International Journal of Professional Business Review
ISSN: 2525-3654
Universidade da Coruña

Ndungu, Stanley; Wanjau, Kenneth; Gichira, Robert; Mwangi, Waweru

MODERATING ROLE OF ENTREPRENEURIAL ORIENTATION ON THE RELATIONSHIP BETWEEN INFORMATION SECURITY RISK ASSESSMENT AND FIRM PERFORMANCE IN KENYA

International Journal of Professional Business Review,
vol. 3, no. 2, 2018, July-December, pp. 131-152
Universidade da Coruña

DOI: https://doi.org/10.26668/businessreview/2018.v3i2.60

Available in: https://www.redalyc.org/articulo.oa?id=553658822001

How to cite
Complete issue
More information about this article
Journal's webpage in redalyc.org

Scientific Information System Redalyc
Network of Scientific Journals from Latin America and the Caribbean, Spain and Portugal
Project academic non-profit, developed under the open access initiative

e-ISSN:2525-3654

JPBReview

International Journal of Professional Business Review

Responsible Editor: Maria Dolores Sánchez-Fernández, Ph.D.
Associate Editor: Manuel Portugal Ferreira, Ph.D.
Evaluation Process: Double Blind Review pelo SEER/OJS

MODERATING ROLE OF ENTREPRENEURIAL ORIENTATION ON THE RELATIONSHIP BETWEEN INFORMATION SECURITY RISK ASSESSMENT AND FIRM PERFORMANCE IN KENYA

PAPEL MODERADOR DA ORIENTAÇÃO EMPREENDEDORA SOBRE A RELAÇÃO ENTRE A AVALIAÇÃO DO RISCO DA SEGURANÇA DA INFORMAÇÃO E O DESEMPENHO DA EMPRESA NO QUÊNIA

Stanley Ndungu [1]
Kenneth Wanjau [2]
Robert Gichira [3]
Waweru Mwangi [4]

[1]JKUAT – Kenya
E-mail: ndungu867@yahoo.com

[2]Karatina University – Kenya
E-mail: wanjaukenneth@gmail.com

[3]JKUAT – Kenya
E-mail: drogichira@yahoo.com

[4]JKUAT – Kenya
E-mail: waweru_mwangi@icsit.jkuat.ac.ke

ABSTRACT

Information security risk assessments enable SMEs to identify their key information assets and risks in order to develop effective and economically-viable control strategies. In Kenya, SMEs employ about 85 percent of the workforce. The need to link ISRA with firm performance has become vital for firms striving to achieve superior performance. However, limited attention has been paid to the link and more so to the moderating role of EO on ISRA-firm performance relationship model. To better understand this relationship, this paper employed a mixed methods research guided by a cross-sectional research design. Quantitative and qualitative techniques were employed to analyze the collected data using SPSS, Ms-Excel, AMOS, SmartPLS, STATA, R-GUI and ATLAS.ti analytical softwares. Analyses were conducted using a two-phase process consisting of CFA and SEM. The theoretical models and hypotheses were tested based on empirical data gathered from 94 SMEs in the 2013 Top 100 Survey. The study found that ISRA was a significant predictor of firm performance. The results also revealed that entrepreneurial orientation significantly moderated the relationship between ISRA and firm performance in Kenya. This study will enhance the skill set in Kenyan SMEs and produce a more sustainable solution.

Keywords: Information Security Risk Assessment, Risk Assessment Process, SMEs, Information Security Management

