A Framework for Information Security Management in Capital Markets

Research-in-Progress

Haneen Heyasat **Sameera Mubarak**

Nina Evans

Abstract

Obtaining financial data is attractive to criminals. A recent increase in cybersecurity threats in the financial sector has seen capital markets targeted. With the rapid development in information technology, information security is a growing concern for the financial services industry in general, and keeping capital market operations efficient, expeditious, and reliable are some of its highest priorities. This paper forms part of a larger project which investigated the technical, behavioural, managerial, philosophical and organisational aspects of information security. Although not yet applied to real-world data, this paper outlines the methodological and theoretical foundation of a proposed framework to improve information security and risk management practices. The application of such a framework may contribute to improved management of information security in the capital markets sector.

Keywords: Information Security, Risk Management, Capital Market

Introduction

In every country, the capital market plays a critical role in the national economy. The capital market is made up of a wide range of stakeholders (governments, corporations, banks, brokers, custodians, investment funds and mortgages, for example) all of which benefit directly from the investments made in these security markets (Friedhoff 2016). Keeping the data secure in Financial Institutions (FIs) like capital markets is critical for the management of these stakeholders in maintaining their performance and gaining confidence with outside investors. In addition to other widespread negative impacts, when Information Security (IS) incidents occur, the direct financial loss affects capital markets. The most recent forecast by Gartner revealed that by 2018, the total amount spent on IS products and services was $93 billion (Pieri 2017). Being one of the more attractive targets for cyber-attacks (Bouveret 2018), much of this investment has been in the financial services industry. Indeed, of the industries that are vulnerable to security threats, the financial services sector is experiencing the most expensive breaches (NetDiligence 2016). Financial services have been ranked second in the total number of cases of cyber-attacks, after the healthcare sector (Malik 2016).

Various studies have explored different management roles and activities, but none have given a comprehensive picture of these roles and activities to manage IS effectively in the capital market sector. We reviewed the literature relating to management's roles in IS to explore the available solutions

activities that enhance Information Security Management (ISM) in the capital markets. There is a broad consensus among researchers and professionals that, although information security is essential, it is an under-studied research area in the capital market sector. This paper, therefore, offers a new contribution to this important area of research. As part of a larger research project which focusses on organisational IS at the managerial and employee levels in capital markets, and the impact of their application on the protection of these organisations, this paper presents a framework and guidelines for information security risk management for capital markets institutions.We first describe the background to the proposed framework and then identify the qualitative methodological approach we anticipate employing as we apply this framework to our own future research. Expected contributions such research may contribute to the literature and financial industry are identified.

Research Objective and Motivation

Capital markets contain financial transactions and sensitive data. The most important aspect of the capital market sector is time sensitivity. Transactions must be done on a daily basis, and it is not possible to start a new trading session before completing all past transactions. Since the capital markets' dependence on electronic systems is growing, cyber threats are also increasing (Spanos and Angelis 2016). The financial services sector is facing security incidents 300% more frequently than the other industries (Johnson 2016). This is a major concern because all the processes covered by these systems will be unreliable if any security breaches are found in them. For capital markets, therefore, the need to create and develop IT auditing policies and security procedures is important to fight, if not eliminate, cyber-attacks (Sutton 2017). The lack of good IT security practices and weakness in technical controls can open the door to threats (Australian Computer Society (ACS) 2016).

The primary motivation of this paper is to provide a comprehensive overview of current practices and experiences documented in the literature on IS to enhance security management in the capital market. Identifying gaps in security practices in the capital market sector allows us to suggest reccomendations to address the sector's shortcomings. In short, this paper asks: ***How can information security management be enhanced in capital markets?***

Literature Review

According to the latest report issued by the Accenture and Ponemon Institute in 2018, cyber-attacks not only affect financial services more than other industries but are increasing. The estimated loss due to these incidents increased by more than 40% over the past 3 years (McGinn 2018). Table 1 summarises research findings regarding security threats faced by FIs and the need to improve IS practices.

