimensions appears to resonate with a personality type. This is in line with Jarzabkowski et al. (2007)’s argument that the characteristics of a strategist are intertwined with the personality and individuality of the strategist. This suggests that looking for the right CISO as a strategist, should include a means of assessing individual personality. Thus, further research may be required to examine how these strategists’ dimensions translate to personalities, by utilising existing or modified personality tests.

References

Ahmad, A., Bosua, R., and Scheepers, R. 2014a. "Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective," *Computers & Security* (42), pp 27-39.

Ahmad, A., and Maynard, S. 2014. "Teaching Information Security Management: Reflections and Experiences," *Information Management & Computer Security* (22:5), pp 513-536.

Ahmad, A., Maynard, S., and Shanks, G. 2015. "A Case Analysis of Information Systems and Security Incident Responses," *International Journal of Information Management*).

Ahmad, A., Maynard, S.B., and Park, S. 2014b. "Information Security Strategies: Towards an Organizational Multi-Strategy Perspective," *Journal of Intelligent Manufacturing*).

Alexander, A., and Cummings, J. 2016. "The Rise of the Chief Information Security Officer," *People & Strategy* (39:1), Winter2016, pp 10-13.

Alshaikh, M., Ahmad, A., Maynard, S.B., and Chang, S. 2014. "Towards a Taxonomy of Information Security Management Practices in Organisations," ACIS.

Alshaikh, M., Maynard, S.B., Ahmad, A., and Chang, S. 2018. "An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations," in: *Proceedings of the 51st Hawaii International Conference on System Sciences*. Hawaii: p. 10.

Angwin, D., Paroutis, S., and Mitson, S. 2009. "Connecting up Strategy: Are Senior Strategy Directors a Missing Link?," *California Management Review* (51:3), Spring2009, pp 74-94.

Ashenden, D. 2008. "Information Security Management: A Human Challenge?," *Information Security Technical Report* (13:4), pp 195-201.

Ashenden, D., and Sasse, A. 2013. "Cisos and Organisational Culture: Their Own Worst Enemy?," *Computers and Security* (39:PART B), pp 396-405.

Austen Johnson, H. 2007. "Artistry for the Strategist," *Journal of Business Strategy* (28:4), pp 13-21.

Barry, D., Elmes, M., Johanson, U., Hatch, M.J., and Hazen, M.A. 1997. "Strategy Retold: Toward a Narrative View of Strategic Discourse," *Academy of Management Review*), pp 429-452.

Baskerville, R., Spagnoletti, P., and Kim, J. 2014. "Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response," *Information & Management* (51:1), pp 138-151.

Beaver, G. 2002. "The Chief Executive Officer: Showman, Statesman and Strategist," *Strategic Change* (11:6), pp 287-289.

Behnam, M., and Rasche, A. 2009. "'Are Strategists from Mars and Ethicists from Venus?'–Strategizing as Ethical Reflection," *Journal of Business Ethics* (84:1), pp 79-88.

Breene, R.T.S., Nunes, P.F., and Shill, W.E. 2007. "The Chief Strategy Officer," *Harvard Business Review* (85:10), pp 84-93.

Brooks, N.G., Greer, T.H., and Morris, S.A. 2018. "Information Systems Security Job Advertisement Analysis: Skills Review and Implications for Information Systems Curriculum," *Journal of Education for Business* (93:5), pp 213-221.

Carter, M., Grover, V., and Thatcher, J.B. 2011. "The Emerging Cio Role of Business Technology Strategist," *MIS Quarterly Executive* (10:1), pp 19-29.

Cattani, G., Porac, J.F., and Thomas, H. 2017. "Categories and Competition," *Strategic Management Journal* (38:1), pp 64-92.

Choi, M. 2016. "Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing," *Sustainability* (8:7), p 638.

Choo, K.-K.R. 2011. "The Cyber Threat Landscape: Challenges and Future Research Directions," *Computers & Security* (30), 1/1/2011, pp 719-731.

Critelli, M.J. 2005. "Back Where We Belong," *Harvard business review* (83:5), pp 47-54, 152.