RESUMO

Avaliações de risco da segurança da informação possibilitam que as PMEs identifiquem seus principais riscos e ativos de informações, para desenvolver estratégias de controle eficazes e economicamente viáveis. No Quênia, as PMEs empregam cerca de 85% da força de trabalho. A necessidade de conectar a ISRA com o desempenho da empresa tornou-se vital para as empresas empenhadas e que buscam alcançar um desempenho superior. Entretanto, a atenção tem sido limitada para tal conexão e ainda mais para moderar o papel do EO sobre o modelo de relação e desempenho da empresa e da ISRA. Para melhor compreender esta relação, este artigo empregou um método de pesquisa combinado, guiado por um projeto de pesquisa transversal. Técnicas quantitativas e qualitativas foram aplicadas para analisar a coleção de dados, utilizando SPSS, Ms Excel, AMOS, SmartPLS, STATA, R-GUI e ATLAS.ti programas analíticos. As análises foram conduzidas utilizando um processo de duas fases consistindo de CFA e SEM. Os modelos teóricos e as hipóteses foram testadas com base em dados empíricos coletados de 94 PMEs em pesquisa no Top 100 do ano de 2013. O estudo encontrou que a ISRA foi um indicado significante do desempenho da empresa. Os resultados também revelaram que a orientação empresarial moderou significativamente o relacionamento entre a ISRA e o desempenho da empresa no Kenya. Este estudo irá melhorar o conjunto de competências nas PMEs quenianas e produzir uma solução mais sustentável.

Palavras-chave: Avaliação de risco da Segurança da Informação, Processo de Avaliação do Risco, PMEs, Gestão da Segurança da Informação

Received on November 04, 2017
Approved on January 29, 2018

How to Cite (APA)
Ndungu, S., Wanjau, K., Gichira, R. & Mwangi, W. (2018). Moderating role of entrepreneurial orientation on the relationship between information security risk assessment and firm performance in Kenya. *International Journal of Professional Business Review*, 3 (2), 131–152. http://dx.doi.org/10.26668/businessreview/2018.v3i2.60

INTRODUCTION

In this era of fast paced technological advancements, security issues and risks related to it have become a key concern for all organizations (Pramod, Raman, & Bharathi, 2013). This in turn has made information security become an essential entity for organizations across the globe to eliminate the possible risks in their organizations by conducting information security risk assessment (ISRA) (Shamala, Ahmad, Zolait & Sahib, 2015). That is why information security has drawn attention from researchers, professionals, journalists, legislators, governments and citizens. This raises awareness among organizations to invest in information security for decision-making and for the continuance of high-standard business operations (Jourdan, Rainer, Marshall & Ford, 2010). Hence, regardless of being government, private or public organizations, most of them are currently applying a range of security counter measures, policies, procedures and guidelines to protect their organizations.

This awareness is due to the fact that security incidents can lead to severely adverse consequences for organizations, such as a loss in organizational reputation and customer confidence, substantial losses to the industry through the direct loss of information assets and financial impact and a loss of employee productivity or the risk of legal issues (Shedden, Scheepers, Smith & Ahmad, 2011). This results in overall poor performance of the organization. To maintain confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability, the organizations apply ISRA to determine the extent of the potential threats and the risks associated with the information technology (IT) system (Söderström, Åhlfeldt & Eriksson, 2009). An ISRA method identifies the security risks in the organizations and provides a measured, analyzed security risk profile of the critical assets in order to build plans to treat the risks (Shedden et al., 2011).

Thus, ISRAs are performed to allow organizations to assess, identify and modify their overall security posture (Shamala, Ahmad & Yusoff, 2013). ISRAs are also performed to enable security, operations, organizational management and other personnel to collaborate and view the entire organization from an attacker's perspective. This process, Shamala et al further opine, is required to obtain organizational management's commitment to allocate resources and implement the appropriate security solutions.

Saleh and Alfantookh (2011) aver that a comprehensive enterprise security risk assessment also helps determine the value of the various types of data generated and stored across the organization. Without valuing the various types of data in the organization, it is nearly impossible to prioritize and allocate technology resources where they are needed the most. To accurately assess risk, management must identify the data that are most valuable to the organization, the storage mechanisms of said data and their associated vulnerabilities (Dzazali & Zolait, 2012).