Table 1. Summary of Literature Review Challenges Faced by Organisations

Reference	Conclusion / Findings
(Bjerken 2017)	Organisations fail to adopt active cybersecurity strategies because many companies do not use the available best practices and they lack sufficient specialists in IS and experience.
(Pelletier 2017)	Failure to deal with the main threats to an organisation implies that a serious problem of data breaches leading to huge losses in the whole finance industry.
(Stephens 2017)	Threats caused by internal users may be sometimes more significant than that caused by external cyber attackers, and insiders can work with criminals or on their own to steal data or financial information.
(Johnson 2016)	Various financial service regulators have published best practices for FIs to consider when creating and modifying their individual cybersecurity programs.
(Clark 2016)	Best practices guide executives, managers, and IT employees to think about how to improve ways to manage risk and protect the organisation assets.
(Spanos and Angelis 2016)	Security breaches have a direct impact on the market value of a firm.

(Kongnso 2015)	Some technology leaders lack best practices to reduce data security breaches. Awareness and compliance are neglected despite the fact that IS standards are increasingly critical to organisations. Institutions must work hard to embed ISM culture in employees. Their technical skills must continually be updated.
(Raytheon 2015)	An effective ISM culture depends on the ability of senior or executive management to make informed decisions and continuously reinforce employees' skills to build this culture.
(Narain Singh et al. 2014)	ISM best practices may help organisations to guard against risks.
(Herath and Rao 2009)	Several factors affect the security of information systems such as employees, technology, and cultures.

The main challenges faced by organisations related to the lack of information's security practices, policies, guidelines and lack of sufficient awareness about the riskiness of the situation and how to protect their assets. All these challenges will be covered through the suggested framework.

Information Security and Risk Management in the Capital Market

Using an IS and a risk management system has become a significant requirement for all institutions, especially those working in the finance industry (Narain Singh et al. 2014). This is due to the complexity of security issues in FIs and given that the capital market is an important part of it. This study puts forward a framework that may effectively address these IS challenges and requirements, and therefore encourage organisations to adopt a balanced mix of management, human and technical aspects of IS and risk management.

Information Security Management in the Capital Market

Some studies specifically discuss the challenges of the capital market. Defending the capital market in the financial sector against cyber-attacks is a top-tier priority. Given that the finance industry deals in billions of dollars, corruption in this operation causes a massive loss of confidence, reputation, profits, the value of the currency and other real intangible costs (Raytheon 2015). The IS and risks must be managed effectively; the practices and procedures must be impeccable (Zhiwei and Zhongyuan 2012). Using the building trust approach in managing information security risks in capital market organisations is very useful, mainly because there are certain breaches of information systems which have non-financial implications for a business (Raytheon 2015).

In the years ahead, to achieve success, capital market institutions will depend on their ability to manage risks arising from the new technologies and their exceeding dependence on the internet and information systems. Consequently, challenges will increase not only in number but also in the types of attacks. It must be noted that the users with a modest digital experience also pose a threat to organisations from an IS perspective (Raytheon 2015). In view of the reported incidents, it is certain that even those organisations with the most sophisticated security risk management measures are susceptible to attacks, especially those where sensitive information is in motion, like capital markets (Line et al. 2016). Studies show that security breaches have a direct impact on the market value of a firm (Spanos and Angelis 2016). This constitutes another critical reason to find the best IS practices in the capital markets.

The capital market institutions must embed ISM culture in their units/departments, etc., and the skills of management, as well as employees, must continually be updated on technology and security matters (Kongnso 2015).

Risk Management in the Capital Market

Because of the critical business demands of FIs, dealing with risks is very important. Higher levels of data protection are needed to prevent their sensitive information from leakage and breaches which include financial and customers' sensitive data (Qiu et al. 2013). Nelson (2003) emphasised the importance of risk management in FIs as part of the IS program. Two activities, firstly, identifying the

risks that may threaten customer information, and secondly, developing a written plan consisting of policies and procedures to manage and control the risks, were considered among the major components of the IS program in FIs (Nelson 2003). Further, the Federal Financial Institute Executive Council (FFIEC) suggests that FIs face several risks, i.e. operational, reputation, strategic, interest rate (liquidity), environmental and compliance (legal) risks (FFIEC 2018).

Operational risks relate to the malfunctioning or breaking down of existing technology or support systems (Rampini et al. 2017). This research focuses on individual operating problems, which, although small, can easily expose an institution to adverse outcomes with inordinate consequences. Most FIs today have developed their own processes for evaluating the risks associated with their businesses. Generally, they attempt to choose an approach that can deal with those risks based on institutional priorities as well as internal and external constraints (Qiu et al. 2014). Our proposed framework explores risk management in capital markets to model financially safe practices aligned with business objectives. Operational and technological risks are primarily explored because they are closely related to the focus of this research.

