Information Security Risk Management in Small Business Enterprises (SMES)

Nyapete Nicholus Mitende [1] & Kimani John Muhoho[2]
St Paul's University

Abstract

The desire to optimize organizational processes such as planning, control, communication, and collaboration is a significant driver for business enterprises, especially SMEs, to invest in Information Technology (IT). IT investments contribute to improved operational efficiency, financial management, flexibility, and agility, providing a competitive edge in the market. SMEs particularly invest in IT to facilitate new partnerships and collaborations through electronic linkages, enabling them to overcome barriers and enhance business performance. However, IT investments in SMEs face numerous challenges, including insufficient resources, lack of time for implementation, poor IT staff expertise, and inadequate management commitment. Inadequate IT investments often result in Information Security (IS) breaches, leading to significant financial and non-financial losses. Non-financial losses included damage to reputation, product piracy, and theft of critical business information. Effective Information Security Risk Management Investment (ISRMI) is essential for ensuring long-term competitiveness and survival, guiding the selection of security measures to protect IT assets while ensuring data confidentiality, integrity, and availability. However, existing literature lacks guidance on effective ISRMI strategies, focusing primarily on the implementation of ISRM approaches rather than the economics of security investment. This research aimed to explore the ISRMI strategies adopted by SMEs within Nairobi's Central Business District, based on SMEs that have implemented ISRM programs, through a review of literature and interviews with information security experts.

Key Words: *Information Security Risk Management, Information Technology Investment Strategies, Small Business Enterprises (SMEs)*

1.0 Introduction

Wang et al (2010) established that the desire to optimize key organization processes such as planning, controlling, collaboration and communication is a major ingredient for business enterprises to invest in Information Technology (IT). Oladejo and Yinus (2014) concurred by observing that IT investment contributes to improved financial management, operational efficiency, flexibility and agility in responding to increased market pressure while achieving market competitive advantage. Bansal and Sharma (2006) also established that the desire to participate in new forms of partnerships and collaborations enabled by electronic linkages has prompted most business enterprises especially SMEs to perform IT investment. Correct/appropriate IT investment can transform the dynamics of business management and offers

opportunities for business enterprises especially small and medium enterprises (SMEs) to overcome key barriers and improve their survivability in a competitive environment (Manmood&Man, 2008).

The strategic benefits associated with IT have made most business enterprises make huge investment but, McDonagh and Prothero (2009) point out that IT investment in the context of SMEs experiences a variety of challenges such as: insufficient resources dedicated to IT investment, insufficient time devoted to the implementation and maintenance of IT, poor/inadequate IT staff knowledge and impartial advice, poor management attitudes towards IT investment, poor IT investment benefit quantification and lack of formal structure for planning and controlling IT investment procedures within SMEs.

Poor and low IT investments contribute to major Information Security (IS) breaches among SMEs which translate to both financial and non-financial losses. PWC (2015) report points out that in 2014, financial losses incurred by SMEs globally as a result of IS breaches stood at $23 trillion. These financial losses range from decreased revenue, disruption of business systems and regulatory penalty to erosion of customer's confidence. Non-financial losses emanating from IS breaches include damage to business reputation, products piracy, diversion of research and development (R&D) information, negative impact to innovation through stolen products design or prototypes, theft of business and manufacturing processes, and loss of important information such as organization strategic plan.

Serianu's (2014) report established that due to poor IT investment, the IS breaches increased by 100% especially in the last quarter of 2019 and predicted 2020 and beyond as tough periods for SMEs, as IS breaches are likely to increase due to improved IT knowledge among young people. Kaspersky Lab's (2016) report echoes Serianu findings by pointing out that in 2015, SMEs in Kenya suffered an annual loss approximated at $146 due to IS breaches.

An effective Information Security Risk Management Investment (ISRMI) strategy is a key determinant of long-term organization competitiveness and survival. Therefore,its implementation should take into consideration the prudent use of enterprise resources, while ensuring realization

of the core objectives of protecting key organization IT assets from both external and internal threats, and minimizing losses resulting from the occurrence of IS risks incidences. Verendel (2008) established that an effective ISRMI strategy should guide the selection and implementation of the best combination of IT security measures to meet a firm's strategic objectives. While taking into consideration the decision maker's biasness, its successful implementation should provide the board of directors, senior management, regulators and other external stakeholders with confidence that IT can deliver business value efficiently and securely, while providing high-quality assurance around data integrity, availability, and confidentiality (CIA).

The literature on ISRM lacks studies that guide enterprises in performing effective Information Security Risk Management Investment (Al-Ahmad &Mohammad, 2013). Al-Jaghoub, Al-Yaseen, andAl-Hourani (2010) point out that, although some research works attempt to analyze existing ISRM approaches, they mainly focus on listing the advantages and disadvantages of the approaches, and how to implement and manage them and not the economics of information security investment. The purpose of this research was to establish Information Security Risk Management Investment Strategies adopted by Small and Medium Enterprises.

The study was based on SMEs within Nairobi's Central Business District (CBD). During the study, only SMEs that had implemented ISRM program were involved. In order to assess the state of the enterprise ISRM program, a review of relevant literature was carried out together with several interviews with information security experts and practitioners

Small and Medium Enterprises (SMEs)

Small and medium enterprises (SMEs) are the global actors in economic and social growth. A Small and Medium Enterprise is a business segment term used differently in various countries. For instance, in the United States of America (USA), it refers to any business enterprise or firm included in Russel indices. In Europe SME's are considered to be business enterprises or firms with less than 250 employees and an annual turnover not exceeding 50 million Euros, or an annual balance sheet total not exceeding 43 million Euros. In addition, International Chambers of Commerce (ICC) defines SMEs as business entity having 100-2000 employees. In this Study the

researcher adopted the European definition of SMEs, because most of the SMEs in Kenya, especially those in the Microfinance sectors fit to this definition.

Globally, SMEs constitute 80% of business enterprises and contribute between 50%-60% of Gross Domestic Product (GDP). In the European Union (EU), SMEs account for approximately 99% of all business enterprises and employ about 65 million people making the European Parliament to recognize SMEs as an integral engine of growth. Mbogo (2011) points out that in Kenya, SMEs constitute 75% of all the businesses that offer employment to approximately 4.6million people annually, provide 87% of new employment opportunities and contribute 18.4% of the country Gross Domestic Product (GDP). Onyango (2014) also concurs that SMEs are key producers, services providers and facilitators of innovation in Kenya. Therefore, the government of Kenya has prioritized it as the epicenter of economic and industrial development.

