CYBER RESILIENCY FOR DIGITAL ENTERPRISES: A STRATEGIC LEADERSHIP PERSPECTIVE

Authors:

J. Loonam, J.B. Zwiegelaar, V. Kumar, C. Booth

Abstract

As organizations increasingly view information as one of their most valuable assets, which supports the creation and distribution of their products and services, information security will be an integral part of the design and operation of organizational business processes. Yet, risks associated with cyber attacks are on the rise. Organizations that are subjected to attacks can suffer significant reputational damage as well as loss of information and knowledge. As a consequence, effective leadership is cited as a critical factor for ensuring corporate level attention for information security. However, there is a lack of empirical understanding as to the roles strategic leaders play in shaping and supporting the cyber security strategy. This study seeks to address this gap in the literature by focusing on how senior leaders support the cyber security strategy. The authors conducted a series of exploratory interviews with leaders in the positions of Chief Information Officer, Chief Security Information Officer, and Chief Technology Officer. The findings revealed that leaders are engaged in both transitional, where the focus is on improving governance and integration, and transformational support, which involves fostering a new cultural mindset for cyber resiliency and the development of an ecosystem approach to security thinking.

Managerial relevance statement

Our findings provide interesting insights for managers particularly those in the role of Chief Information Officers (CIOs), Chief Security Information Officers (CSIOs), and Chief Technology Officers (CTOs). We propose a Cyber Security Strategy Framework (CSSF) which can be used by these information/technology managers to design an effective organizational strategy to develop cyber resilience in their organization. Our framework suggests that managers should focus on transitional and transformational support. The transitional support focuses on improving governance and integration whereas transformational support focuses on the emphasis of fostering a new cultural mindset for cyber resiliency and the development of an ecosystem approach to security thinking. Our findings provide good evidence showing how leaders can support more effective cyber security initiatives.

Keywords: *Cyber Security, Leadership, CIO, CISO, Qualitative inquiry, Interviews.*

1. INTRODUCTION

Organizations that are subjected to attacks can endure significant reputational damage as well as loss of information and knowledge. The emergence of digital technologies is providing enormous opportunities for work and is supporting the emergence of the digital enterprise. Loonam et al. (2018) highlights that digital enterprises are empowered by the deployment of information systems that combine three key technologies, namely; (i) virtualization systems, e.g. cloud computing (ii) mobility systems, e.g. social media, the Internet of Things, smartphones and tablets, and (iii) embedded analytics systems, e.g. big data. They further assert that these three technologies are supported with integrated back-office information systems such as Enterprise Systems, that are enabling the emergence of digital enterprises. Digital native organizations, such as Facebook, Google, Airbnb, and Uber, are illustrating the significant advantages that can be accrued by leveraging Information Systems (IS) to become digital enterprises. For example, according to a McKinsey Global Institute report, the networking efficiencies and opportunities created by the Internet of Things may have a global impact of as much as $11 trillion per year by 2025 across multiple sectors (Deichmann et al., 2015). As organizations rush to embrace digital technologies, they will continue to move greater amounts of in-house corporate data online, look for more interconnected approaches to supply chain integration, and provide their employees, customers, and business partners with greater access to internal information assets and capabilities.

While digital transformation initiatives offer enormous opportunities, it often requires

rethinking a company's business model, restructuring organizational design, and implementing a new digital cultural mindset. Invariably, such initiatives require organizations to become more porous, allowing a more seamless flow of information from inside to outside between stakeholders. Such a seamless approach to information potentially opens the organization, and its respective stakeholders whether employees, customers or suppliers, to significant cyber attack risks. According to a report commissioned by the Department for Culture, Media, and Sport, for example, 46% of UK businesses experienced a security breach in 2016 (McGoogan, 2017). As Samtani et al. (2017: 1024) note "cyber attacks, or the deliberate exploitation of computer systems through the use of malicious tools and techniques such as Ransomware, Zeus Trojans, and Keyloggers, cost the global economy approximately $445 billion per year and have negatively affected health-care organizations like Premera Blue Cross, government entities such as the Office of Personnel Management (OPM), and large retail and consumer companies including Target, Home Depot, Sony, and Xbox Live". In 2017 a global ransomware attack, known as 'WannaCry', affected more than 200,000 computers in at least 100 countries and in the UK particularly, this affected the National Health Services (NHS) England, who declared the cyber-attack a major incident and implemented its emergency arrangements to maintain health and patient care (NAO, 2018). Similar frequent ransomware and cyber-attacks have become a common practice these days. The Federation of Small Businesses (FSB) in the UK reports that the annual cost of the attacks is estimated to be £4.5bn, with the average cost of an individual attack amounting to £1,300 and almost 10,000 cyber-attacks per day. These growing cyber-attacks have compelled organizations to re-think the ways of effectively dealing with such issues.

As stated earlier, cyber security has gained prominent attention in the worldwide

media in recent years due to numerous cyber-attacks. The term cyber security is often used interchangeably with information security, however, Solms and Van Niekerk (2013) contended that there is a substantial overlap between *cyber security* and *information security* as these two concepts are not totally analogous. They also suggest that *cyber security* goes beyond the boundaries of traditional *information security* to include not only the protection of information resources, but also that of other assets, including the person him/herself. While an information system prevails in all aspects of a firm's value chain, Dutta, and McCrohan (2002) emphasized that senior management must play a much more significant role in maintaining security of their organization. Many organizations are thus investing in early detection of cyber security events such as attacks however predicting such events is a challenging task given the constantly evolving threat landscape. In the era of industry 4.0, emerging technologies such as social media, cloud computing, smartphone technology, and Internet of Things (IoTs) amongst others are leading to new attack patterns which further increases the complexity of effectively dealing with those threats. However, many researchers such as Narayanan et al. (2018), Arabo (2015) and others have proposed various methods to assist security analysts.

Cybersecurity affects enterprises in that it affects and impacts on their knowledge management. Cyber security is more than just the technologies used; rather it affects business intelligence (Tisdale, 2015). There are important challenges to ensure that information about the business is protected. Within the context of cybersecurity strategy there are some key discussions about the use and application of the strategies to business and countries. Cyber threats are increasingly persistent, severe and becoming more frequent. A company's cyber risk profile is a function of its' threats, vulnerabilities, the cyber security environment, and company internal mitigation

strategies. Threats and weaknesses increase cyber risk, while a company's mitigation acts and the cybersecurity environment lowers the risk (Hiller & Russel, 2013). Business intelligence requires integration of the strategies for both the business and it functions to ensure cyber-resiliency. The alignment improves better business processes and business performance (McGoogan, 2017; Mircea & Andreescu, 2009).

There are some specific actions needed to consider how to deal with cybersecurity in practice. There are some useful and suggested principles, which the EU strategy on this issue of cybersecurity has outlined. The overarching principles of the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" (EC, 2013) of making sure that digital exchanges are open to all, democratically governed and provided and conducted safely in a positive environment of shared responsibility are the guiding principles for future action. Within this context, various stakeholders are considered in order to make sure that the digital exchanges are open to all. While these are useful principles, there are challenges in relation to data (Mircea and Andreescu, 2009). Although wider access to data in business might be needed, it potentially allows for security issues such as 'breaches' to take place more frequently (McGoogan, 2017). Business intelligence is needed to ensure that the decision making about the use of data takes account of both internal and external stakeholders needs (Dayal et al., 2009). Invariably, it is about ensuring that the roles and responsibilities for particular access levels are appropriate and that there is clear guidance within and across the organization clearly communicated to the employees (Guo et al., 2009; Siponen, Mahmood, & Pahnila, 2009). A culture of trust is thus required to engage with top-down direction, formal communication, or programmed training but there needs to be building a bottom-up level of understanding for the potential risks and threats confronting the organization. Belanger et al. (2017) demonstrated that the levels of

trust lead to better outcomes for preventing cybersecurity issues and engendering a shared responsibility for security. Ultimately, a proactive approach to information security across the organization leads to more willing involvement among employees and invariably promotes a culture of trust rather than suspicion. Specific processes are required to ensure that the employees are operating in an environment that is safe but also allows them to carry out their normal functions.

