A Minor Research Project (25pts ISYS90044)

The Information Security Manager as a Strategist

Submitted by

Mazino Benson Onibere [602792]

Supervised by

Dr Atif Ahmad and Dr Sean Maynard

04 November 2015

Department of Computing and Information Systems

School of Engineering

University of Melbourne

Abstract

The modern organisation operates within a highly complex and sophisticated security threat landscape that exposes its information infrastructure to a range of security risks. This threat landscape includes advanced persistent threat (APT) – attackers are well-trained, organised, well-funded and capable of utilising a range of technologies to inflict damage over a prolonged period of time (Giura & Wang 2012; Ahmad 2010). 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. The fundamental premise of this thesis is that the level of sophistication of threat requires organisations to develop novel security strategies that draw on creative and lateral thinking approaches. Such a security campaign requires the security manager to function as a 'strategist' by exercising 'strategic thinking'.

A review of security literature found little or no evidence that security managers are able or expected to function as strategists. Therefore this research project aims to identify the specific capabilities required by security managers to become effective strategists. A systematic literature review approach was adopted to determine 1) the existing role of the security manager from security literature, and 2) characteristics of a strategist from the management literature. Findings from a review of these literatures revealed 1) a strategic perspective of Information Security Management is missing, and 2) the management literature identifies a range of characteristics and qualities of a strategist. The latter was coded into the 5 dimensions of the strategist. These 5 dimensions are then discussed in the context of security managers and current strategic challenges facing security management. The result was a set of security capabilities required by security mangers to function as strategists. The thesis outlines implications for further research, including the need to expand the scope of literature review to warfare literature and the need to empirically test the 5 dimensions.

Declaration

I certify that

- this thesis does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any university; and that to the best of my knowledge and belief it does not contain any material previously published or written by another person where due reference is not made in the text
- where necessary I have received clearance for this research from the University's Ethics Committee (Approval Number: N/A) and have submitted all required data to the Department
- the thesis is 8867 words in length (excluding text in images, table, bibliographies and appendices)

…….

Mazino Onibere (602792)

Acknowledgements

To my wife, daughter and son, for their love and understanding.

To my supervisors, for their clear guidance and unwavering support.

Table of Content

1.0 Introduction

Over the years organisations have increasingly become dependent on information and information processing systems for the operation of business processes. Such that the achievement and sustenance of competitive advantage in the highly competitive business market space has become contingent on having the right information resources (McFadzean, Ezingeard & Birchall 2007). The modern organisation operates within a highly complex and sophisticated security threat landscape that exposes its information infrastructure to a range of security risks. This threat landscape includes advanced persistent threats (APT) – attackers are well-trained, organised, well-funded and capable of utilising a range of technologies to inflict damage over a prolonged period of time (Giura & Wang 2012; Ahmad 2010). 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, Bosua & Scheepers 2014). 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, Maynard & Park 2014). The risks to organisations' information resources have thus become significantly heightened and require a novel approach to protection. Traditional approaches, which have remained constant over the years, are losing their relevance today. Information security, as the function responsible for the protection of information by ensuring the confidentiality, integrity and availability of information assets, has consequently increased in relevance to become a business enabling, organisational level strategic function (Kayworth & Whitten 2010).

Novel information security strategies that recognise the complexity of the prevailing threat environment are now therefore required to ensure the adequate security of information resources. The information security manager is now required to be able to develop organisational-level security strategies that drive security policy creation and provide the overall strategic approach in the development and management of the organisation's information security function (Baskerville & Dhillon 2008). It is no longer sufficient to articulate security strategies by adopting a process-based approach in the selection of static security controls; rather, today's security strategies must be fit for purpose and relevant to the organisation and the environment in which it is operating. The strategies need to be flexible, adaptable and readily modifiable in commensuration with a dynamic and volatile environment, while at the same time maintaining rigid alignment with the business strategy. Crafting these business critical security strategies must look beyond the traditional approaches and adopt novel approaches that draw on creative and lateral thinking in order to

contend with evolving and highly sophisticated threat landscape. Developing, implementing and institutionalising these security strategies require the information security manager to effectively become a 'strategist'. This will enable the organisation as a whole to achieve its business goals and objectives.

However, there is little or no evidence in security literature to show that the security manager is required to function as a strategist, and craft effective business aligned security strategies for the organisation. A review of literature shows that though information security management is generally discussed in terms of practices, such as security policy management and security risk management practice areas, there is no practice area dedicated to the development and implementation of security strategy (see Alshaikh et al. 2014). In light of the strategic relevance of the information security function within the organisation and the need for the security managers to become strategists, we may ask: Are security managers capable of assuming a strategic role within the organisation? Do they have the capabilities required to function effectively as a strategist? This thesis therefore poses the following research question:

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

The rest of the thesis is structured as follows: to lay the foundation for the remainder of the thesis, section 2 provides background information on the Information Security function and its associated management practices areas; it mentions the current operational responsibilities of the security manager, the missing strategic perspective, and then describes as a consequence, the strategic challenges faced by security management. A description of security environment and the criticality of strategizing in a dynamic security environment is also included in this section. Section 3 describes how systematic literature reviews were conducted in security literature to identify current roles of security manager and in management literature to identify capabilities and qualities of a strategist. It further describes how the findings from the management literature were coded and condensed into the 5 dimensions of the strategist. These findings were presented in section 4. The first part of which presents the overview of findings from security literature which shows that strategizing activities and strategy formulation are curiously missing; while the second part presents a description of the 5 dimensions of the strategist from the management literature perspective. Section 5 presents a discussion on how security managers exhibiting the capabilities defined within the 5 dimensions of the strategist from the management literature will be able to overcome the ISM strategic challenges presented in the background section. Section 6 provides closing remarks, contribution, limitations of this study and opportunities for further research.