Research problem

The Top 100 medium-sized companies (which are essentially SMEs) play a critical role in the development of the Kenya economy (ICPAK, 2015). They have an estimated combined annual turnover of nearly Sh100 billion and the sector accounts for 60% of the country's labor market, Juma (2011) as cited in (Ndung'u, 2014). But due to security incidents, SMEs are facing severe adverse consequences such as loss in organizational reputation and customer

confidence, substantial losses through direct loss of information assets and financial impact, loss of employee productivity, and the risk of legal issues (Shedden et al, 2011), resulting in overall poor performance. This is despite conducting information security risk assessment (ISRA) to eliminate the possible risks in their organizations (Shamala et al, 2015). Top 100 medium-sized firms, and SMEs in general, have the potential to contribute more positively to the Kenyan economy than is currently the case. But to survive in a turbulent and dynamic business environment, they have to formulate and implement their strategy by engaging in entrepreneurial behaviors (Ndung'u, 2014).

One prominent concept of strategy-making in entrepreneurship literature is entrepreneurial orientation (EO) (Schiendel & Hitt, 2007). Therefore it is expected that adopting entrepreneurial orientation may enhance the ISRA-firm performance relationship in SMEs in Kenya, particularly given their resource limitations. There have also been no rich literature available that directly investigate the role of entrepreneurial orientation on the relationship between ISRA and firm performance. Specifically, the impact of ISRA on firm performance is expected to depend on firm's entrepreneurial orientation. This is the rationale for conducting this research. Overall, the research advances technology entrepreneurship anchored on Schumpeterian competition, or more specifically, the theory of creative destruction.

Research objective

The objective of this study is to investigate the effect of entrepreneurial orientation on the relationship between information security risk assessment and firm performance in Kenya.

Research hypothesis

The study hypothesized that;

H1a: There is no positive relationship between information security risk assessment and firm performance in Kenya.

The study also hypothesized that;

H1b: Entrepreneurial orientation does not moderate the influence of information security risk assessment on firm performance in Kenya.

LITERATURE REVIEW

It is widely acknowledged in the security research and practice that the rising number of security breaches over the years has led to the increased security concerns among organizations throughout the world (Shamala, Ahmad, Zolait & Sahib, 2015). Organizations conduct ISRA by identifying their security risks in terms of confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability. ISRA is able to determine the extent of the potential threat and the risk associated with an IT system and provide a measured, analyzed profile of critical assets to develop effective plans to treat the risk (Shedden et al., 2011).

A risk management approach must address at least the following criteria: the criteria for risk assessment, the impact criteria, and the risk acceptance criteria (Pathak, 2005). Besides this, the organization assesses whether it has the necessary resources to perform risk assessment and the development of a risk treatment plan. Also, the organization assesses the definition and implementation of policies and procedures, including the implementation of selected controls for risk treatment, controls monitoring, and risk management process monitoring.

Risk assessment criteria are developed to assess information security risks on the organization, taking into account the strategic value of information processes within the organization, the importance of information assets involved, and the legal requirements and contractual obligations (Amancei, 2011). The criteria also takes into account the organizational and operational importance of the availability, confidentiality and integrity of information. Lastly, the criteria takes into account the expectations and perceptions of shareholders, customers and suppliers of the company and the negative consequences it can have on reputation (Ivan, Noşca & Capisizu, 2005).

Impact criteria are developed and specified as the level of damage caused (Saleh & Alfantookh, 2011). They can also be specified as the cost for organization produced by an event that affected the security of information, taking into account the classification of information assets affected, and the security gap produced (loss of confidentiality, integrity and availability). Taken into account also is the affected operations (internal or external), financial losses, delay in meeting deadlines, and loss of reputation for the organization.

Treatment of risks entails choosing an action or response strategy for each risk analyzed, and presenting it in the plan of risk treatment (Pramod et al., 2013). The treatment options include risk avoidance to eliminate uncertainty by not undertaking the actions regarded as very risky to the business, risk transfer by using risk ownership transfer, or by using insurance, guarantees or contractual clauses, and risk reduction by changing the risk exposure. Another treatment option is risk acceptance which relates to getting approval from top management to accept the current level of risk, without implementing security measures.