Despite SMEs being key ingredient to most global economies, Kivue and Ofafa (2013), established that SMEs experience varied challenges which include: poor market access, poor access to information, inaccessible finances and poor technology. These challenges make it impractical for most SMEs to realize their strategic objectives. To overcome the challenges and improve market access, SMEs are heavily investing in IT. Gupta and Hammond (2005) point out that IT has become an indispensable tool in this highly globalized economy, but its adoption exposes SMEs to IT security breaches. SMEs are more vulnerable to IT attacks because they lack the necessary financial resources, proper infrastructure and expertise to develop comprehensive and well-documented ISRM investment procedures resulting in poor security budgets, making SME's organizations particularly susceptible to IT-related breaches.

Small and Medium Enterprises (SMEs) are increasingly becoming targets of cyber threats due to their limited resources and inadequate investment in information security risk management (Zafar and Clark 2009). In today's digital landscape, SMEs handle sensitive data, perform online transactions, and rely heavily on technology for their operations, making them vulnerable to various security risks. However, many SMEs struggle to implement effective Information Security Risk Management (ISRM) strategies due to constrained financial and human resources (Richardson, 2011).

In Nairobi's Central Business District (CBD), where SMEs play a crucial role in economic growth, there is a lack of clear understanding of how these enterprises allocate resources toward ISRM, the types of investment approach they adopt, and the effectiveness of these approaches in mitigating risks. Insufficient ISRM investment can lead to data breaches, financial losses, reputational damage, and compliance failures, all of which can have severe consequences for SMEs' survival and growth.

This study sought to address the gap in understanding by evaluating the Information Security Risk Management investment approaches implemented by SMEs in Nairobi's CBD. By identifying the strategies used and their effectiveness, the research aimed to provide insights into how SMEs can optimize resource allocation to better manage information security risks.

2.0 Literature Review

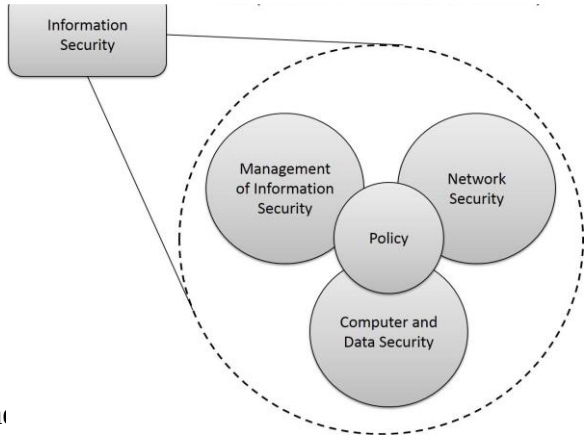
Information Security Risk Management (ISRM)

Information Security Risk Management (ISRM) is the process of recognizing IT-related threats, determining their consequences on the organization's resources, and applying modifying factors in a cost-effective manner to keep adverse consequences within boundary(Nazımoğlu & Özsen, 2010). Andreasson and Koivisto (2013) argued that the purpose of the ISRM is to secure the continuous operation of information systems and data networks which are crucial for business, to protect the unauthorized usage of the data and information systems, unintended and intended data destruction or distortion, and to minimize the derived damages.

Though ISRM assists in securing organizations' key IT assets by maintaining integrity, confidentiality and authenticity, Whitman and Mattord (2013), observe that an effective ISRM program should take into consideration the information system as whole and apply an appropriate policy, training and awareness programs and technology to enhance the integrity of information. Beeb et al(2014), argue that an ISRM's success depends on its ability to ensure accountability, improve Information Security effectiveness and compliance with existing legal frameworks. An effective ISRM can help SMEs to manage risk posture, through proactive determination of key IS threats in both external and internal organization environment and lead a proactive response to

combat the identified threats. Al-Jaghoub et al (2010), argue that an effective ISRM can assist organization top-level management in identifying, managing and optimising risks, by turning organization IS risks into advantages and correctly aligning management's risk appetite with a desired return. Ciorciari and Blattner (2008) also concur by pointing out that effective ISRM can help SMEs define a comprehensive view of IS risks, by continuously refreshing the IT risks inventory and contributing to the creation of strategies to prevent, mitigate, or accept and monitor risk against defined tolerance. Therefore, the management should ensure that ISRM is properly planned, organized, staffed, directed and controlled.

Whitman and Mattord (2013) argued that effective ISRM in an organization is achieved through the combination and implementation of various plans of action, where each plan of action concentrates on a given area of IS within an enterprise. They listed core components of effective ISRM plans of action to include: management of information security, policy, computer and data security and network security.



ISRM Compon

Drivers for the Adoption of Information Security Risk Management among SMEs

Al-Jaghoub et al (2010), argue that the desire to mitigate information security risks is the key objective behind most organizations investing in ISRM. This objective has made most business enterprises globally adopt internationally accepted frameworks, best practices and approaches such as: COBIT5, ISO 27005, MAHERI, and NIST 30-800, Grundultz among others. Other key motivation for the adoption of ISRM among SMEs also include: business requirements, regulators

and compliance mandates, the need to establish proper corporate governance, increasing risk awareness and enterprise competitive market advantage through image building.

Another major business driver for ISRM adoption in SMEs is the need to fill in the gaps and lack of experience in certain areas where SMEs cannot build or establish proprietary standards based on their staff competencies. Also, the need to provide confidence to trading partners, stakeholders, and customers, reducing liability due to unimplemented or enforced policies and procedures, get senior management ownership and involvement and establish a mechanism for measuring the success of the security controls are other key drivers for the adoption of ISRM among SMEs.

Despite the criticality of Information Security Risk Management to business organizations, Earnest and Young report (2013), established that over 50% of ISRM implemented especially in SMEs globally have not yet matured to provide full protection of information. The report further established that though the ISRM uptake among SMEs in developing countries is still low, tremendous progress has been made especially among SMEs in microfinance sectors.

Factors Influencing Information Security Risk Management Investment among SMEs

To gain a competitive advantage and to weather the economic pressure, SMEs are heavily investing in IT. Though there are several cardinals in the business environment which determine how ISRM investment should be structured in the organization, most business enterprises especially SMEs experience some of the following challenges when performing ISRM investment.

Alignment to Business Strategy

The upward trends portrayed by the global information security breaches translate to the increasing economic pressure among business enterprises especially SMEs. Ariyachandra and Frolick (2008) argue that this trend makes ISRMI and business strategy alignment a fundamentally critical ingredient for effective ISRMI. Magnusson (2007), points out that for SMEs to realize the business strategic goal of improving shareholders wealth, the management should ensure that all necessary strategic investment procedures for managing enterprise daily operations are put in place and in tandem with an organization's strategic objective. From ISRM point of view, it is essential that in a competitive environment the right information systems or technology investments are selected in order to sustain corporate viability and prosperity. Therefore, for effective ISRMI, the

management must ensure that each ISRMI component maps to the organization's strategic business objectives. Karim et al. (2007) argue that ISRMI can improve enterprise performance only if it matches business processes and is supported by business structures and processes. They established that despite significant investment, most organization have not realized full benefits due to their own inability to effectively deploy ISRM in their own business strategies. Ensuring that an ISRMI is in alignment and provides support to an organization's strategy is critical for business success (Bleistein, Cox, Verner, &Phalp, 2006). Duh et al. (2006) argue that a quality ISRMI is contingent to on organization strategy.