2.0 Background

This section presents foundational information referred to frequently in the remainder of the thesis. Firstly, it describes Information Security Management (ISM) and its current focus on operational activities; secondly it describes the concept of the security environment, noting that the remainder of the thesis focuses on the unstable security environment; and thirdly, it describes strategic challenges currently faced by the ISM.

2.1 Missing Strategic Perspective in Information Security management

Information security (InfoSec) is the function responsible for protecting information assets by safeguarding their confidentiality, integrity and availability, regardless of which form they are in (electronic, physical, otherwise). Information Security Management (ISM) is responsible for the lifecycle of the InfoSec function within an organisation. ISM is responsible for the identification of information assets, determination of possible and probable threats, selection of appropriate safeguards, and ensuring the effective and efficient implementation of selected safeguards. A review of security literature shows that the activities that make up the lifecycle of the InfoSec function within organisations are grouped into practice areas such as security policy management and security risk management (see Alshaikh et al. 2014). While the focus of this thesis is on strategic capabilities of the information security manager, the ISM practice areas present operational responsibilities of the security manager. This apparent lack of strategic perspective is explored in more details in *section 4.1 Role of the information security manager.*

2.2 Criticality of Strategizing in Dynamic Security Environments

Any organisation that has information-intensive business processes, that is successful in any field, that has any form of intellectual property, or that owns critical infrastructure is a likely target for financial gain, espionage and/or sabotage. These organisations fall under the category of unstable security environment. An understanding of the type of organisation helps us understand the nature of threats faced by the organisation. This consequently determines the strategy employed to setup safeguards to protect assets from the threats. Both Ahmad, Maynard and Park (2014) and Baskerville, Spagnoletti and Kim (2014) use the term security environment to describe the state of an organisation with respect to the nature of threats faced, underlying external regulations and expectations, and the security capabilities of the organisation. Baskerville et al. (2014) further divides security environment into stable and unstable. Such that a stable security environment is one

in which the relationship between information assets, threats and security controls is stable, static and predictable; and an unstable environment is one in which the threats are unpredictable and transient with an indeterminate relation between assets, threats and controls. This thesis focuses the criticality of strategizing by security managers in organisations operating in dynamic and unstable security environments.

2.3 Information Security Management Strategic Challenges

This sub-section had been put together following a preliminary review of security literature which reveals a number of key themes brought up by several authors. It provides a detailed description of strategic challenges currently faced by ISM within organisations. The strategic nature of these challenges has in part motivated the need for security managers with strategic perspective.

2.3.1 Evolving Threat Landscape Requires an Innovative Strategy

Traditional information security involved identifying information assets and applying corresponding preventative security measures which were contingent on clearly distinguishable boundary and perimeter (Durbin 2011). However, with advancements and innovations in Information Communications Technology (ICT); and emerging trends such as consumerisation of Information Technology (IT), ubiquitousness of smart devices with high-computing functionalities, bring your own device (BYOD), enterprise mobility and teleworking; employees now have access to company information assets at work, at home and on-the-go (Castro-Leon 2014). Ahmad, Bosua and Scheepers (2014) therefore argue that the risk of leakage of sensitive information has been exacerbated by these boundary spanning technologies and trends which have made the lines of boundary around company information assets become blurred and almost non-existent.

Silic and Back (2014) furthermore demonstrate that the trend of consumerisation of IT – rise of consumer grade IT solutions that appears to meet the needs and wants of the business without having the restrictions imposed by enterprise grade solutions deployed by IT; has led to the phenomenon known as Shadow IT. Such that individual business units now adopt and utilise IT solutions and services for business purposes within the organisation without the knowledge and/or consent of the IT function. The use of personal cloud services for business purposes is a typical example of this phenomenon (Walter 2013). Ahmad, Maynard and Park (2014) suggest that security management's inclination to declare as unsanctioned any technology that they cannot control has further contributed to this phenomenon. Shadow IT clearly does not conform to the organisation's security processes and diminishes the overall security posture of the organisation.

Traditionally 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 financial gain (Smiraus & Jasek 2011; Sood & Enbody 2013; Tankard 2011). Attackers are no longer youngsters, computer whiz kids or any of the other stereotypes associated with hackers; rather, they are entities such as organisations 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, Garg & Summers 2014). Consequently, cyber-attacks have evolved over time and have now become highly sophisticated, and targeted, commonly referred to as the Advanced Persistent Threat (APT). APT is a stealthy form of cyber-attack that is launched at a specific target, using a mixture of sophisticated attack tools and techniques over a long period of time, in order to accomplish a specific objective (Smiraus & Jasek 2011; Sood & Enbody 2013; Tankard 2011). Stuxnet is an example of an APT that exploited multiple zero day vulnerabilities and employed innovative methods to compromise an adequately secured nuclear network environment (Choo 2011).

Therefore, in line with the argument posed by Baskerville 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.

2.3.2 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, Sarkani & Mazzuchi 2011), security management is still seen as an IT problem – to be handled by technical people (McFadzean et al. 2007; Von Solms & von Solms 2004). Kayworth and Whitten (2010) affirm that in organisations with this perception, the strategic business context within which the information assets are utilised is lost. The security manager usually does 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, Torres & Sarriegi 2009). Sveen et al. (2009) argue further that without the strategic and business context, Security activities are skewed towards the operational with a systems-view, resulting in a narrow fit. This operations-focused Security function is thus reactive in nature, and does not support the long-term orientation of the organisation; while a system-centric view lacks alignment with the business objectives.