Amancei (2011) avers that risk acceptance approach is preferable in the situations where the cost of implementing protective measures exceeds the benefits, or when the level of risk is necessary for business development. Risk acceptance criteria depend on policies, objectives and interests of parties involved in the organization. It is instructive to note that all these treatment options are not unescapably mutually exclusive or suitable in all cases.

Information security risk assessment process is the important prerequisite to achieving scientific and effective risk assessment. To make the ISRA process more systematic and effective, practitioners need to properly define detailed steps in risk assessment planning. Risk assessment process involves a series of tasks broken down by phases where each phase requires information for its success. Many organizations are facing problems in selecting suitable methods that would augur well in meeting their needs (Saleh & Alfantookh, 2011). All in all, information risk management frameworks like COBIT and NIST 800-30 are available with their respective guidelines for conducting the risk assessment and mitigation (Pramod, et al., 2013).

Information security risk assessment process includes preparation of risk assessment, asset identification, threat identification, vulnerability identification, and risk calculation and other stages. It can be divided into six steps in specification operation (Fu & Xiao, 2012). The first step involves determination of assessment object. This step entails defining the information system data, hardware, software assets etc, giving a system function, borders, critical assets and sensitive assets, and determining the scope

of the assessment. In the second step, assessment performance is done. Here, the evaluation plan is developed in accordance with the requirements, assessment process is determined, appropriate assessment methods and tools selected, and the system group is set up (Lee, 2014).

The third step involves risk identification. In this step critical assets and general assets are identified within the scope of assessment. Also, threats in operating environment are identified, including asset vulnerability. Step four is risk analysis. Here, the property of assets are combined, the possibility and consequences of threat used by vulnerability analyzed, and the results of assessment calculated. Also, the analysis of the effectiveness and reasonableness of existing security measures is done. Step five involves risk assessment, where the results are evaluated, and formation of the risk assessment report combined with the expert's opinion is given. Lastly, step six is risk control, which, according to the instructions, require to take effective measures to transfer, avoid or reduce risk, in order to control the system risk effectively (Lee, 2014).

Risks to assets are identified in terms of confidentiality, integrity and availability (Shedden, et al., 2011), and the criticality of each risk is rated according to potential impact and likelihood of occurrence. There are a number of popular Information Security Risk Assessment methodologies in global use in the industries including FRAP, CRAMM, ISRAM, COBRA, OCTAVE, BSI Guide, RuSecure, OCTAVE-S and CORAS, Dhillon (2007) as cited in (Ndung'u, 2014). Although they differ in their make-up, order and depth of activities, they generally follow a three-stage pattern: context establishment, risk identification, and risk analysis. Ndung'u explains that context establishment stage allows for the scoping and focus of the rest of the risk assessment process for maximum effectiveness and to ensure that any risks inherent in the organization's industry or line of business are identified. Risk identification concerns the identification of the threats and vulnerabilities of each of the most critical assets. Risk analysis concerns the determination of probability and impact (the cost of compromising the asset). The integration of the probability and impact will present the level of risk.

It is essential to understand the focus of risk assessment with specific reference to Confidentiality, Integrity or Availability prior to going ahead with risk assessment. The right way to conduct a risk assessment within the scope can be achieved by focusing on risks that are associated with each general control process area (Pramod, et al., 2013). Examples of these include change management, logical access, computer operations, job scheduling and third parties/service organizations that manage applications or data centers.

Methods to reduce risk, Amancei (2011) opines, include implementation of security controls, improving procedures, and changing the environment by reducing exposure to vulnerabilities. Others are implementation of early detection methods to catch the threat when it happens and to reduce potential damage that this may cause, and change continuity plan, to address how the business can continue if a specific threat appears. Lastly, security awareness training sessions where applicable.