Research Gap

There remains a research gap between current studies and the IS of capital markets. It emerges that most studies on the capital market are concerned with the impact of information technology problems and events, concentrating on the market value of organisations (Barua and Mani 2018; Schatz and Bashroush 2016), investment (Kim et al. 2017) and corporate securities prices (Mithas and Rust 2016). No research to date has discussed IS and risk management practices, and their impact on the capital market sector. Given this challenge, security management practices should be aware of what hides under the continuous availability of information systems holding very sensitive information (Ma and Pearson 2005). The uniqueness of the capital market role requires distinct analysis of the security challenges. On its own, neither technology nor products can solve the problem of IS. The whole environment in which institutions or organisations function must be taken into account (Tang 2013). Studying the findings of various other industries and applying them to the capital market may be one way of addressing this gap.

Theoretical Background to the Framework

Two main aspects of the capital market, technical and non-technical factors, provide the theoretical footing to our proposed framework.

The technical factors include hardware, software, policies, and procedures, and these aspects from part of our framework as investigated through the lens of General Systems Theory (GST). Proposed by Bertalanffy (1969), GST is one of the dominant organisational theories in management. GST posits that all the components in an organisation must work properly and as an integrated whole to accomplish business objectives so that any security threats are effectively solved (Kast and Rosenzweig 1972). Researchers found that IS failures appear when the system components do not work as one unit (Coole and Brooks 2014). This theory is relevant to analysing a system regarding its components, which in turn helps determine the factors causing problems and fixing them (Mitleton-Kelly 2011). GST was chosen as the conceptual framework to understand the phenomena discussed here and to discover the shortcomings in practices which lead to IS problems and data breaches.

Non-technical factors refer to organisational factors such as environment, employees and their behaviours. Environmental factors could include organisational culture and the impact of organisational culture on information security culture (Tang et al. 2016). In developing our proposed framework, we concerned ourselves with these factors through the lens of Social Cognitive Theory (SCT) proposed by Bandura (1986). It is considered one of the important theories for mitigating security risks, as it uniquely understands the human element, and centres on security-compliant behaviour and employees' reactions (Compeau et al. 1999). By analysing participants' behaviours, their environments, and their workplace actions, this theory helps to study variables theoretically linked to the individual, behavioural and environmental factors in investigating the information protection behaviour in capital markets. It is also useful in exploring effective ways to limit and minimise cybercrimes resulting from employees'

behaviours (Mischel and Shoda 1995), particularly in the capital markets context of their use of electronic systems, the internet and IS practices (Ifinedo 2014).

Research Methodology: Applying the Framework to Future Research

To develop and apply our framework, we propose a future qualitative research approach using the case study method. Qualitative case studies will allow us to gather in-depth information and provide greater insights about participants' understanding of responsibility for IS (Creswell 2014; Yin 2014). The data used in our proposed application of the framework will be collected from five different capital market institutions. Data will primarily be generated from semi-structured direct face-to-face interviews with participants (three different levels of employees from the capital market institutions: 1) executives, 2) high-level managers or administrators, and 3) other staff). Secondary data will be collected through observations and analysis of documents. This data will reflect real-life experiences of employees in the capital market institutions. It will focus on identifying: 1) the determinants of IS and risk management in the capital market sector; and 2) the impact of those determinants on decisions or outcomes. Following Charmaz (2014), we will start analysing the data during the data collection phase. Furthermore, this research will employ an interpretive approach to analyse the data of participants' insights. The constructivist grounded theory will guide the data collection and data analysis activities for this study.

Most information security frameworks are limited in scope and are not flexible to meet the unique needs of capital market organisations. Some of these frameworks, like Hofstede's framework for explaining the relation between organisational culture and information security culture (Hofstede et al. 1990; Tang et al. 2016), will help to understand one aspect of our focus, namely non-technical factors.

Proposed Framework and Expected Contributions

The accuracy and speed of access to information in the capital market is a fundamental and essential factor. If the arrival of information is late or inappropriate, this information loses its importance, while the accuracy and speed of information access increase efficiency. Awareness and compliance with policies and procedures have been neglected despite the fact that IS standards are increasingly critical to organisations' data (Kongnso 2015).