Organizational Culture

Organizational culture refers to a set of shared values, beliefs, assumptions, and practices that shape and direct members' attitudes and behaviours in an organization. Whitman and Mattord (2013) observe that organizational culture is one of the key challenges to successful ISRMI implementation in business enterprises, especially SMEs. It is extremely challenging to realize quality information security if senior management and staff believe that ISRMI is not a priority but a waste of organization resources. The negative attitude towards ISRMI by the management and staff translates to poor attitude and low priority for ISRMI, which results in small and poorly structured ISRM initiatives within the business enterprise. But, if staff and senior management consider ISRM to be a critical success factor to the organization, they will support it and invest on it adequately, hence improving mitigation to IS threats. Whitman and Mattord (2013) saw it critical that information security and the culture of an organization are aligned.

Fenz et al (2011) established that poor organizational culture has resulted to a lack of quality knowledge and training on ISRM among managers and staffs and this is the core contributor to the non-existence or inadequate ISRM budget within organizations, especially SMEs. Baker and Wallace (2007) concur by pointing out that despite best ISRM approaches and guidelines, without a well-grounded organization culture that promotes quality knowledge on potential attacks, vulnerabilities, and mitigation strategies, efficient ISRMI cannot be realized. without the information security experts, the organization will not have the necessary capacity to consider the complex relationships between various levels of ISRM concepts translating to non-holistic ISRM which puts into risk the operations of the organization.

Wood and Park (2008) opine that poor organization culture translates to poor budget for ISRM activities, bad IS staff attitude and low keenness, less time devoted on ISRM, poor security policy and safeguards implementation and low priority for ISRMI supporting initiatives. Lander and Pinches (2009) also observe that lack of ISRM knowledge results to poor ISRMI decisions, which is a major hindrance to effective ISRM investment. Bommer and Straub (2008), point out that over 80% of ISRM failures emanate from components related to poor organization culture such as adoption of silo approaches to ISRMI. They pointed out that for success in ISRMI organizations, SMEs should adopt a well-integrated and defined organization culture which embeds information security and protection considerations in the management mindset. Good organization culture should support all organization activities, such that information security becomes a natural aspect of every employee's daily routine. However, the integration of Information Security Culture organizations still faces challenges which include: Information Security Culture not being an integral part of the organization, difficulty in getting a sufficient budget for ISRM activities, poor locus of responsibility, and varied perception towards ISRM activities.

Poor locus of responsibility is a core hindrance to ISRMI activities within the organization, for effective planning, controlling and implementation of ISRMI, a distributed approach that involves and makes every employee an integral part of ISRMI should be adopted (Koh et al.,2005). Maynad and Ruigaver (2006) emphasized that effective organisational culture should capture employee motivation which is key to the success of the ISRMI. They pointed out that management should motivate employees to embrace ISRMI initiatives and not consider it an external interference, but a major component of organization operations.

Investment Valuation and Trade-Off

Investment in ISRM constitutes a larger portion of most organizational expenses. As a result, managers should have sound knowledge of the likely impact and a mechanism to justify and realize value from their ISRMI and related resource allocation processes (Mithas et al., 2012). Bardhan et al. (2004), point out that the valuation of ISRMI is challenging as it is characterized by long payback periods, uncertainty, and constantly changing business environments. They pointed out that the widely used utility theory-based RCDM is not suited for ISRMI since it does not

objectively account for the flexibility inherent in most ISRMI decisions. Without taking the option value of flexibility into consideration, firms will not be able to justify strategic ISRMI that provide an accurate representation of strategic business value.

Tsiakis and Pekos (2008) point out that defining ISRMI and having a criteria to evaluate itis a nightmare to most organizations especially SMEs which lacks qualified valuation experts. They argued that since returns on ISRMI cannot be measured quantitatively, considering it in the same footing as other investments results to management viewing ISRMI as an inhibitor to business daily operation. Magnusson et al (2007) point out that identifying and quantifying the benefits of ISRMI is an enormous challenge; this is even made more complex by its dynamic nature which makes it difficult to produce correct calculations for ISRMI compared to other investments.

Lack of proper financial analysis is a core issue/concern towards efficient ISRMI. Wood and Parker (2004) argue that measuring ISRMI is a business issue that must be resolved within the firm's strategic drivers. in addition, White and Mattord (2009) argue that the availability of a wide spectrum of ISRM approaches and absence of quality ISRMI decision making methods makes it absolute difficult for managers to perform effective risks versus cost trade-off in the context of ISRMI. Tsiakis and Pekos (2008) concur by pointing out that ISRMI has both technical and human management issues that require establishment of proper valuation and cost trade-off policies and engagement of qualified staffs.

Stakeholder Participation

Duh et al (2006) explained that a quality ISRMI level is contingent to organization strategy and to other organizational resources which interact with IT and other external environment. They pointed out that ISRM investment independently does not bring any competitive advantage, and that its success requires senior management and staffs to re-engineers core business process by involving key external and internal stakeholders in all critical ISRMI decisions. Turkman(2010) identified organizational environment as a core contingent variable in the determining the levels of ISRMI.

Whitman and Mattord (2013) explain that ISRMI is quite a challenge both indecision making and measuring their efficiency. Therefore for effective information security investment, there is need for an ISRMI investment plan with full participation of all the necessary key stakeholders that interact with the organization. But on the contrary, Wood and Parker (2004) established that most organizations management do not involve key stakeholders in ISRMI decisions, but, instead keep secret losses that emanates from IS breaches, as most managers are not willing to tarnish organizations reputation by informing about the damage that IS breach has caused.

Approaches to Information Security Risk Management Investment (ISRMI)

Studies shows that due to strategic benefits associated with information security initiatives, most organizations are heavily investing in it to minimize losses and potential damages associated with the use and integration of IT in the business environment. Most studies carried out by researchers and academicians on ISRMI have focused and promoted the use of Rational Choice Decision Model (RCDM) to guide ISRMI within organizations since they have approached the ISRMI issues theoretically (Gordon and Loeb, 2002 and Huang et al.,2008). Some of ISRMI approaches based on RCDM include:

Experts of optimum ISRMI methods have proposed various strategies to determine the optimum resources that firms should dedicate to ISRM activities. Kort et al. (2004) proposed two frameworks that can be used to determine optimum resource firms can dedicate to ISRMI. In the first framework, they considered the firm's objective to be reduction of losses due to felonious (incomplete). In this scenario they pointed out that the discounted streams of reduction in criminal activities is equal to marginal ISRMI. In the second framework, they considered firms reputation as the key driver for ISRMI. They established that successful organizations with good reputation but without ISRM are in greater risks of security breaches. Kort frameworks established that the optimum ISRM decision maker objective is to improve the net income streams while enhancing the security of organization critical assets and reputation.