This study therefore seeks to address the gap in the literature by focusing on how senior leaders support the cyber security strategy. The next section provides a review of the strategic, information systems and operational management literature, summarizing the continued lack of empirical understanding of the proposed study. An overview of the research design is provided thereafter, before discussing data collection, and analysis, and the emerging findings.

2. Information Systems Security Management

The concept of Information Systems Security (ISS) has been important to the field of Information Systems (IS) over the past decades, with studies first appearing in IS journals in the early 1990s (Nazareth and Choi, 2015). Briefly reviewing the ISS literature from top IS journals, we find that the field has focused on a range of topics over the past decades, most notably from security risk management (Straub and Welke, 1998; Chen et al., 2011), security training and awareness (D'Arcy et al., 2009; Bulgurcu et al., 2010; Karjalainen and Siponen, 2011; Tsohou et al, 2012; Benson et al, 2015), information security and individual/employee behaviors (Goodhue and Straub, 1991; Frank et al., 1991; Liang and Xue, 2010; Anderson and Agarwal, 2010; Guo et al, 2011; Yoon and Kim, 2013; Boss et al., 2015; Chatterjee et al., 2015; Dang-Pham et al, 2017; and Bélanger et al, 2017), deployment of security resources (Gordon, 2006; and

Nazareth and Choi, 2015), information security and IT outsourcing (Hui et al., 2012 and Dhillon et al., 2017), security standards and policy compliance (Siponen and Willison, 2009; Siponen et al., 2009; Chen et al., 2012; and Doherty and Tajuddin, 2018), employee motivation and participation, (Johnston and Warkentin, 2010; Spears and Barki, 2010; Son, 2011; Vance et al., 2012; and Menard et al., 2017), security deterrence (Herath and Rao, 2009; and Hu et al, 2011), and organizational- level issues (Straub, 1990; Dhillion and Backhouse, 2001; Hu et al., 2007; and Guo, 2012).

Research into ISS has paralleled the path of general IS inquiry (where information systems have evolved from functional-level to enterprise-wide systems), with an initial focus on technical solutions followed by a greater call for organizational-wide scrutiny. As organizations increasingly view information as one of their most valuable assets, which support the creation and distribution of their products and services, information security will be an integral part of the design and operation of organizational business processes, rather than as a separate issue (Doherty and Tajuddin, 2018). This was also echoed by Dutta and McCrohan (2002) who highlighted that most organizations recognize the need to secure their information assets, however, they largely view it mainly as a technical problem to be addressed by system managers and/or the IT function. They further assert that security is not a technical issue; rather a management issue and it should be dealt with seriously.

In particular, strategic leadership support is cited as a critical factor for ensuring corporate level attention for information security (Dutta and McCrohan, 2002; Ezingeard and Bowen-Schrire, 2007; Hu et al., 2012; Kwon et al, 2012; Soomro et al., 2016; and Barton et al., 2016). Yet, within the ISS literature there has been a lack of empirical evidence exploring how senior leaders can support information security. Hu et al. (2012) for example, noted that the ISS literature has primarily adopted an

employee-centric perspective when exploring information security, however, a focus on strategic leadership support has remained somewhat opaque. Similarly, Barton et al. (2016: 9) noted that while "research has shown that senior management participation is critical to IS security, it has not explained how senior managers are motivated to participate in IS security". Soomra et al. (2016), found that while the topic of management's role in ISS has become critical, research needs a more holistic understanding of how strategic leaders support IS security.

A brief review of strategic leaders supports from an IS perspective, reveals the enduring and perennial importance of the topic in the last decades (Kriebel, 1968, Doll, 1985, Jarvenpaa and Ives, 1991, Dong et al., 2009, and Loonam et al., 2014). Dong et al. (2009), noted, from in-depth case studies at two Canadian Universities, that strategic leadership support for IS requires three distinct types of approaches, that is actions that supply key resources such as; technologies, staff, user training, change management actions where top managers foster organizational receptivity for a new IS, and finally vision-sharing support actions that ensure lower-level managers develop a common understanding of the core objectives for new IS. Similarly, Loonam et al. (2014), in conducting a literature review of strategic leadership support for IS initiatives, posited that the concept of CEO involvement and participation involves a multi-faceted approach. For example, the authors found that top managers would need to apply a number of levers when supporting IS-enabled change initiatives, which include the importance of maintaining a positive attitude towards change, building an effective and powerful coalition group, creating an inclusive steering committee, developing a strong vision for IS across the organization, aligning the IS strategy with the corporate strategy, communicating the IS initiative across the entire organization, and providing sufficient resources for the IS initiative.

Yet, similar to the ISS literature, Dong et al. (2009) highlighted that despite the general consensus regarding the critical role of strategic leaders in the information systems implementation process, the literature has not yet provided a clear and compelling understanding of the strategic leadership support concept. Focusing on the critical importance of cyber security for organizations, and the importance of protecting customers, suppliers, employees, and broader eco-system stakeholders, exploring how strategic leaders support ISS is of paramount importance. In fact, Von Solms and Van Niekerk (2013) note that strategic leadership support for cyber security initiatives has greater consequences for organizations, their employees, and respective industry stakeholders.

The case literature notes that 'cyber security issues should be every executives job', where top managers should liaise with the chief information security officers to fully grasp the challenges associated with cyber attacks, provide adequate training to employees, and conduct a thorough annual risk assessment of information assets (Sweeney, 2016). Similarly, Bailey et al. (2014) noted that top managers play a critical role in advancing the cause of cyber security performance across the organization. The authors note that senior leaders can engage a number of actions to improve cyber security initiatives, most notably by ensuring effective governance and reporting is in place, model their own behavior so that lower level managers can adapt and correspond accordingly, drive consideration for cyber security implications across business functions, and finally assess risk and cyber security issues strategically with the organization.

3. RESEARCH METHODOLOGY

The lack of developed empirical understanding of how strategic leaders can support ISS, and more specifically cyber security initiatives, dictates an exploratory approach to inquiry. Traditionally many IS and ISS studies have relied on positivist approaches for investigation due to the focus on functional-level IS applications and systems implementations (Orlikowski and Baroudi, 1991). Similarly, as organizations move to become digital enterprises, securing information assets from cyber attacks will require a more holistic approach from strategic leaders. To explore this holistic approach, and understand the social and organizational nuances of systems, this study adopts a qualitative approach to inquiry.

The qualitative interview is particularly suited to studies that are seeking to explore a phenomenon or topics (Chinedu Eze et al., 2014). Myers and Newman (2007) identify the qualitative interview as the most common and one of the most important data gathering tools in qualitative research. This study conducted unstructured and semi-structured interviews between February and August 2019. In total, eight interviews were held with participants at Chief Information Officer (CIO), Chief Technology Officer (CTO) and Chief Information Security Officer (CISO) levels (see Appendix 1 for List of Interviewees). The interviewee sample was generated from the authors' respective searches of LinkedIn under the search terms "CIO" or "CISO" across the UK and Ireland. Over 100 potential interviewees s were approached for interview. Authors worked from a list of seven key questions that guided the interview process (see Appendix 2 for Interview Theme Sheet). Prior to interview commencement, key interviewees s were informed, via e-mail, as to the nature of the research inquiry and the forthcoming interview. Similar to Koh et al. (2004), note taking was the preferred approach to data collection as the researchers felt it would allow the conversation to develop more naturally. All interviews were written up directly after each session. Interviews were

scheduled for a 30-45 minutes long session. The interviewers also kept memos of each meeting, which in turn assisted with the process of probing and questioning the data. Such an approach greatly facilitated with sharpening and focusing future interview sessions.