As a consequence of this narrow view or system-centric focus of the security manager, emphasis is placed on the protection of information and data, with little recognition of knowledge protection

measures and strategies. According to resource based theory, knowledge which is a combination of *experiences, values, contextual information and expert insight,* is considered a source of competitive advantage to an organisation, and should thus be developed and protected as other organisational competitive resources (Ahmad, Bosua & Scheepers 2014). Hall, Sarkani and Mazzuchi (2011) argue that there is a relationship between the performance of an organisation and the Information Security strategy, and that this relationship is contingent on the recognition of organisational capabilities such as knowledge. *An effective security strategy therefore requires a holistic view of the organisation's information assets and a recognition of all organisational capabilities.*

2.3.3 Response to Strategic Change Requires Situational Awareness

Security managers as part of their operational responsibilities respond to technical issues and technical changes but have not been required to recognise and respond to changes in business strategy, the general environment and organisational issues. ISM is usually a part of or affiliated with incident response teams (IRTs) of organisations. These IRTs are required to detect, respond to and resolve incidents. Incident management, the umbrella process which includes incident response, is operational in nature and has the operational priority of recovery from the incident and restoration of service (Tan, Ruighaver & Ahmad 2003).

However, Ahmad, Maynard and Shanks (2015) argue that operational security incidents and seemingly innocuous anomalies are usually pointers to new patterns of attacks and threats; and that if properly investigated and learned from, can result in 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 is instrumental to the detection and identification of changes in the environmental context on which the organisational ability to respond to change is contingent. Unfortunately, as demonstrated by Ahmad, Hadgkiss and Ruighaver (2012) in a case study, organisations are not learning from incidents. As a consequence of poor situational awareness, ISM is not able to respond to changes in the security environmental context within which the organisation is operating. Webb et al. (2014) further argue that 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 situation.

2.3.4 Security Strategy Transcends Compliance

Security strategy developed with the intent of just satisfying compliance requirements does not translate to an effective security posture. Organisations that do not recognise nor understand the relevance of security and the role it needs to play in the organisation but rather are compelled by

regulatory and legal requirements to implement security controls end up having a situation where ISM becomes a compliance problem (Tan et al. 2010). Security requirements are derived from a number of sources such as operational, legal, contractual, regulatory, and competition requirements. Unfortunately due to a systemic issue where there is an inadequate recognition of the value of security in organisations, ISM tends to focus only on compliance requirements. Compliance appears to be the most compelling due to the known fact that lack of adherence results in clearly understood penalties. Security requirements arising from other sources such as operations and those derived from competition are left out. Even though some of the requirements from other sources may be covered by compliance, they are with a different intention and may not have the same outcome. When this occurs, the security managers may either turn to their technical expertise in developing and crafting a technically focused security program or may adopt 'best-practice' international standards and security frameworks such as the ISO 27001, PCI DSS, etc. as part of their security program based on available budget without a contextual understanding of the organisation, the assets to be protected and the prevailing security threat landscape. Thus resulting in a static security strategy that does not take into cognisance any change in environmental context.

As most of these 'best-practice' frameworks include risk management, the risk identification and assessment assumes an orientation towards technical information assets (Shedden et al. 2011); while the security managers thus conduct risks assessments perfunctorily such that significant sources of risk are ignored and risk assessments are performed without appropriate reference the organisation's actual situation (Webb et al. 2014). Furthermore, different security requirements present sources of risk for an organisation's risk management process. A compliance mentality narrows down sources of risk to clearly understood and predictable threats, thus blinding organisations to a number of risks that are equally relevant to the organisation.

2.3.5 Security Strategy Requires Effective Communication

A communication gap has been seen to exist between ISM and senior management or board members of an organisation (Ashenden 2008). This gap in turn 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 not realising security is a business issue rather than technical, is one of the ten deadly sins of information security.

Furthermore, 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 (Alshaikh et al. 2014), has also been seen to be a strategic challenge. In a case study conducted by Ahmad, Maynard and Shanks (2015), it was observed that members of a particular group or unit tend to focus only on what they do, insular about other units and teams. Information within one team is not readily disseminated to other teams within the organisation leading to communication breakdown.

Lastly, creating a culture of security and realising desired behaviour change within the organisation requires effective communication (Lim et al. 2009; Lim et al. 2010; Ruighaver, Maynard & Chang 2007). Unfortunately, inadequate communication with employees by ISM has been the norm in that security managers have relied on one-way communication to broadcast security awareness messages to the people with no means of obtaining relevant feedback (Ashenden & Sasse 2013). Communication sits at the heart of transformation, and if an organisation would transform as a result of its experiences and learnings, then there must be effective communication and collaboration. Security managers need to communicate with senior management, other functional areas and to all employees of the organisation. Poor communication within security management detracts from the overall effectiveness of security practice and the security posture of the organisation.

3.0 Methodology

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

In the management literature, search string used on the Scorpus online database was '*role'* AND '*strategist'*. Initial search yielded 126 articles. After reading the abstracts, keywords and skimming through, the number of relevant articles was reduced 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, an exploratory approach was also used in parallel. This primarily involved trying various keywords using the University of Melbourne's Discovery Search tool for its fast and thorough combination of multiple databases such as AIS, ACM, Emerald, Elsevier etc. 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 management literature. At the end of the exploratory search, the final number of relevant publications from security literature was increased to 20; and from management literature was increased to 55. These were then used for the literature review. Subsequently, each selected publication was read thoroughly.