Gordon and Loeb (2006) developed an economic model which determines an optimum amount of investment that can provide security to a set of organization assets and resources. The model postulates that the ISRM implementer in an organization is risk impartial when making decisions as relates to ISRM investment. The model argued that risk impartial enterprises will improve their

expected value from ISRMI. In their model, Gordon and Loeb evaluated how the vulnerability within the organization and potential loss from such vulnerabilities influences the optimum amount to be committed in securing organizational assets and resources. In their approach, they argued that the expenses incurred in securing organization assets should not exceed 37% of the expected loss emanating from the occurrence of the security breach. They postulated that since extremely vulnerable information asset may be difficult to protect, an organization may better concentrate its energy on assets with mid-level vulnerabilities. Gordon and Loeb further opined that for business enterprise to drive full benefit from their ISRM investment activities, they should only commit a small fraction to the ISRMI processes.

Huang et al (2008) model determines optimum investment levels while addressing multiple information security breaches and countermeasure technology. The model proposed several findings on ISRM practices. It approaches Optimum ISRM investments with the assumption that the decision makers are risk averse. This assumption informs the difference between Huang model and the Loeb's model. Huang et al (2008) model shows that organizations with performance above average are risk averse and this makes them to be willing to invest more in ISRM initiatives, though they do not consider some risk worth investing in. Huang et al views on ISRM investment is supported by Fiegenbaun and Thomas (2003), when they pointed out that threat perverse organization spend more on ISRMI process. Huang's model offers core managerial insight into the process of making ISRM investment decision by pointing out that for organizations to invest in ISRM, then the information security breaches must meet a set threshold which is worth investing in. The Huang model argues that ISRMI does not always increase with effectiveness of investment, and does not increase proportionally with the decision maker risk averse... They observe that for successful ISRMI practices, the organization should carefully evaluate the risk impact on other businesses. They also point out that the optimum investment level will increase proportionately to organization risks, therefore, before considering the ISRM investment, an organization should first evaluate its risks environment.

Hausken (2006) using the economic model determined the relationship between ISRMI and vulnerability. They evaluated the effect of return on optimum investment levels, where they established that the nature of return is a core determinant in ISRMI decision process. Hausken

identified four categories of ISRM investment breach functions and also identified four types of marginal returns compared to Gordon and Loeb one marginal return.

Wang et al (2008) developed a probability based framework to determine the chance of attacks on the organization secured assets and the amount of resources to be committed in protecting the asset with the support of API algorithm and OSI algorithm. The proposed API algorithm employed is anchored on the threat flows approach which models probabilistic flows of ISRM breaches. The OSI algorithm is anchored on a threat impartial perspective which argues that the optimum resources committed to ISRM should improve cumulative value for the organization.

Matsuura (2003) criticized Gordon and Loeb model since it was based on a single decision variable. Tatsumi et al. (2009) also pointed at the weakness of Gordon and Loeb model as it did not take into consideration dynamism prospects such as changing value of money with time. To counter these shortcomings, they proposed real option theory for the achievement of Optimal timing of ISRM investment levels. Moreover, the core findings of their studies had established that absolute change of the threats results to greater and future expenditures, while negative drift of threats results to less and immediate ISRM expenses. In their study, they established that early ISRMI is a major contributor to threat mitigation. Therefore, effective mitigation technology should encourage or promote early ISRM investment activities. Based on their studies and findings, they emphasized the need to identify and determine the form of vulnerabilities and the impact.

In their research, Cavusoglu et al.(2008) while analyzing challenges of ISRMI decisions from Game Theory point of view discovered that conventional ISRM methods are incomplete and instead they proposed this theory as a solution to ISRMI challenges. In their studies they took into consideration the sequential and simultaneous game approaches between various organizations and attackers and compared the outcome along varied dimensions which include investment levels, vulnerabilities and investment payoff. Their research established that organizations can learn from prior observation of the attacker effort and use the experience to estimate the future attacks. The difference between outcome when the decision and Game Theory is used diminishes overtime. Cavusoglu et al (2008) theory approach is based on the assertion that both the organization and the

attacker are well aware of the vulnerabilities to be exploited. Cavusoglu et al (2008) model is more objective when ISRMI challenges integrate both targeted and random attack.

Bandyopadhyay et al (2012) established that attackers study potential targets to identify vulnerabilities through creation of competition in ISRMI among organization that posses similar IT assets. They proposed the use of differential game model to analyze ISRMI decision. In their research, they discovered that ISRM planning should not be treated as internal affair but knowledge sharing should be ensured across all the organizations that can be of interest to the attacker. In their study, they established that for effective knowledge sharing among organization, the organization with the critical and superior information resources or assets should initiate the process and provide necessary motivational for other organization.

Ionnidis et al (2011) proposed utility theoretic model with core objective of establishing optimum intervention in ISRMI, through utilization of Utility Theory. They designed limiting conditions under which given realized risk, decision to invest, delay or abandon can be justified. Their core aim was decision making as regards to differed costly deterministic investment, when the cost associated with future ISRM vulnerabilities are not known clearly. Their investment function has irreversible fixed costs which introduces rigidity into the ISRM investment decision making process. The rigidity causes delays in the implementation of security measures, which translate to cyclic ISRM investment.

Karjalainen et al. (2014) studied ISRMI from stakeholder theory perspective established that ISRMI processes involve more than identifying optimum investment level or agreeable return on ISRM investment. Based on their empirical findings, they proposed a stakeholder value theory which is both descriptive and instrumental to ISRMI. Their theory is descriptive since it identifies the key stakeholders, their values and values orientation towards ISRMI decision making. The theory explains that ISRMI decisions are driven by three key stakeholders who are the users, information security professionals and organization managers. They also observed that all the key stakeholders have different value orientation which must be satisfied for them to support ISRMI. Karjalainen et al (2014) theory is considered instrumental because it clearly outlines the process of ensuring the success of ISRMI. The key contribution of the theory is the recognition of various

stakeholders, appreciation of their value and value orientation in ISRM investment process. Overall the theory recognizes efficiency as the expectation of all the stakeholders and explains that this can be achieved through critically evaluating and understanding the differences in opinion among the key stakeholders.