Through reviewing the current empirical research on IS practices, we have provided a framework for studying and analysing IS practices in capital markets. To achieve the research goals, it is anticipated that the proposed framework will combine literature and real-life experience as discussed during the interviews with the industry professionals. The initial version of the framework is shown in Figure 1 below. The research objectives will be pursued in the finance industry by understanding the IS and risk management practices and finding deficiencies in this area. Next, a framework for managing IS and risk management would be developed one that is suitable for their business specialty and business life cycle.

IS enhancement will depend on understanding how the capital market organisations are interdependent. Using the knowledge base as in Figure 1 below will provide a basis for exploring components of data security in capital market organisations. Adding this knowledge gained from the literature review to the current state of the capital market will be very useful to suggest improvements in the ISM area. Specifically, the objectives of the framework are as follows: 1) Develop a framework that is based on theory and informed by existing IS practices in capital market research. 2) Use the framework to summarise what is known about ISM research. 3) Review and analyse the ISM literature from a qualitative methodological approach.

Analysing the information which will be obtained through interviews to understand the current practices regarding IS in the capital markets and using the available literature to understand the factors impacting the IS practices in capital markets will give us a unique knowledge to understand how we can solve the industry problem. The best practices will be extracted from the literature and will then be discussed during the interviews. The analysis of the findings will generate the output of this research. We anticipate that the findings of applying the framework will highlight the importance of ISM and its

application in the capital market sector as well as provide insight into current research for both academics and practitioners.

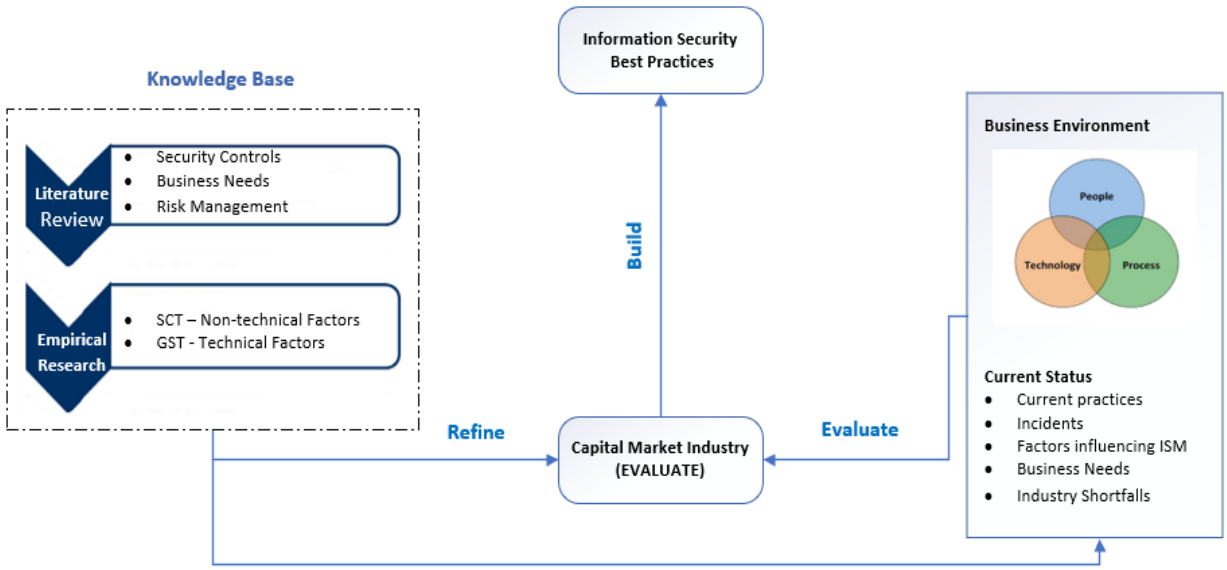

Figure 1. Proposed Research Framework

Expected Contributions

Given the limitations that mentioned by the literature reviews and through the suggested framework will make the following contributions:

- This research will add knowledge and help the capital markets and the research community to understand IS and risk management. Since there is no clear evidence of such research in the literature.
- This research will help executives, IT managers and other technology-related employees and staff to justify prioritisation of IS and risk management, particularly in IT strategy and planning.
- The results will motivate the capital markets to re-evaluate and enhance the internal strategies and guidelines of their data protection and transmitting their sensitive and financial data. It might reduce apprehension by identifying vulnerabilities to minimise data security breaches.
- The findings could support leaders of the capital markets to improve business performance through proactive data security measures so that security breach damages are mitigated, and gaps in their technical practices are addressed as recommended by Kongnso (2015).
- The results will help identify security procedures, daily processes and employees' skills for preventing unauthorised access and security breaches to their assets.
- The results will identify limitations in technical and non-technical environments. This will help to develop appropriate policies to protect the capital markets' financial and sensitive data.
- Evaluating current practices can lead the capital market to identify shortcomings in their daily processes and ways of dealing with sensitive data. Applying the proposed recommendations will lead to creating awareness, increasing efficiency in data management and improving security.