Relevant *words, phrases and sentences* describing the roles of security managers were extracted from each security literature article. The analysis of the extracted texts revealed that security management roles were discussed predominantly from a functional or practice point of view, rather than in terms of capabilities; furthermore, there was no practice area for strategizing or development of security strategy, see section 4.1.

Similarly, relevant *words, phrases and sentences* describing characteristics of strategists were extracted from each management literature article. The extracted texts were analysed using thematic analysis technique, and were then grouped into 5 categories. These categories of similar capabilities were then named as the 5 dimensions of the strategist, which are described in *section 4.2*.

4.0 The Information Security Manager as a Strategist

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.

4.1 Role of the Information Security Manager

The perceived strategic relevance of information security in an organisation will determine where the role responsible for information security will be placed within the organisational hierarchical structure (Kayworth & Whitten 2010). In organisations where security is perceived to be of strategic value and critical to the attainment and sustenance of competitive advantage, a dedicated executive

level security function may be created such as a chief security officer (CSO) or a chief information security officer (CISO). In other organisations, an existing executive may be assigned the additional role of accountability for security while a senior or middle management level role of the information security manager is responsible for ISM within the organisation. This thesis uses the term information security manager to refer to the position directly responsible for the management of the information security function within the organisation and does not distinguish between the hierarchical level at which the person operates.

To be successful in the ISM practice areas, security managers are required to understand the organisation and industry they are in (Whitten 2008). 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 managers 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 security manager has the responsibility for designing, implementing and managing security safeguards and countermeasures based on risk management. Thus the security manager, 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. Security managers 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 2008; Whitten 2008; Williams 2007).

4.1.1 Gap in Security Literature on the Security Manager as Strategist

As described in section 2.1, developing and executing a security strategy is not considered as an ISM practice area. Though references are made to security strategy and aligning security strategy with business strategy, there is no formal recognition of security strategy as a practice upon which all other security management practice areas are contingent. Furthermore, very little has been mentioned about the role of the security manager as a strategist and security strategizing activities; and also very little has been mentioned about the characteristics or qualities the security manager requires 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 management literature. Hence we turn to management literature to examine the characteristics required for a good strategist and will relate these to the security manager.

4.2 A Management Literature Perspective of a Strategist

As described in the methodology section, a review of management literature revealed a number of characteristics and qualities of a strategist which have been synthesised and condensed into 5 dimensions of the strategist:

1) the dimension of Thought
2) the dimension of Contextualisation
3) the dimension of Execution
4) the dimension of Response
5) the dimension of Advocacy

4.2.1 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). Grazzini (2013) argues that 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. 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, Sambamurthy & Agarwal 2006); and their actions precipitate the creation of new possibilities for the organisation (Carter, Groover & Thatcher 2011).

Kets De Vries (2007) describes the strategist as a person with capacity to think laterally and abstractly. 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).

4.2.2 The Dimension of Contextualisation

The strategist must be able to place strategy in context. Dreams and visions of the future must be juxtaposed with the prevailing environmental context keeping the long term objectives in sight. Mintzberg (1994) argues that 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. They have achieved contextual awareness which is valuable to the crafting and refining of strategy. Watkins (2012) supports this view by further arguing that an 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.

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; Gavetti 2011; Dragoni et al. 2011).

4.2.3 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, Paroutis & Mitson 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 & 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 2012; Hoffmann 2012; Kets De Vries 2007)

4.2.4 The Dimension of Response

A change in environmental context may require a commensurate modification or refinement of strategy. Strategy is not static and should not be cast in stone. 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 a new threat or opportunity has been spotted, 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).

The ability to make quick decisions in the face of changing environmental context is a vital quality of an effective strategist (Breene et al. 2007). The strategist must be able to decide which detected changes in the environment should be responded to, thus avoiding distractions (Beaver 2002).

4.2.5 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 strategist must be

able to sell his 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 things are done in an organisation. 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 & 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).

Mintzberg (1996) describes a category of great strategists as 'generous' because of their ability to "bring strategy out in other people" (p.63). These strategists transform the organisation and create an atmosphere of creativity, strategic thinking and collective learning.

4.3 Summary of characteristics and corresponding references

Characteristics	Capabilities	References
Dimension of thought	▪ Ability to conceptualise ▪ Ability to think creatively ▪ Ability to think imaginatively ▪ Ability to think abstractly ▪ Ability to think laterally ▪ Ability to think to think and devise new solutions without having all facts.	▪ Mintzberg (1996) ▪ Grazzini (2013) ▪ Rooke and Torbert (2005) ▪ Smaltz et al. (2006) ▪ Beaver (2002) ▪ Stopford (2001) ▪ Carter et al. (2011)
Dimension of Contextualisation	▪ Ability to recognise and place strategy in the organisational context, ▪ Ability to assume a holistic/big-picture view ▪ Ability to assume long-term orientation ▪ Ability to maintain a keen awareness of environment.	▪ Watkins (2012) ▪ Carter et al. (2011) ▪ Gavetti (2011) ▪ Dragoni et al. (2011) ▪ Angwin et al. (2009)
Dimension of Execution	▪ Ability to translate vision and strategy into actionable plan, ▪ Ability to execute strategic plan ▪ Ability to ensure alignment of	▪ Angwin et al. (2009) ▪ Hoffmann (2012) ▪ Beaver (2002). ▪ Carter et al. (2011)

