PACIS 2017 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Summer 7-19-2017

The Chief Information Security Officer and the Five Dimensions of a Strategist

Mazino Onibere
The University of Melbourne, mazino.onibere@unimelb.edu.au

Atif Ahmad
The University of Melbourne, atif@unimelb.edu.au

Sean Maynard
The University of Melbourne, seanbm@unimelb.edu.au

Recommended Citation

Onibere, Mazino; Ahmad, Atif; and Maynard, Sean, "The Chief Information Security Officer and the Five Dimensions of a Strategist" (2017). *PACIS 2017 Proceedings*. 77.
http://aisel.aisnet.org/pacis2017/77

The Chief Information Security Officer and the Five Dimensions of a Strategist

Indicate Submission Type: Completed Research Paper

Mazino Onibere
University of Melbourne
Australia
mazino.onibere@unimelb.edu.au

Atif Ahmad
University of Melbourne
Australia
atif@unimelb.edu.au

Sean B Maynard
University of Melbourne
Australia
seanbm@unimelb.edu.au

Abstract

The modern organisation operates within a sophisticated and evolving security threat landscape that exposes its information infrastructure to a range of security risks. Unsurprisingly, despite the existence of industry 'best-practice' security standards and unprecedented levels of investment in security technology, the rate of incidents continues to escalate. Furthermore, a review of security literature reveals an apparent lack of strategic perspective in the field of information security management (ISM) which results in a number of strategic challenges for ISM function in organisations. The level of sophistication and dynamism of threat requires organisations to develop novel security strategies that draw on creative and lateral thinking approaches. Such a security campaign requires the Chief Information Security Officer (CISO) to function as a 'strategist'. However, there is little or no evidence in security literature to show that the security leader is required to function as a strategist. In this research, we set out to identify the specific competencies required by CISOs to become effective strategists by performing a systematic literature review of both security and strategic management literature. We thematically analysed and coded the characteristics extracted from strategic management literature into the five dimensions of the strategist. We discuss these macro competencies in the context of ISM, and argue that CISOs with these five dimensions of a strategist will be able to overcome the existing strategic challenges facing ISM in organisations.

Keywords: Information Security; Information Security Strategy; Information Security Management; Chief Information Security Officer; Strategist; Competencies

Introduction

The modern organisation operates within a sophisticated and evolving security threat landscape that exposes its information infrastructure to a range of security risks. Organisations may suffer reputational damage, loss of revenue, costs arising from breaches of confidentiality agreements and loss of productivity as a result of leakage of sensitive information (Ahmad et al. 2014a). Unsurprisingly, despite the existence of industry 'best-practice' security standards and unprecedented levels of investment in security infrastructure, the rate of incidents continues to escalate (Ahmad et al. 2014b). The risks to organisations have thus become significantly heightened and require novel information security strategies that recognise the complexity of the prevailing threat environment. As a result, the role of the chief information security officer (CISO) is increasingly gaining presence in the boardroom, with greater input into strategy and is rising to the level of other C-level executives (Alexander and Cummings 2016; Dawson et al. 2010). The CISO is now required to become a strategist who is able to develop organisational-level security strategies that are flexible, adaptable and readily modifiable in commensuration with a dynamic and volatile environment, while at the same time aligning with the business strategy. A strategist develops and drives the implementation of strategies that enable organisations to achieve their goals and objectives (Smaltz et al. 2006).

However, a review of security literature reveals an apparent lack of strategic perspective in the field of information security management (ISM); a number of strategic challenges for ISM function in organisations; and little or no evidence to show that the security leader is required to function as a strategist. We address this gap by asking the following research question:

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

Consequently, we have developed the five dimensions of a strategist, which represent specific competencies required for the CISO to effectively become a strategist. We argue that with these 5 dimensions the CISO will be able to overcome the existing strategic challenges facing ISM in organisations.