3.0 Methodology

To sufficiently achieve the core objective of this study, the researcher adopted a mixed-methods study approach. Further, to realize better research outcomes when applying the chosen research design, study strategies that support mixed study techniques were implemented. The selected research strategy for the study used the descriptive survey strategy since it provides an accurate and valid representation of variables and establishes causal links between variables that pertain to the research problem. Also the study strategy can effectively support triangulation since it can be corroborated.

The study area was Nairobi Central Business District (CBD). The location was chosen due to the following reasons: It had the highest number of Microfinance SMEs in Kenya; most of the Microfinance SMEs in the area had implemented ISRM and therefore we experiencing ISRM investment challenges and the researcher(s) also came from the study location.

Sample Size

Since the researcher used a mixed methods approach in the study, there was a -need to adopt a sample size that could be effectively generalized to provide in depth understanding of the study elements. The selection of the sample size was also influenced by factors such as population size, purpose of the study, level of precision, level of confidence and degree of variability in the attribute being studied. As advised by Kothari (2006) for the descriptive component of the study 95% confidence level, ±5 precision and confidence level was realized through the use of Cochran formulae.

Cochran formulae for Infinite population (n_0)= $\frac{z^2PQ}{E^2}$

Where N is Population size, n_0 is infinite sample size, Z is desired confidence level, P is estimated proportion of attribute present in the population, Q is 1-p, E is the desired level of precision.

Cochran's infinite sample size (n_0) = $\frac{z^2PQ}{E^2}$

= ***1.96 X(0.5)(O.5)*** $\Big/$ ***(0.5^2)***

= 383

In this research the study population was finite and Cochran's formulae was adopted to determine the sample size as follow:

Population size (***N***) =600 people

Desired confidence level (Z)= 95%

Estimated proportion of attribute present in the population (P)=0.5

1-P (Q) = 1-0.5=0.5

Desired level of Precision= 0.05

Infinite population sample size (n_0)=383 *

Sample Size (n) = $\frac{n_0}{1+\frac{(n_0-1)}{N}}$

N= $\frac{383}{1+\frac{383-1}{600}}$ **= 106 People**

Response Rate

After the identification and demarcation of the study organizations and participants, the research instruments (questionnaires) were distributed. For this study, 106 questionnaires were distributed to the targeted staffs in Information Technology, Finance and Accounts, and Purchasing and

Supplies departments, of which 103 of the questionnaires were returned thereby translating to 97% response rate

4.0 Results and Discussion

The research findings pointed out that most SME organizations were pursuing information security objectives with the core interest of protecting the confidentiality, integrity, and availability of information systems even in adverse situations in order to gain competitive advantage through building a good reputation that promotes stakeholders' confidence (Beebe et al,2014). Al-Jaghoub (2010) also observes that the desire to mitigate information security risks has made most business organization to invest in information security risk management through implementing various risk approaches to information security.

The study findings established that: business requirements, human resource, regulatory and compliance requirements are the major drivers for Information Security Risk Management Investment within SMEs. The study established that most of the SMEs within the study area had implemented information security risk management approaches such as NIST SP 800-30, ISO 27005, ITIL, among other approaches. On factors that influenced the Information Security approaches implemented, the study established that most SMEs choice of the framework was influenced by what other organizations in the same line of business had implemented and marketing advice from the implementers.

The study findings recognized organizational culture as a major hindrance to effective Information Security Risk Management. The researcher established that management and staff in most SMEs did not value, or appreciate the impact of Information Security Risk Management Investments, resulting in less time and budget devoted to information security risk management investment activities. The study also pointed out that poor organizational culture among SMEs resulted to poor and haphazardly implemented information security policies and organizational structure that hindered effective communication. In addition, there was low management and staff commitment to information security risk management, and poor knowledge among staff and management on information security risk management. The findings of the study on organizational culture were congruent with Whitman and Mattord (2013) who established that it is difficult to realize quality information security within the organization if the management and staff have low interest in

information security risk management investment. Mithas et al (2012) support the study finding by pointing out that for effective information security risk management within the organization, management should have sound mastery of Information Security Risk Management Investment. Wood and Park (2008) also concur with the study findings by pointing out that a poor organizational culture translates to a poor information security budget, poor management and staff keenness on information security and poor organization security policy.

The study findings pointed to the fact that most SMEs which participated in the study did not have well documented risks and asset inventories. For an effective information security risk management investment within SMEs, there is need to correctly identify and develop an up to date organization and asset inventories. The study established that correct information security risk management investment was strongly influenced by the correct identification and documentation of organization assets and risks.

Alignment of business strategy to organization Information Security Risk Management is critical for the success of efficient ISRMI. The study established that most SMEs' business strategy did not recognise and prioritize Information Security. This resulted in increased vulnerability among most SMEs due to poor ISRM investments. Previous studies such as Karim et al (2007) pointed out that Information Security risk Management Investment can only improve business enterprise performance if it is supported by business strategy. They also pointed/explained/expounded out that failure to align information security to business strategy results to poor management attitude towards information security resulting in poor budget allocation for information security investment initiatives within the organization.. Duh et al (2006) echo the study findings by pointing out that quality Information Security Risk Management Investment is contingent on organization business strategy. They established that information security risk management investment initiatives independently did not have any competitive advantages. The study pointed out that aligning information security risk management investment to business strategy would make the management and staff have positive attitudes towards information security risk management investment resulting in correct information security investments.

The finding of the study also established that correct valuation and trade-off of information security risk management investment was a major challenge experienced by SMEs. The study established that most SMEs did not have a well-defined valuation and trade-off models and lacked expertise with valuation skills for Information Security Risk Management investment decision. For investment valuation and trade-offs, the study established that most SMEs use utility theory based Rational Choice Decision Model, which is not effective when it comes to ISRMI. Since past study findings had established that quantifying information security investment is difficult. Tsiakis and Pekos (2008) supported the study findings by pointing out that defining criteria for ISRM investment is a nightmare for most organizations especially SMEs. Bardhan et al (2004) established that valuation of ISRM investment is a major challenge experienced by SMEs because ISRM investment experiences long time payback period.

The study findings also established that effective Information Security Risk Management requires the involvement of both internal and external stakeholders. But in most SMEs, it was discovered that most key players in information security investment did not consult the necessary key stakeholders resulting to poor or low knowledge. The study established organizations' senior management tendencies to keep information security breaches secret due to phobia of tarnishing organization reputation as a key challenge to information security risk management since it hinders effective knowledge sharing.

5.0 Conclusion

The study established that an efficient Information Security Risk Management Investment model should take into consideration the human perception factors such as framing and evaluation and organization factors such as organization culture, investment valuation, business strategy, stakeholder participation, IT asset inventory, and risk inventory**.**

References

Al-Jaghoub, S., Al-Yaseen, H., & Al-Hourani, M. (2010). Evaluation of Awareness and Acceptability of Using e-. Government Services in Developing Countries: the Case of Jordan. *The Electronic Journal Information Systems Evaluation*, *13*(1), 1–8.