Conclusion and Future Work

This research emphasises the need for improving information security practices in the capital market sector through the empirical suggested framework. An evidence-based framework and guidelines for information security risk management for capital markets institutions has been developed. The application of this framework will help in improve understanding of 1) the electronic threats and emerging trends and challenges impacting on the capital markets; 2) current IS practices, and 3)

deficiencies in security management. During the next stages of this research, the proposed framework will be tested by collecting empirical data through face-to-face interviews. The findings will be used to develop security guidelines for the benefit of capital markets.

References

Australian Computer Society (ACS). 2016. "Cybersecurity Threats Challenges Opportunities." Retrieved 1 January 2019, Sydney NSW, from https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

Bandura, A. 1986. *Social Foundations of Thought and Action: A Social Cognitive Theory*. USA: Englewood Cliffs, NJ: Prentice-Hall.

Barua, A., and Mani, D. 2018. "Reexamining the Market Value of Information Technology Events," *Information Systems Research* (29:1), pp. 225-240.

Bertalanffy, L. v. 1969. *General System Theory: Foundations, Development, Applications*. New York: George Braziller.

Bjerken, A. A. 2017. "Identifying Why Organizations Fail to Adopt Active Cyber-Security Strategies Assessed Using the Unified Theory of Acceptance and Use of Technology Survey (Utaut-S)." USA: Northcentral University.

Bouveret, A. 2018. "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment." International Monetary Fund (IMF) , from: file:///C:/Users/heyhn001/Downloads/wp18143.pdf.

Charmaz, K. 2014. *Constructing Grounded Theory*, (2nd ed.). London: Sage.

Clark, B. W. 2016. "The Effectiveness of a Compliance Strategy to Improve Information Security in the Us Healthcare Sector." USA: Utica College.

Compeau, D., Higgins, C. A., and Huff, S. 1999. "Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study," *MIS Quarterly* (23:2), pp. 145-158.

Coole, M., and Brooks, D. J. 2014. "Do Security Systems Fail Because of Entropy," *Journal of Physical Security* (7:2), pp. 50-76.

Creswell, J. W. 2014. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, (4th ed.). Thousand Oaks, California: Sage.

Federal Financial Institute Executive Council (FFIEC). 2018. "Risk Management." Retrieved 1 February 2018, from https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/risk-management.aspx

Friedhoff, G. M. 2016. "Monitoring Technology Risks across Extended Enterprise Operations: A Case-Study within the U.S. Capital Market." USA: Stevens Institute of Technology.

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Hofstede, G., Neuijen, B., Ohayv, D. D., and Sanders, G. 1990. "Measuring Organizational Cultures: A Qualitative and Quantitative Study across Twenty Cases," *Administrative science quarterly*), pp. 286-316.

Ifinedo, P. 2014. "Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition," *Information & Management* (51:1), pp. 69-79.

Johnson, A. L. 2016. "Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation," *North Carolina Banking Institute* (20:1), pp. 277-310.

Kast, F. E., and Rosenzweig, J. E. 1972. "General Systems Theory: Applications for Organization and Management," *Academy of Management Journal* (15:4), pp. 447-465.

Kim, K., Mithas, S., and Kimbrough, M. 2017. "Information Technology Investments and Firm Risk across Industries: Evidence from the Bond Market," *MIS Quarterly* (41:4), pp. 1347-1367.

Kongnso, F. 2015. "Best Practices to Minimize Data Security Breaches for Increased Business Performance." USA: Walden University.

Line, M. B., Tøndel, I. A., and Jaatun, M. G. 2016. "Current Practices and Challenges in Industrial Control Organizations Regarding Information Security Incident Management–Does Size Matter? Information Security Incident Management in Large and Small Industrial Control Organizations," *International Journal of Critical Infrastructure Protection* (12), pp. 12-26.