The paper is organised as follows. First, we discuss the missing strategic perspective of ISM and the resulting ISM strategic challenges. Next, we develop and describe the five dimensions of the strategist based on thematic analysis of characteristics and qualities of strategists extracted from strategic management literature. Next, we 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 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 organisation. 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 organisations into practice areas such as security policy management and security risk management (Alshaikh et al. 2014). While the focus of this paper is 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 organisations 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 organised 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). 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 Organisational View

Despite the increasing recognition of the role of Information Security in protecting an organisation's information assets, and the corresponding increase in security spend (Hall et al. 2011), ISM is still seen as a technical problem – to be handled by IT (McFadzean et al. 2007; von Solms and von Solms 2004). Consequently, the strategic business context within which the organisation'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 organisation, and a system-centric view lacks alignment with the business objectives. *An effective security strategy therefore requires a holistic view of the organisation's information assets and a recognition of all organisational capabilities.*

Response to Strategic Change Requires Situational Awareness

As part of operational requirements, ISM responds to security incidents and technical changes within the organisation. However, the ISM function has no strategic response requirements. Strategic response is the ability to recognise changes in the organisation's environmental context or to any of the parameters considered during strategy development, and be able to respond accordingly by modifying strategy. In contrast, incident response is operational in nature and has the goal of recovery from incidents and restoration of service (Tan et al. 2003).

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 organisations properly investigated and learned from these incidents and anomalies, they will 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 organisation's capacity for strategic response.

Unfortunately, as Ahmad et al. (2012) demonstrated in a case study, organisations are not learning from incidents. Because of poor situational awareness, ISM is not able to respond to changes in the security environmental context within which the organisation 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 organisation's actual context (Webb et al. 2014).

Security Strategy Transcends Compliance

Security strategy developed with the intent of just satisfying compliance requirements does not translate to an effective security posture. ISM becomes a compliance problem in organisations 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 (Tan et al. 2003). Organisations derive security requirements from a number of sources such as operational, legal, contractual, regulatory, and competition requirements. Compliance appears to be the most 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 technical orientation (Shedden et al. 2011); and risk assessments are performed without appropriate reference to the organisation's actual situation (Webb et al. 2014).

When this occurs, the CISOs either may turn to their technical expertise in creating a technically 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 organisation and the prevailing security threat landscape. Thus resulting 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 organisation. This gap results in further dissociation of the security function from the business – strengthening the perception that security is a technical 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 technical.

Furthermore, Alshaikh et al. (2014) has identified intra-organisational liaison which involves communication, collaboration and coordination activities between security management and other functional parts of the organisation such as human resources and finance, as a strategic challenge. In a case study, Ahmad et al. (2015) observed that members of a particular group or unit tend to focus only on what they do, insular about other units and teams. Such that different teams do not readily disseminate information to one another within the organisation, leading to communication breakdown.

Lastly, creating a culture of security and realising desired behavioural change within the organisation requires effective communication (Lim et al. 2010; Lim et al. 2009; Ruighaver et al. 2007). 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 organisation 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 organisation. Poor communication within security management affects the security posture of the organisation.

Methodology

In this research study, we assessed publications from both security literature and strategic management literature (SML) using systematic literature review technique (Kitchenham 2004; Webster and Watson 2002). In order to identify relevant publications, we used the Scopus online database to search for the relevant terms, because of its good coverage of academic journals. In the security literature, we performed the initial search for publications by using '*information security manager*' AND '*strategist*' as search string, this yielded no results. We adjusted the search to look for '*role*' AND '*information security manager*', and 'r*ole*' AND '*CISO*' (Chief Information Security Officer). These searches yielded 7 and 14 articles, respectively. After reading the abstracts and skimming through the papers, we eventually reduced the number of relevant articles to a total of 11 publications. In SML, we used the search string '*role*' AND '*strategist*' in the Scopus online database. Initial search yielded 126 articles. After reading the abstracts, keywords and skimming through the papers, we reduced the number of relevant articles to 27.

Recognising that the sole use of the systematic approach has the potential weakness of missing out some publications, which might have referred to search key words with different names, we therefore utilised an exploratory approach in parallel. This primarily involved trying various keywords and following up references cited by the publications identified during the systematic review. These search keywords were 'IT Security manager', 'CISO', or 'information security manager' AND '*role' or 'functions'* in security literature; and '*strategist'* AND '*role', 'function', 'qualities' or 'characteristics'* in SML. At the end of the exploratory search, we increased the final number of relevant publications from security literature to 20; and from SML to 55. These were then used for the literature review. We extracted relevant *words, phrases and sentences* describing the roles of security leaders from each security literature article. The analysis of the extracted texts revealed that scholars discuss security management roles 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 thematic analysis technique, and grouped them 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 literature review. The first part presents findings from security literature; and the second part, findings from management literature.