The authors adopted a 4-stage approach to the design of research analysis, following perspectives from grounded theory (Strauss and Corbin, 1997) and thematic analysis (as documented by Chinedu Eze et al, 2014) for data analysis. The stages included (i) theoretical sampling-where the research allowed current data sampling to drive future data collection, (ii) opening the data and the emergence of codes, (iii) creating higher order categories and (iv) selecting key themes and interpretation of codes with literature. (See Appendix 3 for sample coding sheet). Braun and Clarke (2006) highlights that this is a method of searching, identifying, analyzing, and reporting themes that is important to the phenomenon being investigated.

The first stage of the research design began with theoretical sampling. The initial interest in this study stemmed from the lead researcher's ongoing empirical interest in the topic of strategic leadership and information systems. A preliminary review of the IS security literature revealed the importance of effective leadership in delivering successful cyber strategies. Yet, as noted above there has been a lack of empirical understanding about this issue. The second stage of data analysis involved 'opening the data' to allow codes to emerge. This involved looking for patterns and reoccurring events in the data by constantly comparing the data. As Goulding (2002) noted, interview, observational and other data forms are broken down into distinct units of meaning, which are then labelled to generate concepts. The third stage of the research design involved creating higher order categories, where the emerging concepts are clustered into descriptive categories that help to provide clarity around key patterns or

activities of the phenomenon under inquiry. The final stage of the research design involved the selection of key themes, which are further compared to the extant literature in order to verify and validate data. Four themes were selected to support the development of an organizing framework. These themes includes (i) governance-how organizations prepare leaders to manage cyber security programs, (ii) integration-how the organization integrates both back office and front office IT systems and business processes, (iii) fostering a cyber resilient culture-how employees and extended organizational stakeholders develop a culture of trust to overcome cyber threats, and lastly (iv) developing a cyber resilient ecosystem-where the organization is clear about its partners, industry and entire business ecosystem.

4. ANALYSIS & FINDINGS

Throughout the interviewing process key themes began to emerge from the data. The authors found eight themes that help to explain how leaders can support cyber resiliency across their respective organizations, these include:

1. Ensuring cyber strategy is aligned to business strategy-otherwise there is the possibility of viewing the initiative as an IT project;
2. Rethinking organizational "business processes" and their susceptibility to cyber risk/threats;
3. Fostering a "culture of trust" across the organization, where cyber resiliency becomes part of employee and team behavior;
4. Making "cyber resiliency" a key competency/capability of organization- many interviewees spoke of the importance of viewing cyber resiliency as a key capability rather than "just another project" that will lose importance as newer initiatives are launched;

5. Ecosystem-Understanding "partners/suppliers' relationships" in value chain and extended value network-ensuring they understand your cyber strategy and meet the standards and protocols in place to protect organizational products/services;
6. Ensuring "governance" structures are in place and accountability/responsibility assigned for ensuring success of cyber strategy
7. Reporting level of CIO/CISO in particular-are they part of the strategic leadership team?
8. Prioritize critical data/information assets-some data is simply more important than others. Has the organization conducted a benchmarking exercise to know its critical information assets?

These themes will be discussed below, providing evidence from the interviewees for their inclusion.

1. Ensuring **cyber strategy is aligned** to business strategy-otherwise there is the possibility of viewing the initiative as an IT project. As one interviewee (P1) noted *"keeping cyber strategy aligned to the organization, its critical to start off with business first and build cyber into organizational strategy. Otherwise you could end up taking an overly technical view of the whole thing and suddenly holes appear in your security analysis because important things are not protected and aligned to the business".* This point of alignment is further compounded by another interviewee (P2) who stated "another challenge has been the *"air-gap" or crocodile pit between the 'back-end' and 'front-end' information systems. How do we integrate both without breaching internal security and allowing threats inside? There is an advantage to public procurement in supporting alignment, i.e. it encourages a heterogenous environment, where different suppliers, and processes can help to grow difference internally-but it is critical that we think about the business first and business problems first and then match the systems and*

security needs accordingly". Alignment was further asserted by another interviewee (P3) who stated *"a challenge from a cyber program perspective, has been the legacy systems within different businesses. Large-scale IT projects, such as ERP, are great in the sense that it is tangible to develop a cyber strategy on this data, but legacy systems are unknown and local-difficult to know exactly where data resides and how it is open to threat. This lack of alignment can lead to resentment about new change initiatives-people will find it difficult to buy into new vision."* This notion was further echoed by another interviewee (P4) who emphasized that the organization must look at cyber program from a business perspective. Interviewee (P4) further stated that *"There has to be an integration between both worlds (business & IT) otherwise it becomes a typical 'IT project".* The above responses clearly point to the importance of attaining effective alignment between the cyber security strategy and the business strategy. Strategic leaders recognize the benefits of attaining effective organization-wide alignment between systems, processes, and structures, to support a more successful approach to cyber security delivery

2. Rethinking organizational **"business processes"** and their susceptibility to cyber risk/threats. The theme of having a clear value stream map conducted to understand organizational business processes is raised by participants throughout the data collection. One interviewee (P2) noted, for example, *"we spend a lot of time looking at our core processes and systems-this is exhausting work but its critical if we are going to match how we work around here with the type of security we need to protect things. We regularly audit our processes, and this throws up potential security issues and we rectify them-but this process helps us to identify what information is important and critical to us"*. Another interviewee (P5) stated that, *"it's all about understanding your core business processes and preparing a plan to protect them-some companies start with the*

systems and security software and apply vendor off-the-shelf solutions-but that misses the point-that's an a la carte approach to security-it doesn't protect the organization but it makes people think we are protected". Similar views were also expressed by another interviewee (P6) who also emphasized the need for a good understanding of the business processes and importance of better planning to secure their business processes as they (P6) state '*My role is to ensure that we plan for the worst outcome and hope for the best outcome and have plans in place for when disasters strike. There is a need to ensure that there is a framework in place. The IT teams are working on different scenarios and definitely working with the business functions across the organization to ensure that they don't worry'*. Again, the importance of understanding organizational business processes in order to protect from external threats is also raised by another interviewee (P7) who stated that *"there is a maturity in the organization that the procedures and processes need to be followed, hence the risk register and creating critical infrastructure. This same maturity is not seen in the marketplace for similar organizations and for the companies where we supply services. The mum and pop shops and the SMEs have definitely not got that level of maturity in understanding and management of risk".* Rethinking the flow of business processes across the organization is, therefore, a critical component of how strategic leaders can support their cyber security strategies. As noted above, this task should not be outsourced or templated by generic software tools, it is a very sensitive issue for organizations and significantly supports a more strategic view of how cyber security systems can effectively protect the organization.