Ma, Q., and Pearson, J. M. 2005. "Iso 17799: "Best Practices" in Information Security Management?," *Communications of the Association for Information Systems* (15:1), pp. 577-591.

Malik, J. 2016. "Security Essentials: Clicking with the Enemy." Retrieved 1 December 2018, from https://www.alienvault.com/blogs/security-essentials/clicking-with-the-enemy

McGinn, M. 2018. "Cybercrime Costs Financial-Services Sector More Than Any Other Industry, with Breach Rate Tripling over Past Five Years, According to Report from Accenture and Ponemon Institute," News release, Accenture.

Mischel, W., and Shoda, Y. 1995. "A Cognitive-Affective System Theory of Personality: Reconceptualizing Situations, Dispositions, Dynamics, and Invariance in Personality Structure," *Psychological Review* (102:2), pp. 246-268.

Mithas, S., and Rust, R. 2016. "How Information Technology Strategy and Investments Influence Firm Performance: Conjecture and Empirical Evidence," *MIS Quarterly* (40:1), pp. 223-245.

Mitleton-Kelly, E. 2011. "A Complexity Theory Approach to Sustainability: A Longitudinal Study in Two London Nhs Hospitals," *The Learning Organization* (18:1), pp. 45-53.

Narain Singh, A., Gupta, M., and Ojha, A. 2014. "Identifying Factors of "Organizational Information Security Management"," *Journal of Enterprise Information Management* (27:5), pp. 644-667.

Nelson, K. 2003. "Security Assessment Guidelines for Financial Institutions ". SANS Institute.

NetDiligence. 2016. "Cyber Claims Study," NetDiligence - Cyber Risk Assessment and Data Breach Services, from https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf.

Pelletier, J. M. 2017. "Effects of Data Breaches on Sector-Wide Systematic Risk in Financial, Technology, Healthcare and Services Sectors." USA: Capella University.

Pieri, A. S. 2017. "Global Information Security Spending to Reach $86.4bn in 2017." Retrieved 16 January 2018, from http://www.itp.net/614342-global-information-security-spending-to-reach-$864bn-in-2017,-says-gartner

Qiu, M., Ming, Z., Wang, J., Yang, L. T., and Xiang, Y. 2014. "Enabling Cloud Computing in Emergency Management Systems," *IEEE Cloud Computing* (1:4), pp. 60-67.

Qiu, M., Zhang, L., Ming, Z., Chen, Z., Qin, X., and Yang, L. T. 2013. "Security-Aware Optimization for Ubiquitous Computing Systems with Seat Graph Approach," *Journal of Computer and System Sciences* (79:5), pp. 518-529.

Rampini, A. A., Viswanathan, S., and Vuillemey, G. 2017. "Risk Management in Financial Institutions." Retrieved 10 January 2018, from http://people.duke.edu/~viswanat/financialinstitutions.pdf

Raytheon. 2015. "2015 Industry Drill-Down Report Financial Services." Retrieved 11 January 2019, Websense Security Labs, from https://www.websense.com/assets/reports/report-2015-industry-drill-down-finance-en.pdf

Schatz, D., and Bashroush, R. 2016. "The Impact of Repeated Data Breach Events on Organisations' Market Value," *Information & Computer Security* (24:1), pp. 73-92.

Spanos, G., and Angelis, L. 2016. "The Impact of Information Security Events to the Stock Market: A Systematic Literature Review," *Computers and Security* (58), pp. 216-229.

Stephens, A. J. 2017. "Understanding Security Compliant Behavior: A Case Study." USA: Northcentral University.

Sutton, M. 2017. "The International Telecommunications Union's Arab Regional Cybersecurity Centre Opens Annual Summit in Oman." Retrieved 1 December 2017, from http://www.itp.net/615840-itu-arab-regional-cybersecurity-centre-opens-annual-summit-in-oman

Tang, M. 2013. "Information Security Engineering: A Framework for Research and Practices," *International Journal of Computers Communications and Control* (8:4), pp. 578-587.

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

Yin, R. K. 2014. *Case Study Research: Design and Methods*, (5th ed.). Thousand Oaks, California: Sage.

Zhiwei, Y., and Zhongyuan, J. 2012. "A Survey on the Evolution of Risk Evaluation for Information Systems Security," *Energy Procedia* (17), pp. 1288-1294.