Role of the Chief Information Security Officer

Security leaders are required to understand the organisation and industry they are in (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 organisation. 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 (Ashenden 2008; Dawson et al. 2010; Lindup 1996; 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 (Ashenden 2008; Dawson et al. 2010; Williams 2007).

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 (Ashenden 2008; Fitzgerald 2007; 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 areas. 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 great strategist is a visionary who sees a world others are unable to see, is a ground breaker, and builds great organisations (Mintzberg 1996). 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 (Grazzini 2013). Strategists are not only great conceptualisers capable of generating ideas (Kets De Vries 2007), they are also masters of the creative art of synthesising different ideas into one strategy (Mintzberg 1994). Strategists are innovation catalysts (Smaltz et al. 2006); and their actions precipitate the creation of new possibilities for the organisation (Carter et al. 2011). The strategist is a person with 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, to break new grounds and generate value and growth for the organisation (Kets De Vries 2007).

The Dimension of Contextualisation

The strategist must be able to place strategy in context. They must juxtapose their dreams and visions of the future with the prevailing environmental context while keeping the long-term objectives in sight. Effective strategists are those who by reason of being immersed in the day to day activities have acquired sufficient awareness of the organisation'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 organisation (Watkins 2012). In the same vein, the strategists must maintain keen awareness of the environment in which the organisation 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 (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 organisation's strategy (Carter et al. 2011; Dragoni 2011; Gavetti 2011).

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). In this dimension, the strategists are action-oriented and are required to develop a plan that will bring into reality the visions of the desired future. They give action to the dimensions of thought and contextualisation. Not only do they develop strategic plan, they also drive the implementation of the plan, steering the execution and ensuring continued alignment with the vision and overall organisational goals and objectives (Carter et al. 2011; MacLean and MacIntosh 2015; Sparrow 2013). The strategist as an entrepreneur, initiates transformational change within the organisation, 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). 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).

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 organisation'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). 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.

The dimension of response requires that the strategist be able to learn and unlearn rapidly as required (Angwin et al. 2009). Ability to quickly learn of what is new in the environment and unlearn when 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. 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). 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.

The Dimension of Advocacy

Strategies are not developed, executed and operationalised in isolation, rather effective strategies require communication, 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. The scope of advocacy is strategic and all reaching – from the senior executive level to the non-management level within the organisation, even extending outside the organisation to key stakeholders and strategic alliances. The strategist must be able to influence reactions of key stakeholders (Watkins 2012).

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 (Gavetti 2011). 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 organisation operates. The strategist, as the advocate, is required to effectively communicate the strategy to the organisation (Carter et al. 2011) and to create a shared understanding of the vision and strategy within the organisation (Breene et al. 2007; Rooke and Torbert 2005). 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; Smaltz et al. 2006; Watkins 2012).

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.

The CISO and the Dimension of Thought

Organisations 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 organisations 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.

T*his 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 organisational 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 organisation for which it is crafted. This requires an understanding of the environment within which the organisation operates, an adequate and sufficient understanding of the prevailing threat landscape the organisation faces, and awareness of current capabilities the organisation 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 posture for the organisations (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 organisation, they understand the long-term objectives and goals of the organisation and are able to measure and/or determine the social context – values, beliefs, behaviours and culture of the organisation. Consequently, they are able to create security strategies that are relevant to the organisation which in turn translate to effective security posture. An effective security strategy must recognise the organisation's contextual environment, which includes the organisation'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 organisational 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 Organisational 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 organisation'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 organisation 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 organisational 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, organisations 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 (Shedden et al., 2010). 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 organisational 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. *It 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 organisation; 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 organisation (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 organisation (Ashenden 2008). 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. 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 organisation – 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 organisational transformation by inspiring shared vision of security across the organisation.

This paper therefore argues that CISO 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 modern organisations operate in has significantly increased the risk to organisation's information resources. The increasing magnitude and impact of security incidents have revealed that traditional approaches to security management are no longer sufficient, and that novel approaches to security strategy are required. Today's security strategies must not only be novel, they must also be dynamic and adaptable in commensuration with the unstable security environment, and still maintain alignment with the business goals and objectives. This security campaign requires CISOs to function as 'strategists' capable of crafting security strategies that will enable organisations 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 organisations faces a number of strategic challenges that detract from the overall effective security posture of the organisations. This requires the security function to assume a strategic orientation and develop strategic competencies before it can overcome these challenges.