3. Fostering a **"culture of trust"** across the organization, where cyber resiliency becomes part of employee and team behavior. A third theme that emerged from the data raised the issue of fostering a culture of trust. One of the interviewee (P1) for

example, states that by *"constantly communicating to the rest of organization about potential from disruption, business must take ownership of cyber resiliency, information governing council comprised of senior managers to ensure communication and response, where our "top priority is our ICT strategy".* This was also echoed by another interviewee (P2) who emphasized that their organization has a strong vigilance of security maintained by the trust levels across the organization. As interviewee (P2) states, *"Look vigilance is critical and standards and protocols for security are critical, but across the organization it's important to have trust between teams and employees-that's how real vigilance occurs".* The evidence from the interview data show that most interviewees were aligned with view to have an organization wide culture supporting cyber resiliency. Interviewee (P4) notes, *"it's important that the whole culture of organization understands importance of cyber resiliency. Change user behavior through education, regular bulletins, recognizes technical complexity from home offices, trade-off in risk management. Objective is to create trust trade-off between cyber compliance and workforce".* Interviewee (P3) comments "*A challenge in embedding the new culture into organization is to create a culture of trust. Management need to appreciate people will make mistakes-so while it's important to have standard and protocols in place, we need to create a culture of openness towards mistakes and error and then this will help us to trust one another more*". The statements above point to the importance of fostering a culture of trust between stakeholders within the organization. Whilst systems and processes are there to ensure threats are found, alerted, and overcome, a culture of trust transforms the way the organization thinks and engages with cyber security issues.

4. Making "cyber resiliency" a **key competency/capability** of organization- many interviewees spoke of the importance of viewing cyber resiliency as a key capability rather than "just another project" that will lose importance as newer initiatives are

launched. As interviewee (P3) states, *"we are looking at making cyber security a key competency for the organization. It's so important to build competency around security by being constantly vigilant and aligning security to work processes. It must work for the business and it then becomes a competency and capability we can deliver upon."* P3 further highlighted that these days users/management do get confused between 'cyber' and 'GDPR' assuming them as the same thing-but they are very different. GDPR is about protecting 'personal information' and ensuring organizations are not breaching protocols around an individual's rights and data whereas 'cyber' is about protecting organizational information assets from criminals and external attacks. Another point was raised, where interviewee P1 stated *"we have separated the cyber security team (at operations level) from the cyber strategy team (focused on future threats and risks)-that helps us to keep double checking what we are doing-putting extra measures in place. Setting benchmarking for security of industry standard shouldn't be about just complying, need to go further, need to exceed what we should be doing. Deficit of skills in this area need greater focus on developing talent management to cope with cyber security shortage of personnel. We try to make it competitive for such staff*". The importance of developing a cyber capability is noted further by interviewee (P2) who stated *"security being everybody's job and increasingly security is viewed as a key capability of organizations. Digital transformation is pushing for cyber security not just within but beyond the organization; therefore organizations need to ensure they have the suite of in-house skills, resources, and competences to cope with such threats. Active management is critical to cyber security-actively have program in house and dedicated resources to look at cyber issues".* In fostering a culture of trust towards cyber security, organizations are seeking to build effective capabilities around talent, skills, methods, and knowledge that will become part of the fabric of the organization.

5. Ecosystem-Understanding **"partners/suppliers relationships"** in value chain and extended value network-ensuring they understand your cyber strategy and meet the standards and protocols in place to protect organizational products/services. As interviewee (P5) noted, *"we've started to discuss cyber protection with our suppliers. This is really becoming an important issue for us. We're so exposed to external threats that it's really important our suppliers and partners get on board with what we are trying to do. That's why board level commitment and engagement is so important. This isn't just a security issue this is a strategic issue now for the organization"*. This statement reflects that organizations these days understand the importance of maintaining good relationships with their suppliers/partners. This is also reflected by interviewee (P1) who stated, *"It's not good enough just to secure the organization internally but you need to know what your partners, whether they are your suppliers or contractors, are up to. We are taking a deep look into what third parties are doing and this will be even more important to us in the future"*. Similarly interviewee (P4) stated, *"A lot of organizations are now looking at securing not just inside the organization but their greater network, suppliers, partners, contractors and even customers. We have just launched a new cyber program that will connect more with our external partners. Yes, this will look like an ecosystem security program in time, where we support security through greater data analytics and AI tools during data analysis"*. Maintaining good relationships with suppliers and partners is essential for organizations, not just for developing cyber resiliency, but also to deal with threats and risks effectively.

6. Ensuring **"governance" structures** are in place and accountability/responsibility assigned for ensuring success of cyber strategy. As one interviewee (P1) noted, "*leading by example, conducting effective risk assessment at executive level to ensure threats are given highest priority and treated seriously. You must have board level oversight with*

effective level of interest from board members. Funding is a critical role of senior management. One budget we do not constrain is cyber security-we will find the funds from across other areas". Interviewee P(3*)* states, *"this program was driven out of IT. The board gave us as much funding as we asked for and told us to go do it. We have a representative at committee that meets quarterly. We have internal communications people driving the comms agenda. We tried to create greater organizational awareness and buy-in by (i) running town-hall meetings across different businesses, (ii) offering training campaign, (iii) ran simulation programs. We commissioned an organization-wide consultant's report on our security needs-which was very helpful-it helped the program to gain further credibility across the board and organization. If I were to do anything differently I would have hired an external person to drive the communications piece-it really needs to be constantly communicated to the organization-especially its value. Each IT function area within each business now has its own security officer who reports to me. Need to support local security needs. Challenge of talent management and getting right people".* Interviewee (P2) noted, the *"board is fully behind ICT. Day to day business must drive business. We have been certified with a number of ISO standards. This assures strategic leaders that ICT strategy and security are meeting international standards and the organization security is at certain level. We have also hired a permanent CISO with a dedicated team of Cyber Security personnel. We also meet with the Board once per year to have a full meeting on Cyber Security"*. Finally, interviewee (P6) noted, *"I have a role of ensuring that the threats and incidences of cyber security are minimized. What am I responsible for now and how do I protect it if there is no visibility across the organization? This is a huge issue for the CISO now. There are issues in my role as I can only protect the infrastructure that I own and am aware, but it needs to be done for the whole organization"*". Strategic leaders play a critical part in

providing resources for cyber initiatives but equally ensuring the structures are in place that gives cyber security teams the authority and power to make effective decisions. This ensures timely and non-partisan decisions can be made that protect the organization and its stakeholders and data from attack.

7. **Reporting level of CIO/CISO.** It is critically important that there is direct access for the CIO/CISO to the senior leadership teams and CEO. As noted by interviewee (P2) who stated, "*previously regarded as IT functional role, key enabler of transformation now, CIO role is one of leadership, trusted advisor, know the business first and align systems to business needs. We have merged our Chief Digital Officer with CIO-so CIO position is critically important to security. It's very important that the CIO is comfortable engaging with teams and constantly educating the business about IT's potential. They need to market ICT and sell its use and possibility. IT today is about pushing change. Change agent piece is important for the CIO*". Similarly, interviewee (P7) noted, *"I've had senior roles in IT for years and it's critical to be part of the executive team"*. Similar view was also shared by another interviewee (P6) who notes *"in order to advance IT at a strategic level and amongst external stakeholders, it is important to be on the strategic leadership team"*. Finally, interviewee (P5) noted*, "As a CISO, I report directly to the CIO who in turn reports to the leadership team. If the CIO wasn't part of the leadership team then I definitely know security wouldn't be as big a priority for everyone as it is. We have had no problems, so far, in getting the funding or commitment we've asked for and I only see this increasing in times ahead".* As illustrated above, it is critical that the cyber security team have a direct reporting relationship to strategic leaders in order to ensure representation of the function at executive level. Again, such a relationship not only allows information to be communicated more urgently and effectively but it also demonstrates to the organization the important role cyber security plays for all.