	execution with strategic context Ability to provide clear direction for the organisation to follow ▪ Ability to effectively and efficiently allocate of resources ▪ Ability to initiate and lead transformational change	▪ Grazzini (2013) ▪ Kets De Vries (2007) ▪ MacLean and MacIntosh (2015) ▪ Sparrow (2013)
Dimension of Response	▪ Ability to timely detect changes in the environmental context ▪ Ability to agilely respond to strategic changes ▪ Ability to modify or refine strategy as required ▪ Ability to learn and unlearn rapidly as required; ▪ Decisive in the face of change.	▪ Angwin et al. (2009) ▪ Beaver (2002) ▪ Breene et al. (2007) ▪ Carter et al. (2011) ▪ Smaltz et al. (2006)
Dimension of Advocacy	▪ Ability to motivate and inspire ▪ Ability to influence and persuade ▪ Ability to collaborate ▪ Ability to clearly communicate strategy ▪ Skilful at conflict resolution ▪ Ability to negotiate and secure buy-in ▪ Ability to champion a cause	▪ Carter et al. (2011) ▪ Rooke and Torbert (2005) ▪ Breene et al. (2007) ▪ Angwin et al. (2009) ▪ Watkins (2012) ▪ Gavetti (2011) ▪ Smaltz et al. (2006)

5.0 Discussion

The capabilities and qualities of the strategist described in the previous section are equally relevant to the ISM domain. This section describes how an information security manager exhibiting the capabilities defined within each of the 5 dimensions of the strategist from the management literature will be able to overcome the ISM strategic challenges presented in the background section.

5.1 The Information Security Manager and the Dimension of Thought

The strategist's dimension of thought employs creativity and imagination, the ability to think abstractly and laterally in the strategy formulation process. The strategist in this dimension is a visionary and is able to see the world in a way others do not, and is thus able to break new grounds.

Organisations are currently faced with a strategic challenge of a highly complex and evolving threat landscape that renders traditional security approaches ineffective (see *section 2.3.1 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.

Security managers functioning as strategists with the capabilities 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 craft effective strategies without having all the fact or knowing what kind of threats to expect.

The Stuxnet attack as described by Choo (2011), is a typical example of a creative and ingenious threat. Although the target centrifugal environment for the nuclear enrichment process had been 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. The attackers, based on intelligence on their target, provided free USB flash drives to people at a conference attended by employees from the Iranian organisation, amongst others. Eventually, one of those employees plugged the infected USB flash drive into a computer in the centrifugal environment. Protecting information resources from attacks like this that employ ingenious and unconventional combination of methods requires security managers that can draw on creativity, imagination, and the power of abstract and lateral thinking to craft strategies of commensurate ingenuity.

The subject of developing strategies that recognise the novel and unpredictable nature of threats is not new in security literature. Baskerville (2005) argues that the traditional approach to security was premised on the fact that threats were known, static and predictable, thus determinate safeguards could be deployed to sufficiently neutralise the threats. He demonstrated that the *probabilistic* logic behind this traditional approach gave way to a *possibilistic* logic when the threats became unknown, transient, unpredictable, resulting in an indeterminate relationship between safeguards and threats. He argued further that organisations operating in an unstable security environment, need to develop security strategies based on a *possibilistic* logic. T*his thesis therefore posits that security managers 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*.

5.2 The Information Security Manager 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 is struggling with 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 *Section 2.3.4 Security Strategy Transcends Compliance).*

Security managers functioning as strategists with the capabilities 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 craft security strategies that are relevant to the organisation which in turn translate to effective security posture.

Target Corporation had implemented security controls and had been certified to the Payment Card Industry Data Security Standard (PCI DSS) prior to the breach of 2013, thus exemplifying that compliance with standards and/or regulations is not enough (Mello Jr. 2014). Post incident analysis of the breach reveals that the success of the attack was contingent on the attackers' profound understanding of Target's contextual environment (Radichel 2014). Such that, intelligence about Target was obtained from Target's vendors, and one of these vendors' network was then used as launching pad to spread malware into Target's environment. About 40 million credit card details and 70 million personal records of customer were stolen; and up to a net amount of 162 million dollars spent as a direct consequence of the data breach (Lunden 2015; Prince 2015). An effective security strategy must therefore recognise the organisation's contextual environment, which includes the organisation's vendors, contractors, customers, competitors and the complex threat landscape. *This thesis therefore posits that Security managers 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.*

5.3 The Information Security Manager 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. Security managers already develop and execute security programs, allocating resources (people, funds, time) accordingly. However, this execution is done 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 strategies have assumed a narrow and system-centric view such that security controls are implemented to solve technical problems with an operational view (see *section 2.3.2 Security Strategy Requires a Holistic Organisational View).*

Security managers 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 over 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. Security managers 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. Once security managers assume a strategic role, the supposedly usual annual system-centric security programs and roadmaps will then be derived from the security strategy and represent actionable strategic plan. *This thesis therefore argues that Security managers must provide clear vision and direction that is translated into an actionable plan that is implemented within the organisational context using efficient and effective allocation of resources.*

5.4 The Information Security Manager 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, as described in *section 2.3.3 Response to Strategic Change Requires Situational Awareness*, organisations are not learning from security incident response process, and thus are not able to derive 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; and the outcome of risk management process is not a true reflection of the organisation (Webb et al. 2014; Shedden, Ruighaver & Ahmad 2010).