Entrepreneurial orientation concept

The last three decades have countersigned the advent of entrepreneurial orientation (EO) as a comprehensively discussed concept in the

management literature (Covin & Lumpkin, 2011). Hundreds of studies exploring the EO concept have been published in a wide variety of scientific journals and presented at top conferences (Wales, Gupta & Mousa, 2011a). Originating in Canada, specifically within a research program at McGill University under the leadership of Pradip Khandwalla and Henry Mintzberg, research on EO is now conducted by scholars around the globe (Basso, Alain & Bouchard, 2009).

Traditionally, EO research has primarily focused on firm-level entrepreneurship (Slevin & Terjesen, 2011). As such, much of the published work investigates the reasons why some firms behave entrepreneurially and the consequences of doing so. Also investigated is the cultural and contextual factors that facilitate or inhibit corporate entrepreneurial behaviors and whether the antecedents and moderating influences differ systematically from conservative firms.

The construct of EO originates from Miller's (1983) work, in which entrepreneurial firms are defined as those that are geared towards innovation in the product-market field by carrying out risky initiatives, and which are the first to develop innovations in a proactive way in an attempt to defeat their competitors (Wójcik-Karpacz, 2016). Miller clarified that EO encompassed a process or a way in which entrepreneurs behave in creating a new firm, a new product or technology, or a new market (Muchiri & McMurray, 2015). Covin and Slevin (1988) proposed that EO should be considered as the strategic dimension which can be observed from the firms' strategic posture running along a continuum from a fully conservative orientation to a completely entrepreneurial one. They suggest that firms with a propensity to engage in relatively high levels of risk-taking, innovations and proactive behaviours, have EO of a high level, while those engaging in relatively low levels of these behaviors have conservative orientation (Covin & Slevin, 1991).

The definition of the concept formulated by Covin and Slevin is the definition which is the base for others to formulate their own ones (Wójcik-Karpacz, 2016). For instance, Tang, Tang, Marino, Zhang and Li (2008) proposed that EO refers to methods, practices and decision-making styles of managers or business owners of the firms which act entrepreneurially. However, Wiklund and Shepherd (2003) opined that EO refers to the strategy-making processes that provide organizations with a basis for entrepreneurial decisions and actions. Lumpkin and Dess (1996) contended that EO refers to the processes, practices and decision-making activities that lead to a new firm, a new product or technology, or a new market They considered EO as a process construct, which is concerned with the methods, practices, and decision-making styles used by the managers (Vij & Bedi, 2012).

Further, Stam and Elfring (2008) describe EO as the simultaneous exhibition of innovativeness, proactiveness and risk taking. But despite the escalating scholarly interest in this area, the issue regarding the dimensionality of EO keep cropping up (Anderson, Kreiser, Kuratko, Hornsby & Eshima, 2015). As originally conceptualized by Miller (1983), EO encompasses a firm's propensity for risk taking, innovation and proactiveness. Later, Lumpkin and Dess (1996) further refined the EO construct, and added the two components of competitive aggressiveness and autonomy. However, it has sometimes been argued that autonomy is an internal organizational driver of entrepreneurship, which influences the

organizational climate for entrepreneurship (Vij & Bedi, 2012). Some researchers also opine that competitive aggressiveness forms a part of the proactiveness dimension and does not represent a separate dimension (Chang & Lin, 2011). EO as multidimensional construct requires all its dimensions to be characterized.

There is widespread agreement amongst researchers that entrepreneurial orientation has three core dimensions: innovativeness, proactiveness and risk-taking (Kroon, Voorde and Timmers, 2013; Hughes and Morgan, 2007; Miller, 1983). Innovativeness is the firm's ability and willingness to support creativity, new ideas and experimentation which may result in new products/services (Lumpkin & Dess, 1996), while proactiveness is the pursuit of opportunities and competitive rivalry in anticipation of future demand to create change and shape the business environment (Lumpkin & Dess, 2001). Relating to risk-taking, it is the firm knowingly devoting resources to projects with chance of high returns but may also entail a possibility of high failure (Lumpkin & Dess, 1996). However, risk-taking is also commonly associated with entrepreneurial behavior and that generally successful entrepreneurs are risk-takers Kuratko and Hodgetts (2001) as cited in (Ndung'u, 2014). Miller (1983) argued that these three components of EO comprised a basic unidimensional strategic orientation.