8. Prioritize **critical data/information assets**. The data reveals that many interviewees are eager to prioritize certain data, "*as some data is simply more important than others"* (P8). As interviewee (P1) noted, *"we need to ask what is our most important information asset or inventory of data and where it is-how do we protect it? Each quarter we look at the top 10 risks-high/low impact and how they will impact upon our critical information assets. Again, this is as much about knowing the business as it is security of data"*. Interviewee (P2) points *out "data is a key asset. We need to know what a key priority for us is and prioritize accordingly. Our audit process throws up potential security issues and we rectify them-but this process helps us to identify what information is important and critical to us"*. Interviewee (P3) highlighted that most of their systems are internal to organization and they don't have customers accessing organizational data (other than nurses accessing patient data). Thus, they focus on securing information assets internally. Finally, interviewee (P7) notes *"some of the biggest threats is that organizations have not identified what their critical information assets are and not gone through giving a value to their information assets".* Finally, it is vital for strategic leaders that they are cognizant of their organizations most critical information assets. Whilst cyber security initiatives seek to protect all data, some data deserve strategic level attention as a security breach of it could threaten the very existence of the organization and its reputation amongst key stakeholders and customers.

5. DISCUSSIONS

In developing an organizing framework (Figure 1), the final stage of the research design approach supports the selection of emergent higher order themes. Four key themes were selected from the data and are discussed in detail below in support of the extant literature. The authors categorized the themes into a two- by-two matrix in order to

illustrate the different dimensions associated with respective themes. Two key dimensions have emerged, which are illustrated along the X and Y-axis. The first dimension focuses on the socio-technical nature of cyber security initiatives. The data reveals that managers need to be cognizant of the organizational and technological perspectives when supporting a cyber strategy.

	Transitional Support	**Transformative Support**
Organization-centric	**a. <u>Ensuring Governance</u>** i. Effective reporting channels for risks/threats; ii. Shared Understanding for Cyber Resiliency across the organization	**c. <u>Cultural Mindset</u>** i. Fostering culture of *'trust'*- positively influencing employee behaviors; ii. Building cyber *'resiliency'* competency/capability as dynamic capability
Technology - centric	**b. <u>Integrating the Organization</u>** i. Integrating back-office and front-office IT systems; ii. Prioritize *"information assets"* in developing cyber resiliency	**d. <u>Securing the Ecosystem</u>** i. Align *"business strategy"* to cyber strategy; ii. New relationship/ integration with ecosystem stakeholders

Figure 1: Cyber-Security Strategy Framework

The second dimension focuses on the nature of support provided by managers. The data reveals that the enormity of cyber risks and threats require a two-step approach to how managers deliver support. The first, which is termed "transitional" in the framework below, requires a short-term and immediate approach to cyber security. Due to the ever-present risks and threats confronting organizations, management support needs to adopt an organization-wide approach where information systems are fully integrated between back-office and front office. The second step is termed

"transformational support", which focuses on developing a significant cultural shift within the organization that places cyber resiliency at the forefront. Developing a cyber resilient organization where extended organizational partners, suppliers, and stakeholders, are aligned within a network ecosystem further supports such a cultural mindset.

5.1. Governance

The first step in supporting a cyber strategy is for the organization to have a clear governance structure in place where senior management are willing to actively support risk assessment and potential cyber threats. Strategic leadership support is often cited as a critical factor for the successful implementation of information systems (Dong et al, 2009), with the IS security literature similarly noting its importance (Preston et al, 2006).

As cyber attacks span business functions and divisions, gaining strategic leadership support helps to bring an organization-wide perspective to security initiatives. There are two key approaches to developing strong governance for the cyber security strategy, (i) ensuring there is an effective 'reporting' relationship between the CIO/CISO and the CEO and strategic leadership team, and (ii) creating a 'shared understanding' within the strategic leadership team for cyber resiliency and risk assessment. Developing an effective reporting relationship between the CIO and the CEO plays a critical role within the general IS leadership literature. According to Garrity (1963: 10), for example, one of the main methods for ensuring the IS executive is able to assert the importance of the IS function throughout the organization, is if they are positioned high enough to have a corporate stature, e.g. within two levels of the chief executive, i.e. the 'reporting relationship' of the improved role of the IS executive will

increase on the managerial food chain. The idea of increasing the IS executive's reporting relationship came out of the need to create greater awareness among strategic leaders of the strategic potential of IS (Lederer and Mendelow, 1988). To sum up, Raghunathan and Raghunathan (1989) believed that it is important to have a direct communication between the senior management and IS executive to substantially enhance senior management's ability to utilize full potential of its information system. As Preston et al. (2006) also highlight that direct communication with CEO and senior management provides the CIOs with opportunities for better engagement and has a greater understanding of the organization's business practices, goals, and vision. In contrast, it also creates a potential forum for the strategic leadership team to better understand the role of IS in supporting business strategy and process. In building greater cyber resiliency, it is therefore critical that the CEO and strategic leadership team have a direct and clear reporting relationship with the CIO and CISO. Direct reporting facilitates the development of cybersecurity policies and controls, which prevents organizational circumvention, and provides a rulebook and constitution as to how risk is assessed, and potential threats minimized and dealt with.

As a consequence of building a direct reporting relationship between the cybersecurity function and the strategic leadership team, the second approach to enabling effective cybersecurity governance is advanced, i.e. the development of a 'shared understanding'. A study by Preston et al. (2006) highlights the importance of shared understanding between the CIO and strategic leadership team for the IS effectiveness within an organization. Earl and Feeny (1994) highlighted that a shared and challenging vision for the role of IS must be achieved. This was also echoed by Reich and Benbasat (2000) who refer to this shared vision, where 'IS and business executives share a common vision of the way in which IS will contribute to the success of the business. A

shared understanding assists in ensuring dedicated resources for the initiative, building effective coalition teams to lead change, and provide a clear vision of the project across the organization. Such a shared understanding provides the cybersecurity function with an organization-wide reach, helping to align the vision with the business strategy.

5.2 Integration

In order to gain greater cyber resiliency, management need to ensure that the organization has a transparent view of its data. To do this, systems, processes and structures must be integrated across the organization. In particular, such organizational level integration requires two key approaches from a cyber security perspective; (i) greater integration between back-office and front office information systems, and (ii) greater prioritization of key organizational business processes and critical information assets.

IT systems such as enterprise systems (ES) have promised to unite disparate systems, delivering a more transparent and enterprise-wide view of data. As Davenport (2000) notes, for example, an ES should not necessarily be defined by the number or use of other technologies and tools along with the central vendor package, instead the package should be defined by its ability to seamlessly integrate business processes and information flows up and down, and perhaps more importantly from now on, across value chains. Such information systems have advanced the discussion on system and process integration and have enabled organizations more recently to start focusing on integrating beyond their boundaries. With the emergence of SMACIT information systems (social media, mobile, analytics, cloud-based systems, and the Internet of Things), a new era of digital transformation is occurring within organizations (Piccoli and Ives, 2005). These technologies offer a new approach to capturing and creating

new value for organizations, whether through fostering closer relationships with customers, gaining greater insights to market and competitor data, or the development of new products/services. However, from a cyber security perspective, the integration of back-office (organization-centric) with front-office (customer-centric) systems has created additional demands. Such openness and ubiquity of information exposes the organization to significant risk and cyber threats. It is, therefore, critical that the CIO starts to take greater ownership of both back-office and front-office, leading with a customer-driven mindset. As Colony, (2018: 75) notes, 'previously, most CIOs were hired to digitize and bring order to companies' internal systems and processes. They saw websites as marketing channels and were happy to let chief marketing officers oversee that province of technology. But now the two sides of IT need to come together, driven by customer needs. Such direct ownership by the CIO can allow for a more cyber security conscious approach to back-office and front office integration.