Dawson, M., Burrell, D.N., Rahim, E., and Brewster, S. 2010. "Examining the Role of the Chief Information

DOI: 10.17705/1pais.10303

Security Officer (Ciso) & Security Plan," *Journal of Information Systems Technology & Planning* (3:6), pp 1-5.

Denning, D.E.R. 1999. *Information Warfare and Security*. Addison-Wesley Reading MA.

Dew, N. 2007. "Abduction: A Pre-Condition for the Intelligent Design of Strategy," *Journal of Business Strategy* (28:4), pp 38-45.

Dillen, Y., Laveren, E., Rudy Marten, Vocht, S.D., and Imschoot, E.V. 2018. "From "Manager" to "Strategist" : An Examination of the Evolving Role of Persistent High-Growth Entrepreneurs," *International Journal of Entrepreneurial Behavior & Research*), pp p. 1-27.

Dragoni, L.-S.O.P.P.E. 2011. "Developing Executive Leaders: The Relative Contribution of Cognitive Ability, Personality, and the Accumulation of Work Experience in Predicting Strategic Thinking Competency," *Personnel Psychology* (64:4), Winter2011, pp 829-864.

Durbin, S. 2011. "Information Security without Boundaries," *Network Security* (2011:2), pp 4-8.

Fitzgerald, T. 2007. "Clarifying the Roles of Information Security: 13 Questions the Ceo, Cio, and Ciso Must Ask Each Other," *Information Systems Security* (16:5), pp 257-263.

Fortino, A. 2008. "The New Cio: From Technician to Business Strategist and the Implications for E-Commerce," *IEEE International Conference on e-Business Engineering*: IEEE, pp. 139-146.

Franke, U., and Brynielsson, J. 2014. "Cyber Situational Awareness–a Systematic Review of the Literature," *Computers & Security* (46), pp 18-31.

Gavetti, G. 2011. "The New Psychology of Strategic Leadership," *Harvard Business Review* (89:7/8), pp 118-125.

Grazzini, F. 2013. "How Do Managers Make Sense of Strategy?," *European Business Review* (25:6), pp 484-517.

Hall, J.H., Sarkani, S., and Mazzuchi, T.A. 2011. "Impacts of Organizational Capabilities in Information Security," *Information Management & Computer Security* (19:3), pp 155-176.

Hautz, J. 2017. "Opening up the Strategy Process–a Network Perspective," *Management Decision* (55:9), pp 1956-1983.

Hinterhuber, H.H., and Popp, W. 1992. "Are You a Strategist or Just a Manager?," *Harvard Business Review* (70:1), pp 105-113.

Hoffmann, L. 2012. "Q&A: Chief Strategist." Association for Computing Machinery, pp. 120-119.

Hunsicker, J.Q. 1980. "Can Top Managers Be Strategists?," *Strategic Management Journal* (1:1), pp 77-83.

Jarzabkowski, P., Balogun, J., and Seidl, D. 2007. "Strategizing: The Challenges of a Practice Perspective," *Human Relations* (60:1), pp 5-27 23p.

Johnson, M.E., and Goetz, E. 2007. "Embedding Information Security into the Organization,").

Karanja, E. 2017. "The Role of the Chief Information Security Officer in the Management of It Security," *Information & Computer Security* (25:3), pp 300-329.

Karanja, E., and Rosso, M.A. 2017. "The Chief Information Security Officer: An Exploratory Study," *Journal of International Technology and Information Management* (26:2).

Karyda, M. 2017. "Fostering Information Security Culture in Organizations: A Research Agenda," in: *MCIS 2017 Proceedings*. p. 28.

Kayworth, T., and Whitten, D. 2010. "Effective Information Security Requires a Balance of Social and

Technology Factors," *MIS Quarterly Executive* (9:3), pp 163-175.

Kets De Vries, M.F., Vrignaud, P., Agrawal, A., and Florent-Treacy, E. 2010. "Development and Application of the Leadership Archetype Questionnaire," *The International Journal of Human Resource Management* (21:15), pp 2848-2863.

Kets De Vries, M.F.R. 2007. "Decoding the Team Conundrum: The Eight Roles Executives Play," *Organizational Dynamics* (36:1), pp 28-44.