Security managers as strategists functioning in the dimension of response recognise that the security environment is subject to change, 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 to detect and respond to the need for changes in strategy. This is in agreement with Baskerville et al. (2014) who argue that there is a paradigmatic difference between 'prevention' and 'response' – such that while *prevention* seeks to prevent security incidents from occurring by implementing controls against known and predictable threats; *response* tends to develop detection and response capabilities that allow detection of unpredictable and novel threats and thus set up controls in an exploratory manner. A dynamic strategy would thus be one that strikes the right balance between the two paradigms of prevention and response (Baskerville et al. 2014). Security managers 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 (Ahmad, Maynard & Shanks 2015; Webb et al. 2014). 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 to develop response capability, to ensure timely detection of incidents and development of corresponding response capability. This thesis therefore extends existing knowledge in security literature by introducing the concept of strategic response in contrast to incident response. *It argues that Security managers must be able to detect and respond to strategic changes within the environmental context and decisively modify security strategy as required*

5.5 The Information Security Manager 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 security management 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 *section 2.3.5 Security Strategy Requires Effective Communication*). Furthermore, a number of reports and surveys attribute a significant percentage of security breaches within organisations to a human problem. For instance, IBM Security Services (2014) in their 2014 Cyber Security Intelligence Index report, attributed over 95 percent of all incidents they investigated worldwide over the course of the previous year to having human error as a contributing factor. Where human error includes system misconfiguration, poor patching, use of default user names and passwords or poor passwords, lost laptops or mobile devices, and inadvertent disclosure of information, opening infected attachments and clicking unsafe URLs (IBM Security Services 2014).

Security literature already recognises the security manager as the spokesperson for security and is required to function as advocate for security within the organisation (see 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 (see section 2.1 Missing Strategic Perspective in Information Security management). While championing a SETA program is operational function, championing the Security strategy is strategic. Furthermore, the alarming statistics of human related factors responsible for successful security incidents can be construed as a failure of security management to inspire and instil a culture of security within the organisations via existing SETA programs.

Security managers operating as strategists within the dimension of advocacy are then 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 security managers 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 thesis therefore argues that Security manager must be able to clearly communicate strategy in order to motivate and influence relevant stakeholders towards inspiring a shared vision of information security.

5.6 Summary of Dimensions

Characteristics	*Summary of Security Capability*
Dimension of Thought	*Security managers 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*
Dimension of Contextualisation	*Security managers 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*
Dimension of Execution	*Security managers must provide clear vision and direction that is translated into an actionable plan that is implemented within the organisational context using efficient and effective allocation of resources*
Dimension of Response	*Security managers must be able to detect and respond to strategic changes within the environmental context and decisively modify security strategy as required*
Dimension of Advocacy	*Security manager must be able to clearly communicate strategy in order to motivate and influence relevant stakeholders towards inspiring a shared vision of information security*

6.0 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 security managers to function as 'strategists' capable of crafting security strategies that will enable organisations to achieve their goals and objectives.

This thesis set out to answer the research question: w*hat characteristics are required by the information security manager to effectively function as a strategist?* It was observed that the security literature had no practice area for security strategizing activities, neither was there any evidence to show that security managers were required to function as strategists. Furthermore, security management within organisations is currently assailed by 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 perspective and develop strategic capabilities before it can overcome these challenges.

We subsequently went into the management literature and identified a number of characteristics and qualities of the strategist, which were then coded using thematic analysis and condensed into the 5 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 thesis posits that security managers require the capabilities inherent in the 5 dimensions to function effectively as strategists. It further argues that security managers with these 5 dimensions are able to overcome the current strategic challenges faced by security management.* 1) In the *dimension of thought*, security managers are able to draw on creative, imaginative, abstract, lateral thinking approaches towards developing novel security strategies to address the highly complex and evolving threat landscape in the face of uncertainty. 2) In the *dimension of contextualisation*, security managers maintain a keen awareness of the environment and are thus able to develop long term, holistic and organisationally relevant security strategies that transcend mere compliance. 3) In the *dimension of execution*, security managers are able to provide clear vision and direction which can be translated into actionable plan and

implemented within the organisational context to overcome the challenge of narrowness and system-centric execution of security controls. 4) In the *dimension of response*, security managers are able to detect and respond to strategic changes within the environmental context and decisively modify security strategy accordingly, by achieving and maintaining situation awareness through rapid learning and unlearning, as required. 5) In the *dimension of advocacy*, security managers are able to break up existing communication gaps by being able to clearly communicate strategy in order to motivate and influence relevant stakeholders towards inspiring a shared vision of information security.

6.1 Contributions

This thesis contributes to *practice*. The 5 dimensions can be used by organisations as a guide to develop testing and selection criteria to recruit the most appropriate security manager. The dimensions provide specific capabilities required to successfully fulfil the strategic responsibilities of a security manager. 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 thesis 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, is well recognised within the security management domain; 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 the crafting of security strategy.

Secondly, it attempts to fill the gap of lacking strategic perspective of security management by introducing the 5 dimensions of capabilities required by security managers to function as strategists. An understanding of these capabilities further provides insight into what is expected of the strategic role of security managers. It is thus hoped that this will pave the way for further research into this strategic perspective until it matures into one of the security management practice areas, just as risk management and policy management areas.

Thirdly, this thesis 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.

6.2 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 security managers may overcome current strategic ISM challenges, using the capabilities of the 5 dimensions of the strategist.

Furthermore, security managers with the 5 dimensions may not be able to overcome all the strategic challenges if their position is not strategically placed within the organisational hierarchy. However, Jarzabkowski, Balogun and Seidl (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 security managers who are not occupying a strategic role within their organisations can still influence and shape organisational-level security strategy using the 5 dimensions.