Transitional support of integration, therefore, requires a focused approach to cyber security. Due to the organizational openness required to integrate front and back office systems and processes, management should prioritize key critical information assets. This is the second approach to organizational integration. The move to become digitally enabled enterprises places information and data at the epicenter of organizational strategies. However, a focused cyber strategy is required to prioritize data accordingly, otherwise organizations could potentially fall foul of spreading their cyber resources too thinly and focus more on reviewing the perimeter of the organization rather than strategically assessing and protecting core digital assets. In order to enable the prioritization of data the business must be clear of what constituents' critical information. Therefore, the business needs to drive the cyber strategy conversation rather than asking the security team to protect the organizations data. Again, within the

IS and IS security literature, we see the importance of the business taking the lead in translating respective organizational issues to these functional departments rather than adopting a hands-off approach and allowing a techno-centric lead of the conversation. Essentially, enabling greater cyber resiliency is a business issue and not just a compliance issue, therefore, it is critically important that management perceive the initiative as such. The CIO, therefore, must collaborate with the strategic leadership team to identify organization-wide critical information assets.

5.3 Cultural Shift

The third step of the framework focuses on building a cultural shift with regard to cyber resiliency within the organization. Effective management support and the pursuit of a more integrative organization promote a new mindset regarding cyber security. In particular, the study found two key approaches adopted by management in fostering a more cyber resilient culture within the organization, namely (i) creating greater trust across the organization and amongst external stakeholders, and (ii) the potential to view cyber security as a key organizational competency and capability. Building trust is central to IS security effectiveness. Dang-Pham et al. (2017) note that people-centric security workplace puts emphasis on trust and collaboration between strategic leaders and the employees, who are empowered by the training and security communities' culture to make their own informed risk decisions. They asserted that employees who are trusted tend to influence other employee's security behaviors as well. Similarly, Choi et al. (2017) note that despite organizations use all kinds of sophisticated technologies and techniques to protect critical business assets, the most important factor in any cybersecurity program is trust. In developing a more 'trusting' culture, strategic leaders play an important part in communicating the cybersecurity message

across the organization, and indeed beyond the organization to external stakeholders. The role strategic leaders play in communicating a clear message across the organization is frequently cited in the literature (Yi et al., 2018, Loonam et al., 2005). Equally, running cybersecurity training programs for employees also assists in developing greater security understanding.

However, fostering a culture of trust is not only about establishing top-down direction, formal communication, or programmed training but of equal importance is building a bottom-up appreciation for the potential risks and threats confronting the organization. Belanger et al. (2017) elaborate on the issue of promoting early conformance with information security policies and highlight that early conformance behaviors are more cost-efficient for organizations and can ultimately help prevent intentional undesired security behaviors. In other words, a proactive approach to information security across the organization will create more willing engagement among employees and invariably foster a culture of trust rather than suspicion.

The second step in advancing a culture of trust is for the organization, and management, to work towards viewing cyber resiliency as an organizational competency or capability. Similarly, reviewing the general IS literature we find that increasingly information systems are viewed from a strategic perspective, affording organizations a significant opportunity to leverage greater competitive advantage in an era of technological ubiquity. Yet, IS security is often viewed through a technical lens, as Nazareth and Choi (2015) point out that security only started appearing in IS journals in the 1990s, with much of the research directed at individual behavior and spanning topics such as Internet abuse, compliance with organization norms, ethical practice regarding computers, and the effect of deterrence on user behavior. They further highlight that, studies at the organizational level are comparatively fewer and are

decreasing in frequency, thus compounding our conversation about IS security further to the realms of technical and functional discussion. Yet, cyber breaches pose existential challenges for organizations, therefore greater attention should be on how organizations can build greater resiliency into their capabilities. Teece et al. (1997), for example, refer to dynamic capabilities as the organization's ability to integrate, build, and reconfigure internal and external competences to address rapidly changing environments. In an era of organizational agility and complexity, competencies such as resiliency, adaptability, and ability to cope with technological innovations are critical for survival. Similarly, organizations than embrace a culture of trust and engagement can create a capability of greater resiliency towards cyber security. For decades, the IS function remained operational in intent, with many organizations only embracing its strategic potential in recent times. Cyber resiliency might offer a significant strategic opportunity to organizations moving from a classical reactive approach to security management to a proactive IS security strategy.

5.4 Securing the Ecosystem

The final step of the framework highlights the importance in developing a more holistic approach to cyber security across the organization and beyond its boundaries. The two key approaches revealed from this study focus on (i) greater alignment between the cyber strategy and business strategy and (ii) nurturing closer relationships amongst all organizational stakeholders (suppliers, partners and customers).

Organizations embedding cyber resiliency into their systems, structures, and processes, are seeking to effectively align the IS security strategy with the business strategy. Alignment has been of significant importance to the IS literature over the past decades. For example, Reich and Benbasat (2000) emphasized that for IS managers the

establishment of strong alignment between information systems and organizational objectives has always been an area of key concerns. This was also echoed in the work of Luftman and Brier (1999) who also stated that, 'a key concern of business executives is alignment applying IS in an appropriate and timely way in harmony with business strategies, goals, and needs. Similarly, Tan and Gallupe (2006: 223) noted that 'alignment may enable a firm to maximize its IS investments and to achieve harmony with the business strategies and plans. This, in turn, usually leads to increased profitability and competitive advantage'. For the IT strategy to be effective from an organizational perspective, clear alignment with the business strategy was required.

From an IS security perspective, however, the literature is predominantly focused on reducing risk and controlling potential threats, with a lack of empirical scrutiny around alignment with organizational strategy (Kayworth and Whitten, 2010). The authors note that 'industry experts have called for organizations to be more strategic in their approach to information security, yet it has not been clear what such an approach looks like in practice or how firms actually achieve this (Kayworth and Whitten: 163). Yet, lessons learned from the general IS literature revealed the importance of tying the technical and organizational elements together in order to ensure project success and organizational harmony. The move to become digitally enabled enterprises, will require a more holistic approach to cyber strategy. The second approach to securing the ecosystem is to focus on creating more secure value network relationships. Many organizations travel outside their value chains in creating and delivering respective products and services and as such most be vigilant of how their respective partners and external stakeholders are securing shared data (Porter and Heppelmann, 2014). For example, in the past decade, the emergence of SMACIT technologies has allowed organizations to extend their internal information systems (normally enterprise-wide

systems) with external systems, which supports access to increased amounts of external data. Accordingly, information security for the entire value network becomes critical to organizations, where a new ecosystem security strategy is reviewed in collaboration with external stakeholders.

6. IMPLICATIONS & FUTURE RESEARCH

This study provides a number of theoretical and managerial implications as a consequence of the study's findings. Future research suggestions will also be made in an effort to advance and deepen this exploratory inquiry.

Theoretical Implications

This study will add to current knowledge within the Information Systems, Operations Management, and Strategic Management literature. Within the Information Systems literature, there are few studies that focus on cyber security information systems and the respective organizational challenges associated with their implementation. This study seeks to contribute to this field of inquiry by focusing on leadership issues associated with cyber system implementation. Similarly, within the operations management discipline, there is a lack of empirical inquiry on how organizations can secure operational activities against cyber threats. This study also seeks to broaden our understanding of how managers can phase in cyber security support across operational activities. Finally, this study will also make a contribution to the general strategic management field. A lack of empirical inquiry within the strategy domain exists around how organizations can leverage cyber security implementation to capture organizational value and potentially create a competitive advantage. By focusing on strategic leaders, this study is elevating the call for greater inquiry into how leaders can ensure a better strategic fit for cyber security programmes. Finally, this study adopts an

interpretivist approach to inquiry, which counters the dominant positivistic methodological approach within the information systems and operations management literature. Due to the lack of empirical investigations within the Cyber Security domain, an exploratory study was selected to tease out emerging themes that could be further validated and generalized in future inquiries. An interpretivist paradigm will contribute to current knowledge and offers exploratory insights for theoretical development. This study thus contributes to theoretical development with the emergence of an exploratory framework. This framework seeks to plot the key actions of senior leaders in supporting cyber security initiatives and building more resilient organizations.