La Paz, A. 2017. "How to Become a Strategist Cio.," *IT Professional* (19:1), pp 48-55.

Le, N.T., & Hoang, D. B. 2017. "Capability Maturity Model and Metrics Framework for Cyber Cloud Security," *Scalable Computing: Practice and Experience* (18:4), pp 277-290.

Lindup, K. 1996. "Role of Information Security in Corporate Governance," *Computers and Security* (15:6), pp 477-485.

MacLean, D., and MacIntosh, R. 2015. "Planning Reconsidered: Paradox, Poetry and People at the Edge of Strategy," *European Management Journal* (33:2), pp 72-78.

Mathiassen, L., Saarinen, T., Tuunanen, T., and Rossi, M. 2007. "A Contingency Model for Requirements Development," *Journal of the Association for Information Systems* (8:11), pp 569-597.

Mintzberg, H. 1994. "Rethinking Strategic Planning Part I: Pitfalls and Fallacies," *Long Range Planning* (27:3), pp 12-21.

Mintzberg, H. 1996. "Musings on Management," *Harvard Business Review* (74:4), pp 61-67.

Montgomery, C.A. 2008. "Putting Leadership Back into Strategy," *Harvard Business Review* (86:1), pp 54-60+134.

Moon, Y.J., Choi, M., and Armstrong, D.J. 2018. "The Impact of Relational Leadership and Social Alignment on Information Security System Effectiveness in Korean Governmental Organizations," *International Journal of Information Management* (40), pp 54-66.

Ringland, G. 2003. "Scenario Planning: Persuading Operating Managers to Take Ownership," *Strategy & Leadership* (31:6), pp 22-28.

Rohrbeck, R., and Gemünden, H.G. 2011. "Corporate Foresight: Its Three Roles in Enhancing the Innovation Capacity of a Firm," *Technological Forecasting and Social Change* (78:2), pp 231-243.

Rooke, D., and Torbert, W.R. 2005. "7 Transformations of Leadership," *Harvard Business Review* (83:4), pp 66-76.

Ruighaver, A.B., Maynard, S.B., and Chang, S. 2007. "Organisational Security Culture: Extending the End-User Perspective," *Computers & Security* (26), 1/1/2007, pp 56-62.

Schiavone, S., Garg, L., and Summers, K. 2014. "Ontology of Information Security in Enterprises," *Electronic Journal Information Systems Evaluation Volume* (17:1).

Shojaie, B. 2018. "Implementation of Information Security Management Systems Based on the Isoiec 27001 Standard in Different Cultures," in: *Department of Informatics*. University of Hamburg.

Smaltz, D.H., Sambamurthy, V., and Agarwal, R. 2006. "The Antecedents of Cio Role Effectiveness in Organizations: An Empirical Study in the Healthcare Sector," *IEEE Transactions on Engineering Management* (53:2), pp 207-222.

Smiraus, M., and Jasek, R. 2011. "Risks of Advanced Persistent Threats and Defense against Them," *Annals of DAAAM & Proceedings*).

DOI: 10.17705/1pais.10303

Sood, A.K., and Enbody, R.J. 2013. "Targeted Cyberattacks: A Superset of Advanced Persistent Threats," *IEEE Security & Privacy Magazine* (11:1), p 54.

Sparrow, J. 2013. "Creating and Sustaining Meaningful Engagement: What Managers Need to Develop in Their Five Roles as Engagers," *Development and Learning in Organisations* (27:3), pp 8-10.

Steinbart, P.J., Raschke, R.L., Gal, G., and Dilla, W.N. 2018. "The Influence of a Good Relationship between the Internal Audit and Information Security Functions on Information Security Outcomes," *Accounting, Organizations and Society* (In Press).

Sveen, F.O., Torres, J.M., and Sarriegi, J.M. 2009. "Blind Information Security Strategy," *International journal of critical infrastructure protection* (2:3), pp 95-109.

Tan, T., Ruighaver, A., and Ahmad, A. 2003. "Incident Handling: Where the Need for Planning Is Often Not Recognised," *Proceedings of the 1st Australian Computer Network, Information & Forensics Conference, Australia*.