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

The following represent additional opportunities for further research. Firstly, as the 5 dimensions represent different types of skills and capabilities that are required at different stages of strategy formulation and strategizing activities. Each dimension and their inherent capabilities should be investigated to determine which is most suitable for each stage of the strategy lifecycle. Consequently, organisations can have a more refined selection criteria for security managers depending on where they are in the strategy lifecycle.

Secondly, further research is required in defining and articulating a practice area for the security strategy practice area. 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 have not been relevant to management strategy, are relevant to security. These characteristics would then be used to expand and enrich the 5 dimensions presented in this thesis.

Finally, each of the 5 dimensions appears to resonate with a personality type, for example, the dimension of thought points to a thinker, while the dimension of execution a doer. 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 security manager 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.

7.0 Reference

Ahmad, A. (2010). Tactics of Attack and Defense in Physical and Digital Environments: An Asymmetric Warfare Approach. *Journal of Information Warfare, 9*(1), 46-57.

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security, 42*, 27-39. doi: http://dx.doi.org/10.1016/j.cose.2014.01.001

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams – Challenges in supporting the organisational security function. *Computers & Security, 31*(5), 643-652. doi: http://dx.doi.org/10.1016/j.cose.2012.04.001

Ahmad, A., & Maynard, S. (2014). Teaching information security management: reflections and experiences. *Information Management & Computer Security, 22*(5), 513-536. doi: 10.1108/IMCS-08-2013-0058

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: towards an organizational multi-strategy perspective. *JOURNAL OF INTELLIGENT MANUFACTURING*(2), 357.

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management, 35*(6), 717-723. doi: http://dx.doi.org/10.1016/j.ijinfomgt.2015.08.001

Alshaikh, M., Ahmad, A., Maynard, S. B., & Chang, S. (2014). *Towards a Taxonomy of Information Security Management Practices in Organisations*.

Angwin, D., Paroutis, S., & Mitson, S. (2009). Connecting Up Strategy: ARE SENIOR STRATEGY DIRECTORS A MISSING LINK? *California Management Review, 51*(3), 74-94.

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report, 13*(4), 195-201. doi: 10.1016/j.istr.2008.10.006

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers and Security, 39*(PART B), 396-405. doi: 10.1016/j.cose.2013.09.004

Baskerville, R. (2005). Information warfare: a comparative framework for business information security. *Journal of Information System Security, 1*(1), 23-50.

Baskerville, R., & Dhillon, G. (2008). Information Systems Security Strategy: A Process View. *ADVANCES IN MANAGEMENT INFORMATION SYSTEMS, 11*, 15-45.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management, 51*(1), 138-151. doi: http://dx.doi.org/10.1016/j.im.2013.11.004

Beaver, G. (2002). The chief executive officer: showman, statesman and strategist. *Strategic Change, 11*(6), 287-289. doi: 10.1002/jsc.592

Breene, R. T. S., Nunes, P. F., & Shill, W. E. (2007). THE CHIEF STRATEGY OFFICER. *Harvard business review, 85*(10), 84-93.

Carter, M., Grover, V., & Thatcher, J. B. (2011). The emerging CIO role of business technology strategist. *MIS QUARTERLY EXECUTIVE, 10*(1), 19-29.

Castro-Leon, E. (2014). Consumerization in the IT Service Ecosystem. *IT Professional, 16*(5), 20-27. doi: 10.1109/MITP.2014.66

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*, 719-731. doi: 10.1016/j.cose.2011.08.004

Dawson, M., Burrell, D. N., Rahim, E., & Brewster, S. (2010). EXAMINING THE ROLE OF THE CHIEF INFORMATION SECURITY OFFICER (CISO) & SECURITY PLAN. *Journal of Information Systems Technology & Planning, 3*(6), 1-5.

Denning, D. E. R. (1999). *Information warfare and security* (Vol. 4): 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), 829-864. doi: 10.1111/j.1744-6570.2011.01229.x

Durbin, S. (2011). Information security without boundaries. *Network Security, 2011*(2), 4-8. doi: 10.1016/S1353-4858(11)70013-7

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), 257-263. doi: 10.1080/10658980701746577