Theoretical review

Risk management theory suggests that through organizational risk analysis and evaluation, the threats and vulnerabilities regarding information security could be estimated and assessed (Hong, Chi, Chao & Tang, 2003). The evaluation results could be used for planning information security requirements and risk control measures, with the ultimate goal of reducing or minimizing information security risk to an acceptable level in an organization.

Wright (1999) revealed that risk management is a process of establishing and maintaining information security inside an organization. Wright posits that the crux of risk management is risk assessment. In other words, through information security risk assessment, a firm could take appropriate measures to protect information cost-effectively. The interaction of risk assessment and risk control minimizes information security risk to an acceptable level and actualizes the control procedures. The relationships could thus be expressed in the following way: information security = f (risk assessment, risk control, review and modification); risk assessment = f (risk analysis, risk estimation); risk control = f (establishment of control measures, implementation); risk analysis = f (threats, vulnerability); and risk estimate = f (impact, asset appraisal).

This theory is important in this study since it understands and copes with insecure environments. This notwithstanding that the theory ignores security policy and information audit mechanisms and overemphasizes on structures.

Conceptual framework

The key variables in this study were categorized as independent variable, moderator and dependent variable. Mugenda (2008) explains that the independent variables are called predictor variables because they predict the amount of variation that occurs in another variable while dependent variable, also called criterion variable, is a variable that is influenced or changed by another variable. The dependent variable is the variable that the researcher wishes to explain. A moderator variable is a variable that alters the strength of the causal

relationship (Frazier, Tix & Barron, 2004). Figure 1 depicts the hypothesized model.