Tang, M., and Zhang, T. 2016. "The Impacts of Organizational Culture on Information Security Culture: A Case Study," *Information Technology and Management* (17:2), pp 179-186.

Tankard, C. 2011. "Advanced Persistent Threats and How to Monitor and Deter Them," *Network Security*:8), p 16.

Tøndel, I.A., Line, M.B., and Jaatun, M.G. 2014. "Information Security Incident Management: Current Practice as Reported in the Literature," *Computers & Security* (45), pp 42-57.

Van Rensburg, M.J., Davis, A., and Venter, P. 2014. "Making Strategy Work: The Role of the Middle Manager," *Journal of Management & Organization* (20:2), pp 165-186.

Von Solms, B., and Von Solms, R. 2004. "The 10 Deadly Sins of Information Security Management," *Computers & Security* (23:5), pp 371-376.

Watkins, M.D. 2012. "How Managers Become Leaders," *Harvard Business Review* (90:6), pp 64-72.

Webb, J., Ahmad, A., Maynard, S.B., Baskerville, R., and Shanks, G. 2017. "Organizational Security Learning from Incident Response," in: *International Conference On Information Systems (ICIS)*. Seoul, South Korea: p. 11.

Webb, J., Ahmad, A., Maynard, S.B., and Shanks, G. 2014. "A Situation Awareness Model for Information Security Risk Management," *Computers & Security* (44), pp 391-404.

Webster, J., and Watson, R.T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review." JSTOR, pp. xiii-xxiii.

Whitten, D. 2008. "The Chief Information Security Officer: An Analysis of the Skills Required for Success," *Journal of Computer Information Systems* (48:3), Spring2008, pp 15-19.

Williams, P. 2007. "Executive and Board Roles in Information Security," *Network Security* (2007:8), pp 11-14.

Appendix 1 – Final List of Articles

Information Security Management

Ahmad, A., Maynard, S.B., and Park, S. 2014b. "Information Security Strategies: Towards an Organizational Multi-Strategy Perspective," Journal of Intelligent Manufacturing).

Alexander, A., and Cummings, J. 2016. "The Rise of the Chief Information Security Officer," People & Strategy (39:1), Winter2016, pp 10-13.

Ashenden, D. 2008. "Information Security Management: A Human Challenge?," Information Security Technical Report (13:4), pp 195-201.

Ashenden, D., and Sasse, A. 2013. "Cisos and Organisational Culture: Their Own Worst Enemy?," Computers and Security (39:PART B), pp 396-405.

Choi, M. 2016. "Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing," Sustainability (8:7), p 638.

Dawson, M., Burrell, D.N., Rahim, E., and Brewster, S. 2010. "Examining the Role of the Chief Information Security Officer (Ciso) & Security Plan," Journal of Information Systems Technology & Planning (3:6), pp 1-5.

Fitzgerald, T. 2007. "Clarifying the Roles of Information Security: 13 Questions the Ceo, Cio, and Ciso Must Ask Each Other," Information Systems Security (16:5), pp 257-263.

Johnson, M.E., and Goetz, E. 2007. "Embedding Information Security into the Organization,").

Karanja, E. 2017. "The Role of the Chief Information Security Officer in the Management of It Security," Information & Computer Security (25:3), pp 300-329.

Karanja, E., and Rosso, M.A. 2017. "The Chief Information Security Officer: An Exploratory Study," Journal of International Technology and Information Management (26:2).

Lindup, K. 1996. "Role of Information Security in Corporate Governance," Computers and Security (15:6), pp 477-485.

Moon, Y.J., Choi, M., and Armstrong, D.J. 2018. "The Impact of Relational Leadership and Social Alignment on Information Security System Effectiveness in Korean Governmental Organizations," International Journal of Information Management (40), pp 54-66.

Steinbart, P.J., Raschke, R.L., Gal, G., and Dilla, W.N. 2018. "The Influence of a Good Relationship between the Internal Audit and Information Security Functions on Information Security Outcomes," Accounting, Organizations and Society (In Press).