Forte, D. V. (2009). The role of the Information Security Manager in cutting-edge companies. *Network Security, 2009*(8), 4-5. doi: 10.1016/S1353-4858(09)70073-X
Gavetti, G. (2011). The New Psychology Of Strategic Leadership. *Harvard business review, 89*(7/8), 118-125.
Giura, P., & Wang, W. (2012, 14-16 Dec. 2012). *A Context-Based Detection Framework for Advanced Persistent Threats.* Paper presented at the 2012 International Conference on Cyber Security.
Grazzini, F. (2013). How do managers make sense of strategy? *European Business Review, 25*(6), 484-517. doi: 10.1108/EBR-12-2012-0074
Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security, 19*(3), 155-176. doi: 10.1108/09685221111153546
Hoffmann, L. (2012). Q&A: Chief Strategist (Vol. 55, pp. 120-119): Association for Computing Machinery.
Jarzabkowski, P., Balogun, J., & Seidl, D. (2007). Strategizing: the challenges of a practice perspective. *Human Relations, 60*(1), 5-27 23p.
Jim, J. S., Chang, S., Maynard, S. B., & Ahmad, A. (2009). Exploring the Relationship between Organizational Culture and Information Security Culture: Research Online, 2009-12-01T08:00:00Z.
Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS quarterly executive : a research journal devoted to improving practice, 9*(3), 163-175.
Kets De Vries, M. F. R. (2007). Decoding the Team Conundrum: The Eight Roles Executives Play. *Organizational Dynamics, 36*(1), 28-44.
Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University, 33*(2004), 1-26.
Lim, J. S., Ahmad, A., Chang, S., & Maynard, S. B. (2010). *Embedding Information Security Culture Emerging Concerns and Challenges.* Paper presented at the PACIS.
Lim, J. S., Chang, S., Maynard, S., & Ahmad, A. (2009). *Exploring the relationship between organizational culture and information security culture.* Paper presented at the Australian Information Security Management Conference.
Lindup, K. (1996). Role of information security in corporate governance. *Computers and Security, 15*(6), 477-485. doi: 10.1016/S0167-4048(97)83121-5
Lunden, I. (2015). Target Says Credit Card Data Breach Cost It $162M In 2013-14. Retrieved 23 October 2015, from http://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14/
MacLean, D., & MacIntosh, R. (2015). Planning reconsidered: Paradox, poetry and people at the edge of strategy. *EUROPEAN MANAGEMENT JOURNAL, 33*(2), 72-78. doi: 10.1016/j.emj.2015.02.003
McFadzean, E., Ezingeard, J.-N., & 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), 622.
Mello Jr., J. P. (2014). Target breach lesson: PCI compliance isn't enough. Retrieved 23 October 2015, from http://www.technewsworld.com/story/80160.html
Mellott, M., Thatcher, J., Roberts, N., & Carter, M. (2012). An Examination of the Role of Military Medical Chief Information Officer. *Military Medicine, 177*(7), 850-855.
Mintzberg, H. (1994). Rethinking Strategic Planning Part I: Pitfalls and Fallacies. *Long Range Planning, 27*(3), 12-21.
Mintzberg, H. (1996). MUSINGS ON MANAGEMENT. *Harvard business review, 74*(4), 61-67.
Montgomery, C. A. (2008). Putting leadership back into strategy. *Harvard business review, 86*(1), 54-60+134.
Prince, B. (2015). Target Data Breach Tally Hits $162 Million in Net Costs. Retrieved 23 October 2015, 2015, from http://www.securityweek.com/target-data-breach-tally-hits-162-million-net-costs
Radichel, T. (2014). Case Study: Critical Controls that Could Have Prevented Target Breach Retrieved 23 October 2015, from https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412
Rooke, D., & Torbert, W. R. (2005). 7 Transformations of Leadership. *Harvard business review, 83*(4), 66-76.
Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*, 56-62. doi: 10.1016/j.cose.2006.10.008
Schiavone, S., Garg, L., & Summers, K. (2014). Ontology of Information Security in Enterprises. *Electronic Journal Information Systems Evaluation Volume, 17*(1).
Services, I. S. (2014). 2014 Cyber Security Intelligence Index. Retrieved 23 October 2015, from http://www-03.ibm.com/security/services/2014-cyber-security-intelligence-index-infographic/index.html
Shedden, P., Ruighaver, A. B., & Ahmad, A. (2010). Risk Management Standards - The Perception of ease of use. *Journal of Information System Security, 6*(3), 23.

Shedden, P., Scheepers, R., Smith, W., & Ahmad, A. (2011). Incorporating a knowledge perspective into security risk assessments. *VINE: The Journal of Information & Knowledge Management Systems, 41*(2), 152-166. doi: 10.1108/03055721111134790

Silic, M., & Back, A. (2014). Shadow IT – A view from behind the curtain. *Computers & Security, 45*, 274-283. doi: 10.1016/j.cose.2014.06.007

Smaltz, D. H., Sambamurthy, V., & 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), 207-222. doi: 10.1109/TEM.2006.872248

Smiraus, M., & Jasek, R. (2011). RISKS OF ADVANCED PERSISTENT THREATS AND DEFENSE AGAINST THEM. *Annals of DAAAM & Proceedings*.

Sood, A. K., & Enbody, R. J. (2013). Targeted Cyberattacks: A Superset of Advanced Persistent Threats. *IEEE Security & Privacy Magazine, 11*(1), 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), 8-10. doi: 10.1108/14777281311315838

Stopford, J. (2001). Should Strategy Makers Become Dream Weavers? *Harvard business review, 79*(1), 165-169.

Sveen, F. O., Torres, J. M., & Sarriegi, J. M. (2009). Blind information security strategy. *INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION, 2*(3), 95-109.

Tan, T., Ruighaver, A., & Ahmad, A. (2003). *Incident Handling: Where the need for planning is often not recognised.* Paper presented at the 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), 16. doi: 10.1016/S1353-4858(11)70086-1

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, 23*(5), 371-376. doi: http://dx.doi.org/10.1016/j.cose.2004.05.002

Walters, R. (2013). Bringing IT out of the shadows. *Network Security, 2013*(4), 5-11. doi: http://dx.doi.org/10.1016/S1353-4858(13)70049-7

Watkins, M. D. (2012). How Managers Become Leaders. *Harvard business review, 90*(6), 64-72.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security, 44*, 1-15. doi: http://dx.doi.org/10.1016/j.cose.2014.04.005

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review, xiii.

Whitten, D. (2008). THE CHIEF INFORMATION SECURITY OFFICER: AN ANALYSIS OF THE SKILLS REQUIRED FOR SUCCESS. *JOURNAL OF COMPUTER INFORMATION SYSTEMS, 48*(3), 15-19.

Williams, P. (2007). Executive and board roles in information security. *Network Security, 2007*(8), 11-14. doi: 10.1016/S1353-4858(07)70073-9