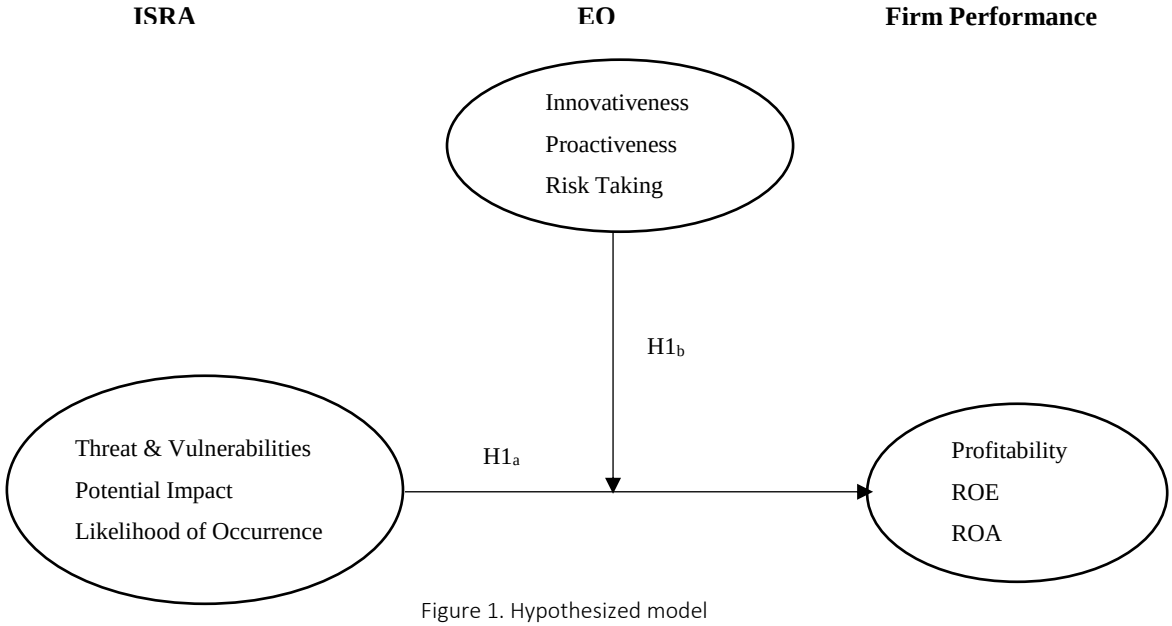

Figure 1. Hypothesized model
Source: Author

Firm performance

Firm performance refers to organizational effectiveness in terms of its financial and operational performance, and a number of indicators are used to measure firm performance (Liang, You & Liu, 2010). These indicators fall into the following general categories: finance, efficiency, customer satisfaction, value addition, and market share. Liang et al. further posits that financial indicators include commonly used measures such as Return on Investment (ROI) or the measure of profitability for a given amount of time, Return on Equity (ROE), Return on Sales (ROS), Return on Assets (ROA) revenue, and sale. These indicators usually can show the firm's capability in making profits.

RESEARCH METHODOLOGY

This study was a mixed methods research guided by cross-sectional survey design. Mixed methods research allows a researcher to combine elements of qualitative and quantitative research approaches (Johnson, Onwuegbuzie & Turner, 2007). The use of mixed methods research allows the researcher to compensate for the weakness of one single approach with the strengths of the other in order to achieve the best results (Cresswell & Clark, 2011). Cross-sectional survey design, on the other hand, helps with hypothesis formulation and testing the analysis of the relationship between variables (Kothari, 2004). Therefore this design was appropriate for this study which extensively tested the analysis of the relationships between variables.

The target population was made up of the small and medium enterprises in Kenya while the accessible population consisted of the small and medium enterprises that participated in the 2013 Top 100 Survey. The respondents were the Information Technology managers of these firms. These managers were considered to be internal champions. Their primary motivation tended to be entrepreneurial performance.

Profit opportunity, entrepreneurial leadership, and the passion and drive of individual employees were factors that motivated them to behave entrepreneurially. They guide or drive how entrepreneurial activities will be manifested in innovation processes within the firms. They are versed with technology-push approach. The sampling frame consisted of the small and medium enterprises in the services and manufacturing sectors in Kenya that had been registered with KPMG for the Top 100 Survey.

Israel (2012) posits that although cost considerations make census technique impossible for large populations, a census is attractive for small populations of 200 or less. Since the accessible population consisted of 100 respondents, this study used the entire population as the sample. The study used a self-administered, semi-structured questionnaire to obtain primary data. Consequently 94 SMEs (53 Services and 41 Manufacturing SMEs) out of 100 responded.

For pilot testing, data from 10 respondents were collected, representing 10% of the population in the study. Cronbach's Alpha statistic ranged from 0.8 to 0.9, indicating high reliability of data. Mertens (2010) avers that the closer the coefficient is to 1.0, the more reliable the measurements. This study adopted construct validity. Mertens advises that factor analysis can be used to validate hypothetical constructs as it attempts to cluster items or characteristics that seem to correlate highly with each other in defining a particular construct.

Eigen values criterion was used to determine the selection of factor loadings for each component. The larger the eigen value loading, the more important the associated principal component (Graham & Midgley, 2000). In this case, the varimax with Kaiser Normalization sampling adequacy with eigen value greater than 1 were used as the rotation method because the items were uncorrelated. Montgomery, Peck and Vining (2001) recommend that a minimum factor loading of 0.40 should be used when factor analysis is used to refine construct validity. All items had factor loadings ranging from 0.408 to 0.990.

IBM Statistical Package for the Social Sciences (SPSS) version 21.0 for Windows 7 and Windows 8 was used for data entry, data cleaning and running the Exploratory Factor Analysis (EFA). Other software applications used were Ms-Excel for Windows 8 for case cleaning, variable screening and as a transit package in that the data from SPSS was saved in Ms-Excel for it to be exported to SmartPLS; Analysis of Moment Structures (AMOS) version 18, which is essentially analysis of mean and co-variance structures, for Initial EFA, Confirmatory Factor Analysis (CFA), Path Analysis and Structural Equation Modeling (SEM); SmartPLS version 2.0 for Path Analysis, SEM with moderation and model diagnostics; STATA version 12.0 for normality testing; R-GUI version 2.10.0 for building plots, for instance box-plots using the Ggplot2 package, and for univariate and multivariate testing of outliers in the dependent variable; and ATLAS.ti for qualitative analysis.