We subsequently went into 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. It further argues that CISOs with these dimensions are able to overcome the current strategic challenges faced by security management.*

Contributions

This paper contributes to *practice*. Organisations can use the five dimensions as a guide to develop testing and selection criteria to recruit the most appropriate CISO. The dimensions provide specific competencies required to succeed in discharging the strategic responsibilities of a CISO. They can thus be used as testing and selection criteria for assessing and determining a candidate's suitability for the role. Having the right person for the job adds value to the organisation.

This paper also contributes to *theory*. Firstly, it introduces the concept of strategic response to security management, in contrast to incident response. While incident management, which focuses on incidents that may compromise the confidentiality, integrity and/or availability of information resources; there is little emphasis on strategic response. Strategic response is the capacity to detect and respond to changes in parameters within the environment, which were taken into consideration in developing security strategy.

Secondly, it attempts to fill the gap of lacking strategic perspective of security management by introducing the five dimensions of competencies required by CISOs to function as strategists. An understanding of these competencies further provides scholars insight into the strategic role of CISOs.

Thirdly, 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 appropriating insights into the security strategy space.

Limitations and Further Research

This study has the following perceived limitations. First, as this was a conceptual study based on a 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. Second, CISOs with the five dimensions may not be able to overcome all strategic challenges if their position is not strategically placed within the organisational hierarchy. However, Jarzabkowski et al. (2007) argue that not only top management can be strategists; middle-management and non-management employees could be important as strategists. This could be investigated further to determine if and how CISOs who are not occupying a strategic role within their organisations can still influence and shape organisational-level security strategy using the five dimensions. Third, 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. First, 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, organisations can have more refined selection criteria for CISOs depending on where they are in the strategy lifecycle.

Second, 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.

Third, 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., Hadgkiss, J., and Ruighaver, A. B. 2012. "Incident Response Teams – Challenges in Supporting the Organisational Security Function," *Computers & Security* (31:5), pp. 643-652.

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. B., and Park, S. 2014b. "Information Security Strategies: Towards an Organizational Multi-Strategy Perspective," *Journal of Intelligent Manufacturing*:2), p. 357.

Ahmad, A., Maynard, S. B., and Shanks, G. 2015. "A Case Analysis of Information Systems and Security Incident Responses," *International Journal of Information Management* (35:6), pp. 717-723.

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

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

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.

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.

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

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.

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

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), 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.

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.

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

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

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

Kitchenham, B. 2004. "Procedures for Performing Systematic Reviews," *Keele, UK, Keele University* (33:2004), pp. 1-26.

Lim, J. S., Ahmad, A., Chang, S., and Maynard, S. B. 2010. "Embedding Information Security Culture Emerging Concerns and Challenges," *PACIS*, p. 43.

Lim, J. S., Chang, S., Maynard, S., and Ahmad, A. 2009. "Exploring the Relationship between Organizational Culture and Information Security Culture," *Australian Information Security Management Conference*, p. 12.

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.

McFadzean, E., Ezingeard, J.-N., and Birchall, D. 2007. "Perception of Risk and the Strategic Impact of Existing It on Information Security Strategy at Board Level," *Online Information Review* (31:5), p. 622.

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.

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), 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).

Shedden, P., Scheepers, R., Smith, W., and Ahmad, A. 2011. "Incorporating a Knowledge Perspective into Security Risk Assessments," *VINE: The Journal of Information & Knowledge Management Systems* (41:2), pp. 152-166.

Shedden, P., Ahmad A., Ruighaver, A.B., 2010. Organisational Learning and Incident Response: Promoting Effective Learning Through the Incident Response Process. Proceedings of the 8th Information Security Management Conference (pp.139-150), Perth, Australia: Edith Cowan University. 30 Nov – 2nd Dec, 2010.

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*).

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.

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*.

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

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., and Shanks, G. 2014. "A Situation Awareness Model for Information Security Risk Management," *Computers & Security* (44), pp. 1-15.

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review." The Society for Information Management and The Management Information Systems Research Center of the University of Minnesota, and The Association for Information Systems, p. xiii.

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

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