Managerial Implications

This study makes a contribution to management by emphasizing the importance of attaining senior leadership support in fostering more cyber resilient organizations. It develops a framework that allows managers to follow key actions. In particular, the findings reveal that support is a two-pronged approach. Transitional support focuses on the socio-technical nature of cyber security initiatives. The data reveals that managers need to be cognizant of the organizational and technological perspectives when supporting a cyber strategy. In other words, managers will need to move beyond just focusing on 'cyber systems' but pay particular attention to the organizational 'processes' and necessary structures required to ensure successful outcomes. Finally, the framework also reveals that support is transformational in nature, which focuses on developing a significant cultural shift within the organization that places cyber resiliency at the forefront. In essence a cultural shift requires significant managerial attention, where managers are not only focused on 'what we do' but move incrementally towards a better understanding of 'how we do things' that supports a more cyber resilient organization. Developing a cyber resilient organization where

extended organizational partners, suppliers, and stakeholders, are aligned within a network ecosystem further supports such a cultural mindset.

Future Research

This study would greatly benefit from further empirical inquiry that sought to validate and deepen the exploratory findings. In particular, potential areas for future research could include;

- Cyber Security and Competitive Advantage: The literature notes the operational role information security has played over the past decades in ensuring organizations have been able to keep respective information and data secure. Organizations seeking to build more cyber resilient enterprises, particularly in light of emerging digital technologies such as the Internet of Things and Big Data, will need to consider a more strategic role for their data. In other words, organizational data, and its consequent security, will become a key focal point for strategists in exploring ways to leverage potential competitive advantage whilst securing and protecting organizational and stakeholder data;
- Leadership team roles: This study focused on the views of CIO's/CISO's. Future research should seek to broaden this remit to focus on leadership teams in general, i.e. senior leadership teams, middle management teams, operational and engineering teams, and line management teams in their involvement in establishing more cyber resilient organizations;
- Cyber Resiliency for Platform Strategies and Organizational Ecosystems: Finally, another avenue for rich empirical inquiry would be to explore cyber security for organizational ecosystems. As traditional organizations move towards platform strategies that move beyond the organizational boundary to entire ecosystems,

managers need a clearer understanding of how they can participate in such strategies whilst securing respective enterprises.

7. CONCLUSIONS

Cyber security has become a critical issue for organizations to protect core data and informational assets and prevent significant reputational damage and long- term customer and supplier concerns. Yet, despite its importance for organizations, there is a lack of knowledge as to how leaders can support more effective cyber security initiatives. This study has sought to explore this topic by interviewing CIO/CISO/CTO positions across different organizations within the UK and Ireland from different sectors. A key challenge for this study has been gaining access to required senior managers. Organizations, understandably, are very protective when discussing IS security and in particular cyber security-so embracing the topic of exploring leadership for cyber security support, whilst critical important, was challenging to conduct empirically from an exploratory perspective. Yet, the study, in revealing four key approaches for leaders to take in supporting more resilient cyber security programs, has taken an important first step in exploring this vitally important topic for all organizations. Future research should therefore focus on collecting empirical evidences from wider stakeholders to generalize the findings across the different sectors.

References

Anderson, C.L. and Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34, pp. 613–643.

Arabo, A. (2015). Cyber security challenges within the connected home ecosystem futures. *Procedia Computer Science*, 61, pp. 227-232.

Bailey, T., Kaplan, J. and Rezek, C. (2014). Why senior leaders are the front line against cyberattacks. *McKinsey Insights*. June 2014, pp. 1-4

Barton, K.A., Tejay, G., Lane, M. and Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, 59, pp. 9-25.

Bélanger, F., Collignon, S., Enget, K. and Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, *54*(7), pp. 887-901.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D. and Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors, *MIS Quarterly*, 39(4), pp. 837-864.

Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology, *Qualitative Research in Psychology*, 3 (2), pp. 77-101.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly*, 34, pp. 523–548.

Chatterjee, S., Sarker, S. and Valacich, J.S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, *31*(4), pp. 49-87.

Chen, P.Y., Kataria, G. and Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly*, 35(2), pp. 397-422.

Chen, Y., Ramamurthy, K., and Wen, K.W. (2012). Organizations' _information security policy compliance: stick or carrot approach? *Journal of Management Information Systems*, 29 (3), pp. 157–188.

Chinedu E, S., Duan, Y. and Chen, H. (2014). Examining emerging ICT's adoption in SMEs

from a dynamic process approach. *Information Technology & People*, 27(1), pp. 63-82.

Choi, J., J. Kaplan, C. Krishnamurthy, and Lung, H. (2017). Hit or myth? Understanding the true costs and impact of cybersecurity programs. McKinsey & Company July 2017, pp. 1-10. https://www.mckinsey.com/ business-functions/digital-mckinsey/our-insights/hit-or-myth-understanding-the-true-costs-and-impact-of-cybersecurity-programs. Accessed [08/09/2019]

Colony, G.F., (2018). CIOs and the future of IT. *MIT Sloan Management Review*, *59*(3), pp.1-7.

D'Arcy, J., Hovav, A., and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, 20, pp. 79-98.

Dang-Pham, D., Pittayachawan, S. and Bruno, V. (2017). Applying network analysis to investigate interpersonal influence of information security behaviors in the workplace. *Information & Management*, *54*(5), pp.625-637.

Deichmann, J., M. Roggendorf, and Wee, D. (2015). Preparing IT systems and organizations for the Internet of Things. McKinsey & Company, November 2015, pp. 1-8.

Dhillon, G., Syed, R. and de Sá-Soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *Information & Management*, *54*(4), pp.452-464.

Doherty, N.F. and Tajuddin, S.T. (2018). Towards a user-centric theory of value- driven information security compliance. *Information Technology & People*, 31(2), pp. 348-367.

Doll, W. J. (1985). Avenues for top management involvement in successful MIS development. *MIS Quarterly*, 9(1), pp. 17-35.

Dong, L, Neufeld, D. and Higgins, C. (2009). Top management support of enterprise

systems implementation. *Journal of Information Technology*. 24(1), pp. 55-80.

Dutta, A., and McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, 45(1), pp. 67-87.

Ezingeard, J.N. and Bowen-Schrire, M. (2007). Triggers of change in information security management practices. *Journal of General Management*, *32*(4), pp.53-72.

Federation of Small Business (FSB), https://www.fsb.org.uk/media-centre/press-releases/small-firms-suffer-close-to-10-000-cyber-attacks-daily

[Accessed 20/09/2019]

Frank, J., Shamir, B. and Briggs, W. (1991), Security-related behavior of PC users in organizations, *Information and Management*, 21 (3), pp. 127-135.

Goodhue, D., and Straub, D.W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security, *Information & Management*, 20 (1), pp. 13–27.

Gordon, L.A. (2006). Budgeting process for information security expenditures. *Communications of the ACM*, 49, pp. 121-125.

Guo, K., Yuan, Y., Archer, N.P. and Connelly, C.E. (2011). Understanding non-malicious security violations in the workplace: a composite behavior model, *Journal of Management Information Systems*. 28 (2), pp. 203–236.