Whitten, D. 2008. "The Chief Information Security Officer: An Analysis of the Skills Required for Success," Journal of Computer Information Systems (48:3), Spring 2008, pp 15-19.

Williams, P. 2007. "Executive and Board Roles in Information Security," Network Security (2007:8), pp 11-14.

Strategic Management

Angwin, D., Paroutis, S., and Mitson, S. 2009. "Connecting up Strategy: Are Senior Strategy Directors a Missing Link?," California Management Review (51:3), Spring2009, pp 74-94.

Austen Johnson, H. 2007. "Artistry for the Strategist," Journal of Business Strategy (28:4), pp 13-21.

Barry, D., Elmes, M., Johanson, U., Hatch, M.J., and Hazen, M.A. 1997. "Strategy Retold: Toward a Narrative View of Strategic Discourse," Academy of Management Review), pp 429-452.

DOI: 10.17705/1pais.10303

Beaver, G. 2002. "The Chief Executive Officer: Showman, Statesman and Strategist," Strategic Change (11:6), pp 287-289.

Behnam, M., and Rasche, A. 2009. "'Are Strategists from Mars and Ethicists from Venus?'–Strategizing as Ethical Reflection," Journal of Business Ethics (84:1), pp 79-88.

Breene, R.T.S., Nunes, P.F., and Shill, W.E. 2007. "The Chief Strategy Officer," Harvard Business Review (85:10), pp 84-93.

Carter, M., Grover, V., and Thatcher, J.B. 2011. "The Emerging Cio Role of Business Technology Strategist," MIS Quarterly Executive (10:1), pp 19-29.

Cattani, G., Porac, J.F., and Thomas, H. 2017. "Categories and Competition," Strategic Management Journal (38:1), pp 64-92.

Critelli, M.J. 2005. "Back Where We Belong," Harvard business review (83:5), pp 47-54, 152.

Dew, N. 2007. "Abduction: A Pre-Condition for the Intelligent Design of Strategy," Journal of Business Strategy (28:4), pp 38-45.

Dillen, Y., Laveren, E., Rudy Marten, Vocht, S.D., and Imschoot, E.V. 2018. "From "Manager" to "Strategist": An Examination of the Evolving Role of Persistent High-Growth Entrepreneurs," International Journal of Entrepreneurial Behavior & Research), pp p. 1-27.

Dragoni, L.-S.O.P.P.E. 2011. "Developing Executive Leaders: The Relative Contribution of Cognitive Ability, Personality, and the Accumulation of Work Experience in Predicting Strategic Thinking Competency," Personnel Psychology (64:4), Winter2011, pp 829-864.

Fortino, A. 2008. "The New Cio: From Technician to Business Strategist and the Implications for E-Commerce," IEEE International Conference on e-Business Engineering: IEEE, pp. 139-146.

Gavetti, G. 2011. "The New Psychology of Strategic Leadership," Harvard Business Review (89:7/8), pp 118-125.

Grazzini, F. 2013. "How Do Managers Make Sense of Strategy?," European Business Review (25:6), pp 484-517.

Hautz, J. 2017. "Opening up the Strategy Process–a Network Perspective," Management Decision (55:9), pp 1956-1983.

Hinterhuber, H.H., and Popp, W. 1992. "Are You a Strategist or Just a Manager?," Harvard Business Review (70:1), pp 105-113.

Hoffmann, L. 2012. "Q&A: Chief Strategist." Association for Computing Machinery, pp. 120-119.

Hunsicker, J.Q. 1980. "Can Top Managers Be Strategists?," Strategic Management Journal (1:1), pp 77-83.

Kets De Vries, M.F., Vrignaud, P., Agrawal, A., and Florent-Treacy, E. 2010. "Development and Application of the Leadership Archetype Questionnaire," The International Journal of Human Resource Management (21:15), pp 2848-2863.

Kets De Vries, M.F.R. 2007. "Decoding the Team Conundrum: The Eight Roles Executives Play," Organizational Dynamics (36:1), pp 28-44.

La Paz, A. 2017. "How to Become a Strategist Cio.," IT Professional (19:1), pp 48-55.