Ariyachandra, T. R., & Frolick, M. N. (2008). Critical Success Factors in Business Performance Management—Striving for Success. *Information Systems Management*, *25*(2), 113–120.

Bacon, C. J. (1994). Why companies invest in information technology. In *Information management* (pp. 31–47). Boston: Springer.

Baker, W. H., Rees, L. P., & Tippett, P. S. (2007). Necessary measures: metric-driven information security risk assessment and decision making. *Communications of the ACM*, *50*(10), 101–106. https://doi.org/10.1145/1290958.1290969

Baker, W., & Wallace, L. (2007). Is Information Security Under Control?: Investigating Quality in Information Security Management. *IEEE Security and Privacy Magazine*, *5*(1), 36–44. https://doi.org/10.1109/MSP.2007.11

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). A framework for integrated risk management in information technology. *Management Decision*, *37*(5), 437–445.

Bandyopadhyay, T., Liu, D., Mookerjee, V. S., & Wilhite, A. W. (2014). Dynamic competition in IT security: A differential games approach. *Information Systems Frontiers*, *16*(4), 643–661.

Barba-Sanchez, V., Martinez-Ruiz, M. del P., & Jimenez-Zarco, A. I. (2007). Drivers, Benefits and Challenges of ICT adoption by small and medium sized enterprises (SMEs): A Literature Review. *Problems and Perspectives in Management (Open-Access)*, *5*(1), 103–114.

Bardhan, I. R., Bagchi, S., & Sougstad, R. (2004). Prioritizing a portfolio of information technology investment projects. *Journal of Management Information Systems*, *21*(2), 33–60.

Barlette, Y., & Fomin, V. (2009). The adoption of Information Security Management Standards: A Literature Review. In *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions* (pp. 119–140). New York: IGI Global.

Behnia, A., Rashid, R. A., & Chaudhry, J. A. (2012). A Survey of Information Security Risk Analysis Methods. *The Smart Computing Review*, *2*(1), 72–94. https://doi.org/10.6029/smartcr.2012.01.007

Bitange - Ndemo, E. (2006). Assessing sustainability of faith based enterprises in Kenya. *International Journal of Social Economics*, *33*(5/6), 446–462.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In *Proceedings of the 2001 workshop on new security paradigms* (pp. 97–104). New York: ACM Press. https://doi.org/10.1145/508171.508187

Bleistein, S. J., Cox, K., Verner, J., & Phalp, K. T. (2006). B-SCP: A requirements analysis framework for validating strategic alignment of organizational IT based on strategy, context, and process. *Information and Software Technology*, *48*(9), 846–868.

Boltz, J. (1999). *Informational Security Risk Assessment: Practices of Leading Organizations*. DIANE Publishing.

Brink, D. (2001). "A guide to determining return on investment for e-security." *RSA Security Inc.*

British Standards Institution. (2013). BS ISO/IEC 27002:2013: information technology - security techniques - code of practice for information security controls (2nd ed.). London: BSI.

Brotby, K. (2009). *Information Security Governance: A Practical Development and Implementation Approach*. London: John Wiley & Sons.

Burnard, P. (1991). A method of analysing interview transcripts in qualitative research. *Nurse Education Today*, *11*(6), 461–466.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A Model for Evaluating IT Security Investments. *Commun. ACM*, *47*(7), 87–92. https://doi.org/10.1145/1005817.1005828

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems*, *25*(2), 281–304.

Church, B. K., Libby, T., & Zhang, P. (2008). Contracting Frame and Individual Behaviour: Experimental Evidence. *Journal of Management Accounting Research*, *20*(1), 153–168.

Ciorciari, M., & Blattner, P. (2008). *Enterprise risk management maturity-level assessment tool* (pp. 1–3). Retrieved from *https://www.soa.org/...monographs/2008...symposium/mono-2008-m-as08-1-ciorciari...*

Cole, F. L. (1988). Content Analysis: Process and Application. *Clinical Nurse Specialist*, *2*(1), 53.

Coles-Kemp, E., & Overill, R. (2006). The Information Security Ownership Question in ISO/IEC 27001 - an Implementation Perspective. In C. Valli, & A. Woodward (Eds.),

Proceedings of the 4th Australian Information Security Management Conference (pp. 49–56). Edith Cowan University.

Dawson, C. (2002). Practical research methods: a user-friendly guide to mastering research q techniques and projects. Oxford: How to Books.

Devers, C. E., McNamara, G., Wiseman, R. M., & Arrfelt, M. (2008). Moving Closer to the action: Examining Compensation Design Effects on Firm Risk. *Organization Science*, *19*(4), 548–566.

Duh, R.-R., Chow, C. W., & Chen, H. (2006). Strategy, IT applications for planning and control, and firm performance: The impact of impediments to IT implementation. *Information & Management*, *43*(8), 939–949.

Edwards, W., Miles, R. F., & von Winterfeldt, D. (Eds.). (2007). *Advances in Decision Analysis: From Foundations to Applications*. Cambridge: Cambridge University Press.

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *Academy of Management Review*, *14*(4), 532–550. https://doi.org/10.5465/AMR.1989.4308385

Eisenhardt, K. M. (1991). Better Stories and Better Constructs: The Case for Rigor and Comparative Logic. *The Academy of Management Review*, *16*(3), 620.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: opportunities and challenges. *Academy of Management Journal*, *50*(1), 25–32. https://doi.org/10.5465/AMJ.2007.24160888

Faraj, S., & Sambamurthy, V. (2006). Leadership of information systems development projects. *IEEE Transactions on Engineering Management*, *53*(2), 238–249. https://doi.org/10.1109/TEM.2006.872245

Fenz, S., Ekelhar, A., & Neubaue, T. (2011). Information Security Risk Management: In which Security Solutions is it worth Investing? *Communications of the Association for Information Systems :*, *28*(1), 329–356.

General Accounting Office. (1996). *Content analysis : a methodology for structuring and analyzing written material*. Washington, D.C.: U.S. General Accounting Office.

Gal-Or, E., & Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research*, *16*(2), 186–208. https://doi.org/10.1287/isre.1050.0053

Ghobakhloo, M., Hong, T. S., Sabouri, M. S., & Zulkifli, N. (2012). Strategies for Successful Information Technology Adoption in Small and Medium-sized Enterprises. *Information*, *3*(4), 36–67. https://doi.org/10.3390/info3010036

Gillham, B. (2005). *Case study research methods*. London: Continuum.