Guo, K.H. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management*, 49, pp. 320-326.

Herath, T., and Rao, H.R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems,* 18, pp. 106–125.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), pp.615-660.

Hu, Q., Hart, P. and Cooke, D. (2007). The role of external and internal influences on information systems security – a neo-institutional perspective. *Journal of Strategic Information Systems*, 16 (2), pp. 153–172.

Hu, Q., Xu, Z., Dinev, T. and Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, 54, pp. 54-60.

Hui, K.L., Hui, W. and Yue, W.T. (2012). Information security outsourcing with system interdependency and mandatory security requirement. *Journal of Management Information Systems*, *29*(3), pp.117-156.

Jarvenpaa, S. L. and Ives, B. (1991). Executive involvement and participation in the management of information technology. *MIS Quarterly,* 15(2), pp. 205-227.

Johnston, A.C., and Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly,* 34, pp. 549-566.

Karjalainen, M. and Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association of Information Systems,* 12 (8), pp. 518–555.

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

Koh, C., Ang, S., & Straub, D. W. (2004). IT outsourcing success: a psychological contract perspective. *Information Systems Research*, 15(4), 356–373.

Kriebel, C. H. (1968). The strategic dimension of computer systems planning.

Long Range Planning, pp. 7-12.

Kwon, J., Ulmer, J.R. and Wang, T. (2012). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems*, 27(1), pp. 219-236.

Liang, H., and Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association of Information Systems*, 11 (7), pp. 394–413.

Loonam, J., Eaves, S., Kumar, V. and Parry, G. (2018). Towards digital transformation: Lessons learned from traditional organizations. *Strategic Change*, 27(2), pp.101-109.

Loonam, J., McDonagh, J., Kumar, V. and O'Regan, N. (2014). Top managers and information systems: 'crossing the rubicon!'. *Strategic Change*, 23(3-4), pp.205- 224.

McGoogan, C. (2017). Cyber attacks hit half of UK businesses in 2016. *The Telegraph*, 19th April 2017.

Menard, P., Bott, G.J. and Crossler, R.E. (2017). User motivations in protecting information security: protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), pp.1203-1230.

Myers, M.D. and Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), pp.2-26.

Narayanan, S. N., Ganesan, A., Joshi, K., Oates, T., Joshi, A., and Finin, T. (2018). Early detection of cybersecurity threats using collaborative cognition. In *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), Philadelphia, Pennsylvania, USA,* pp. 354-363.

National Audit Office (NAO), Investigation: WannaCry cyber attack and the NHS, Report by the Comptroller and Auditor General, Department of Health, UK, 1-31, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Accessed 20/09/2019]

Nazareth, D.L. and Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, *52*(1), pp.123-134.

Orlikowski, W.J. and Baroudi, J.J. (1991). Studying information technology in

organizations: Research approaches and assumptions. *Information Systems Research*, *2*(1), pp.1-28.

Piccoli, G., and Ives, B. (2005). IT-dependent Strategic Initiatives and Sustained Competitive Advantage: A Review and Synthesis of the Literature, *MIS Quarterly*, 29(4), pp. 747-776.

Porter, M.E. and Heppelmann, J.E. (2014). How smart, connected products are transforming competition. *Harvard Business Review*, 92(11), pp.64-88.

Preston, D.S., Karahanna, E. and Rowe, F. (2006). Development of shared understanding between the chief information officer and top management team in US and French organizations: A cross-cultural comparison. *IEEE Transactions on Engineering Management*, *53*(2), pp.191-206.

Samtani, S., Chinn, R., Chen, H. and Nunamaker Jr, J.F. (2017). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *Journal of Management Information Systems*, 34(4), pp.1023-1053.

Siponen, M., Mahmood, M.A. and Pahnila, S. (2009), Are your employees putting your company at risk by not following information security policies?, *Communications of the ACM*, 52 (12), pp. 145-147.

Siponen, M.T. and Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46, pp. 267-270.

Son, J.Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, 48, pp. 296-302.

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), pp.215-225.

Spears, J.L. and Barki, H. (2010). User participation in information systems security risk

management. *MIS Quarterly,* 34 (3), pp.503-522

Straub, D.W., (1990). Effective IS security: An empirical study. *Information Systems Research*, 1, pp. 255-276.

Straub, D.W., and Welke, R.J. (1998). Coping with systems risk: security planning models for management decision-making, *MIS Quarterly*, 22 (4), pp. 441–469.

Strauss, A., and Corbin, J. M. (1997). *Grounded theory in practice*. SAGE, London.

Sweeney, B., (2016). Cybersecurity is every executive's job. *Harvard Business Review*. pp. 2-5.

Tan, F.B. and Gallupe, R.B. (2006). Aligning business and information systems thinking: A cognitive approach. *IEEE Transactions on Engineering Management*, 53(2), pp.223-237.

Teece, D.J., Pisano, G. and Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), pp.509-533.

Vance, A., M. Siponen, and Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49, pp. 190-198.

Von Solms, R. and Van Niekerk, J., (2013). From information security to cyber security. *Computers & Security*, 38, pp.97-102.

Yi, Y., Ndofor, H.A., He, X. and Wei, Z., (2017). Top management team tenure diversity and performance: The moderating role of behavioral integration. *IEEE Transactions on Engineering Management*, 65(1), pp.21-33.

Appendix One-List of Interviewee Participants

Interview Participants	Position	Service/Industry
P1	CIO	Energy
P2	CIO	Public Sector
P3	CIO	Pharmaceutical
P4	CIO	Public Sector
P5	CISO	Government
P6	CIO	Education
P7	CTO	Construction
P8	CISO	Education

Appendix Two-Table of Interview Questions

Theme	Key Interview Question
Challenges	What are the key challenges confronting your organization in protecting itself against the threat of cyber attacks?
Choices	How can the organization overcome these potential challenges?
Culture	How can organizations foster a better culture of cyber surveillance?
Support	How can senior management/CIO support the organization in developing greater cyber resiliency?
Critical Success Factors	What factors do you believe are critical in supporting greater cyber resiliency?
Comments	Are there are additional comments you would like to make?

Appendix 3-Sample of Data Analysis

Data	Case Evidence (quote from interview)	Emerging Concepts	*Higher order Categories and Themes*
Challenge of knowing what's important	*"we spend a lot of time looking at our core processes and systems-this is exhausting work but its critical if we are going to match how we work around here with the type of security we need to protect things. (P2)*	Business Process	*Integration*
Enormity of security task	*"some data is simply more important than others' (P8).*	Priority of Data/ Information	*Integration*
Role for security management is becoming demanding and organizational ubiquitous	*What am I responsible for now and how do I protect it if there is no visibility across the organisation? This is a huge issue for the CISO now. There are issues in my role as I can only protect the infrastructure that I own and am aware, but it needs to be done for the whole organization' (P6).*	Changing CIO role/ membership of TMT	*Governance*
Getting buy-in for security/changing perceptions	*"its important that the whole culture of organization understands importance of cyber resiliency. Culture is big issue-changing culture is difficult. Change user behavior thru education, regular bulletins, recognize technical complexity from home offices, trade-off in risk management. Objective is to create trust trade-off between cyber compliance and workforce" (P4),*	Trust and involvement	*Cultural Shift*
Transformational rethink on how we view cyber security	*"we are looking at making cyber security a key competency for the organization. (P3)*	Resilient Capability	*Cultural Shift*
Security is larger than organisation - there's an entire ecosystem of security required	*"we've started to discuss cyber protection with our suppliers-this is really becoming an important issue for us". (P5)*	Aligning cyber strategy to business strategy	*Securing the ecosystem*