MacLean, D., and MacIntosh, R. 2015. "Planning Reconsidered: Paradox, Poetry and People at the Edge of Strategy," European Management Journal (33:2), pp 72-78.

Mintzberg, H. 1994. "Rethinking Strategic Planning Part I: Pitfalls and Fallacies," Long Range Planning (27:3), pp 12-21.

Mintzberg, H. 1996. "Musings on Management," Harvard Business Review (74:4), pp 61-67.

Montgomery, C.A. 2008. "Putting Leadership Back into Strategy," Harvard Business Review (86:1), pp 54-60+134.

Ringland, G. 2003. "Scenario Planning: Persuading Operating Managers to Take Ownership," Strategy & Leadership (31:6), pp 22-28.

Rohrbeck, R., and Gemünden, H.G. 2011. "Corporate Foresight: Its Three Roles in Enhancing the Innovation Capacity of a Firm," Technological Forecasting and Social Change (78:2), pp 231-243.

Rooke, D., and Torbert, W.R. 2005. "7 Transformations of Leadership," Harvard Business Review (83:4), pp 66-76.

Smaltz, D.H., Sambamurthy, V., and Agarwal, R. 2006. "The Antecedents of Cio Role Effectiveness in Organizations: An Empirical Study in the Healthcare Sector," IEEE Transactions on Engineering Management (53:2), pp 207-222.

Smiraus, M., and Jasek, R. 2011. "Risks of Advanced Persistent Threats and Defense against Them," Annals of DAAAM & Proceedings).

Sparrow, J. 2013. "Creating and Sustaining Meaningful Engagement: What Managers Need to Develop in Their Five Roles as Engagers," Development and Learning in Organisations (27:3), pp 8-10.

Sveen, F.O., Torres, J.M., and Sarriegi, J.M. 2009. "Blind Information Security Strategy," International journal of critical infrastructure protection (2:3), pp 95-109.

Van Rensburg, M.J., Davis, A., and Venter, P. 2014. "Making Strategy Work: The Role of the Middle Manager," Journal of Management & Organization (20:2), pp 165-186.

Watkins, M.D. 2012. "How Managers Become Leaders," Harvard Business Review (90:6), pp 64-72.

Appendix 2 – Concept matrix for the Information Security Literature

Articles	Concepts (role of CISO in)		
	Business / Environment Understanding	**Security Strategy Design**	**Communication / Influencing**
Ahmad et al 2014b		X	
Alexander & Cummings 2016	X	X	X
Ashenden 2008	X	X	X
Ashenden 2013	X	X	X
Choi 2016			X
Dawson et al 2010	X	X	
Fitzgerald 2007			X
Johnson & Goetz 2007	X	X	X
Karanja 2017		X	
Karanja & Rosso 2017		X	X
Lundup 1996	X		
Moon 2018	X		
Steinbart et al. 2018		X	
Whitten 2008	X		X
Williams 2007		X	X

About the Authors

Sean B. Maynard is an academic based at the School of Computing and Information Systems, University of Melbourne, Australia. His research interests are in the management of information security specifically relating to security policy, security culture, security governance, security strategy, security analytics, and incident response. He has over 50 publications on these and other areas. His research has been published in high-impact journals such as Computers & Security and the International Journal of Information Management as well as leading conferences such as the International Conference on Information Systems.

Mazino Onibere is an information security professional with about 16 years' experience in various areas of Information Technology, including security. He is current a part time PhD candidate at the Department of Computing and Information Systems, University of Melbourne, Australia. His research interests are in information security strategy in organisations.

Atif Ahmad is a senior academic at the University of Melbourne's School of Computing & Information Systems. His main areas of expertise are in the strategy, risk and incident response aspects of Information Security Management (ISM). He has authored over seventy scholarly articles in ISM and received over $3M in grant funding. His research has been published in high-impact journals such as Computers & Security and the International Journal of Information Management as well as leading conferences such as the International Conference on Information Systems. Atif has previously served as a cybersecurity consultant for WorleyParsons, Pinkerton and SinclairKnightMerz. He is a Certified Protection Professional with the American Society for Industrial Security.