Goodhue, D. L., & Thompson, R. L. (1995). Task-Technology Fit and Individual Performance. *MIS Quarterly*, *19*(2), 213. https://doi.org/10.2307/249689

Gordon, L. A., & Loeb, M. P. (2007). Economic aspects of information security: An emerging field of research. *Information Systems Frontiers*, *8*(5), 335–337. https://doi.org/10.1007/s10796-006-9010-7

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security*, *13*(4), 297–310. https://doi.org/10.1108/09685220510614425

Halliday, S., Badenhorst, K., & von Solms, R. (1996). A business approach to effective information technology risk analysis and management. *Information Management & Computer Security*, *4*(1), 19–31. https://doi.org/10.1108/09685229610114178

Hausken, K. (2007). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to

vulnerability. *Information Systems Frontiers*, *8*(5), 338–349. https://doi.org/10.1007/s10796-006-9011-6

Herath, H. S. B., & Herath, T. C. (2008). Investments in Information Security: A Real Options Perspective with Bayesian Postaudit. *Journal of Management Information Systems*, *25*(3), 337–375. https://doi.org/10.2753/MIS0742-1222250310

Home land security. (2008). *A roadmap for cyber security research* (pp. 1–126). Washington: INFOSEC Research Council (IRC).

Hornbil Systems. (2009). *ITIL State of the Nation survey* (pp. 1–22). London: Hornbil Systems.

Huang, C. D., Hu, Q., & Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics*, *2*(114), 793–804.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, *13*(4), 247–255.

International Standards Organization (ISO). (2005). *ISO/IEC 27002:2005. Information technology, Security techniques and Code of practice for information security management*. Retrieved from https://www.iso.org/standard/50297.html

Ioannidis, C., Pym, D., & Williams, J. (2013). Fixed Costs, Investment Rigidities, and Risk Aversion in Information Security: A Utility-theoretic Approach. In B. Schneier (Ed.), *Economics of Information Security and Privacy III* (pp. 171–191). New York, NY: Springer New York.

ISACA. (2009). *Risk IT Framework* (pp. 1–106). Rolling Meadows: ISACA.

IT Governance Institute. (2007). *IT controls objectives for Basel II: the importance of governance and risk management for compliance*. Rolling Meadows IL: IT Governance Institute.

Jung, C., Han, I., & Suh, B. (1999). Risk analysis for electronic commerce using case-based reasoning. *International Journal of Intelligent Systems in Accounting, Finance & Management*, *8*(1), 61–73.

Kahneman, D., Slovic, P., & Tversky, A. (1982). *Judgment under Uncertainty: Heuristics and Biases*. New York: Cambridge University Press.

Kahneman, D. (1979). Prospect theory: an analysis of decision under risk. *Econometrica*, *47*(2), 263–291.

Kahneman, D., & Tversky, A. (1973). On the psychology of prediction. *Psychological Review*, *80*(4), 237–251.

Kahneman, D., & Tversky, A. (1982). Subjective probability: A judgment of representativeness. In D. Kahneman, P. Slovic, & A. Tversky (Eds.), *Judgment under uncertainty* (pp. 32–47). Cambridge: Cambridge University Press.

Kahneman, D., & Tversky, A. (1982). The simulation heuristic. In D. Kahneman, P. Slovic, & A. Tversky (Eds.), *Judgment under uncertainty: Heuristics and biases (pp. 201-208).* New York: Cambridge University Press.

Kambil, A., Henderson, J. C., &Mohsenzadeh, H. (1992). *Strategic management of information technology investments: an options perspective*. Cambridge: Massachusetts Institute of Technology.

Karim, J., Somers, T., & Bhattacherjee, A. (2007). The impact of ERP implementation on business process outcomes: a factor-based study. *Journal of Management Information Systems*, *24*(1), 101–134. https://doi.org/10.2753/MIS0742-1222240103

Karjalainen, M., Siponen, M., Kohli, R., & Shao, X. (2014). "*What's in it for me ? A Stakeholder Theory perspective on Information Technology Security Investment," Completed Research Paper (pp. 1–30).* Brisbane: The University of Queensland.

Kiveu, M., & Ofafa, G. (2013). Enhancing market access in Kenyan SMEs using ICT. *Global Business and Economics Research Journal*, *2*(9), 29–46.

Knapp, K. J. (Ed.). (2009). *Cyber-security and global information assurance: threat analysis and response solutions*. Hershey, PA: IGI Global.

Kothari. (2004). *Research methodology methods and techniques* (2nd ed.). New Delhi: New Age International.

Kort, P. M., Haunschmied, J. L., & Feichtinger, G. (1999). Optimal firm investment in security. *Annals of Operations Research*, *88*(0), 81–98.

Kort, P. M., Haunschmied, J. L., & Feichtinger, G. (1999). Optimal firm investment in security. *Annals of Operations Research*, *88*(0), 81–98.

Liu, D., Ji, Y., & Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. *Decision Support Systems*, *52*(1), 95–107.

Li, M. (2014). *A resource management framework for cloud computing* (Thesis). Virginia Polytechnic Institute and State University, Blacksburg.

Magnusson, C., Molvidsson, J., & Zetterqvist, S. (2007). Value creation and return on security investments (ROSI). In *New Approaches for Security, Privacy and Trust in Complex Environments* (pp. 25–35). Springer, Boston.

Marchand, D. A., Kettinger, W., & Rollins, J. D. (2000). Information Orientation: People, Technology and the Bottom Line. *MIT Sloan Management Review*, *42*, 69–80.

Matsuura, K. (2003). Information security and economics in computer networks: an interdisciplinary survey and a proposal of integrated optimization of investment. *Computing in Economics and Finance* (48), 1-13.

Mithas, S., Ramasubbu, N., &Sambamurthy, V. (2011). How Information Management capability influences firm performance. *MIS Quarterly*, 35(1), 237-256.

Mithas, S., Tafti, A., Bardan, I., & Goh, J. M. (2012). Information Technology and Firm Profitability : Mechanisms and Empirical Evidence. *MIS Quarterly*, 36(1), 205-224.

Mizzi, A. (2010). Return on information security investment – The viability of an anti-spam solution in a wireless environment. *International Journal of Network Security* 10(1), 18-24.

Katwalo, A. M., &Muhanji, S. I. (2014). Critical success factors for the “unbanked” customers in Kenya. *International Journal of Bank Marketing*, *32*(2), 88–103.

Myers, M. D. (2009). *Qualitative research in business and management*. Los Angeles: SAGE.

Niederman, F., Brancheau, J.C., Wetherbe, J.C., 1991. Information systems management issues for the 1990s. *MIS Quarterly, 15* (4), 475-502.

NIST 800–30 (2002). Risk Management Guide for Information Technology Systems, Special publication SP 800-30. [Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, last accessed March, 2016].

NIST 800–39 (2008). Managing Risk from Information Systems – An Organizational Perspective, NIST Special Publication 800–39. [Retrieved from: http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf, last accessed January, 2016].

NIST (IR7358) (2007). Program Review for Information Security Management Assistance – PRISMA. [Retrieved from: http://csrc.nist.gov/publications/nistir/ir7358/NISTIR-7358.pdf, last accessed March, 2016].

NIST (2007). Security Maturity Levels. [Retrieved from: http://csrc.nist.gov/groups/SMA/prisma/security_maturity_levels.html, last accessed January, 2016].

Nazımoğlu, Ö., & Özsen, Y. (2010). Analysis of risk dynamics in information technology service delivery. *Journal of Enterprise Information Management*, *23*(3), 350–364.

Oladejo, M. O., & Yinus, O. (2014). An influential analysis of the impact of information technology (IT) on cooperative services in Nigeria. *European Journal of Business and Innovation Research*, *2*(3), 11–24.

Patten, M. L., & Newhart, M. (2017). *Understanding Research Methods: An Overview of the Essentials*. New York: Taylor & Francis.

Purser, S. (2004). Improving the ROI of the security management process. *Computers & Security*, 23 (2004), 542-546.

Price water Coopers.(2015). 2014 annual report of Price Water Coopers. Retrieved from https://www.pwc.com/gx/en/about-pwc/global-annual-review-2015/campaign-site/pwc-global-annual-review-2015.pdf

Ranyard, R., Crozier, W. R., & Svenson, O. (Eds.). (1997). *Decision making: cognitive models and explanations*. London: Routledge.

Raz, T., & Hillson, D. (2005). A Comparative Review of Risk Management Standards. *Risk Management*, *7*(4), 53–66. https://doi.org/10.1057/palgrave.rm.8240227

Royer, I., &Zarlowski, P. (1999). *Research Design.* In Thietart R., A., (ed.), Doing Management Research: A Comprehensive Guide (pp. 126). London: Sage.

Reyck, B. D., Grushka-Cockayne, Y., Lockett, M., Calderini, S., R., Moura, M., and Sloper, A. (2005). The impact of project portfolio management on information technology projects. *International Journal of Information Management* 23 (2005), 524-537.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (5th ed). New York: Prentice Hall.

Schlarman, S. (2007). Selecting an IT Control Framework. *EDPACS*, *35*(2), 11–17.

Smith, S. & Spafford, E. (2004). "Grand Challenges in Information Security: Process and Output," *IEEE Security & Privacy* (2), 69-71.

Sipior, J. C., & Ward, B. T. (2008). A framework for information security management based on guiding standards: a United States perspective. *Issues in Informing Science and Information Technology*, *5*, 051–060.

Stamp, P., Penn, J., Adrian, M., & Gray, B. (2015, August 2) "Increasing Organized Crime Involvement means More Targeted Attacks, Forrester Research. Retrieved from http://www.forrester.com/Research/Document/Excerpt/0,7211,37505,00.html

Stefan Fenz, Johannes Heurix, Thomas Neubauer, & Fabian Pechstein. (2014). Current challenges in information security risk management. Information Management & Computer Security, 22(5), 410–430.

Stewart R. Miller, & Anthony D. Ross. (2003). An exploratory analysis of resource utilization across organizational units. International Journal of Operations & Production Management, 23(9), 1062–1083.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards. *International Journal of Electrical & Computer Sciences*, *35*(1), 7–11.

Symantec Corporation. (2009). *Symantec global internet security threat report: trends for 2008* (pp. 1–110). Boulevard: Symantec Corporation.

Tatsumi K., Goto M. (2010) Optimal Timing of Information Security Investment: A Real Options Approach. In: Moore T., Pym D., Ioannidis C. (eds) *Economics of Information Security and Privacy (pp 211 – 228)*. Boston: Springer

Thompson, B. (Ed.) (2003). *Score reliability: Contemporary thinking on reliability issues*. Newbury Park, CA: Sage.

Trkman, P. (2009). "The critical success factors of business process management. *International Journal of Information Management,* 30 (2010), 125-134.

Tsiakis, T., Kargidis, T., & Katsaros, P. (Eds.). (2014). *Approaches and processes for managing the economics of information systems*. Hershey, Pa: Business Science Reference.

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security. *Computers & Security*, *24*(2), 105–108. https://doi.org/10.1016/j.cose.2005.02.001

Tsiakis, T., & Pekos, G. (Eds.). (2008). *Analyzing and determining return on investment for information security: proceedings of the 2006 International Conference on Applied Economics (ICOAE)*. Cham: Springer.

Tsiakis, T. K., & Pekos, G. D. (2008). Analysing and determining Return on Investment for Information Security. In *International Conference on Applied Economics – ICOAE 2008* (pp. 879–883). Thessaloniki: University of Macedonia.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C., &Gritzalis, S. (2010). A security standards' framework to facilitate best practices' awareness and conformity. *Information Management & Computer Security*, *18*(5), 350–365.

Tversky, A., & Kahneman, D. (1981). The Framing of Decisions and the Psychology of Choice. *Science* 211(4481), 453-458.

Tversky, A., & Kahneman, D. (1992), "Advances in prospect theory: Cumumlative representation of uncertainty," *Journal of Risk and Uncertainty* 5, 297-323.

Wagner, T., Hennig-Thurau, T., & Rudolph, T. (2009), "Does Customer Demotion Jeopardize Loyalty?" *Journal of Marketing* 73(3), 69-85.

Wang, J., Chaudhury, A., and Rao, H.R. (2010). "A Value-At-Risk Approach to Information Security Investment," *Information Systems Research* 19(1), 106-120.

Waweru, N., &Spraakman, G. (2012). The use of performance measures: case studies from the microfinance sector in Kenya. Qualitative Research in Accounting & Management, 9(1), 44–65.

West, R. (2008). The psychology of security. *Communications of the ACM*, *51*(4), 34–40.

Westerlind, K. (2004). *Evaluating return on information technology investment* (Thesis). Gothenburg University, Gothenburg.

Whitman, M. E., & Mattord, H. J. (2013). *Management of information security* (Fourth edition). Stamford: Cengage Learning.

Wood, C. C., & Parker, D. B. (2004). "Why ROI and similar financial tools are not advisable for evaluating the merits of security projects." *Computer Fraud & Security*, *2004*(5), 8–10.

Yin, R. K. (2009). *Case Study Research: Design and Methods* (2nd ed.). Thusand Oaks: SAGE.

Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems*, *24*, 571–596.

Zhou, L., Vasconcelos, A., & Nunes, M. (2008). Supporting decision making in risk management through an evidence-based information systems project risk checklist. *Information Management & Computer Security*, *16*(2), 166–186.