ANALYSIS OF ISRA AMONGST TOP 100 MEDIUM-SIZED FIRMS

Information security risk assessment was operationalized into threats and vulnerabilities, potential impact and likelihood of occurrence. When asked whether risk assessment in their firms determine what consequences would be if the infrastructure became inoperable, majority (95.7%) of the respondents answered in the affirmative while a few (4.3%) said no, as shown in Table 1.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	4	4.3	4.3	4.3
	Yes	90	95.7	95.7	100.0
	Total	94	100.0	100.0	

Table 1 Consequences if infrastructure became inoperable
Source: Author

Absence of a risk assessment process or one that is inadequate, can lead to severe adverse consequences for firms, inter alia, reputation, legal issues or financial loss (Shedden, Scheepers, Smith & Ahmad, 2011). These are the same consequences that would be met if the infrastructure became inoperable. If this happens, many medium-sized firms would experience low entrepreneurial intensity levels, culminating into closure.

On whether risk assessment in their organizations considered what information assets were subject to laws and regulations and whether the assessment results were adequate in procedure to assure compliance, majority (89.4%) answered in the affirmative while a few (10.6%) said no, as shown in Table 2.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	10	10.6	10.6	10.6
	Yes	84	89.4	89.4	100.0
	Total	94	100.0	100.0	

Table 2. Risk assessment and information assets subject to laws and regulations
Source: Author

Being a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security program (ITGI, 2006), information security governance would guide firms on what information assets were subject to laws and regulations.

Information security governance could help in making certain that organizations are complying with not only applicable laws and regulations, but also codes of practice (von Solms, 2005). This makes it easy for medium-sized firms to adopt best practices as a way of enhancing strategic entrepreneurship. Hitt, Ireland, Camp and Sexton (2001) in their study on Guest Editors' Introduction to the Special Issue Strategic Entrepreneurship: Entrepreneurial Strategies for Wealth Creation, urged firms to have a strategic perspective in their operational processes. Lumpkin and Dess (1996) examined the management processes resulting in entrepreneurial activity, and identified the underlying elements which influenced and enhanced such action. In particular, they introduced the notion of entrepreneurial orientation as a specific concept at the connection between strategy and entrepreneurship and presented this as the right approach.

On whether medium-sized firms made security and risk assessment part of the way they do business, majority (93.6%) answered in the affirmative, a few (5.3%) said no while 1.1% did not respond, as shown in Table 3.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	5	5.3	5.4	5.4
	Yes	88	93.6	94.6	100.0
	Total	93	98.9	100.0	
Missing	System	1	1.1		
Total		94	100.0		

Table 3. Security and risk assessment part of the way business is done
Source: Author

Information security should not be regarded as a technical issue, but a business and governance challenge that involves adequate risk management, reporting, and accountability (Abu-Musa, 2010). It seems medium-sized firms were leading in this going by the high percentage of affirmative respondents. This finding contradicts an earlier one by Dojkovski, Lichtenstein and Warren (2007) who pointed out that SMEs generally have a weak understanding of information security, security technologies and control measures, and neglect to carry out risk assessment. Top 100 medium-sized firms in Kenya should make security and risk assessment part of the way they do business. This in itself is an entrepreneurial activity with a strategic perspective. This undoubtedly refers to strategic entrepreneurship which involves simultaneous opportunity-seeking and advantage-seeking behaviors (entrepreneurial orientation and strategic orientation respectively) and results in superior firm performance (Ireland et al., 2003).

Measurement of threats & vulnerabilities factor amongst Top 100 Medium-sized firms

Threats and vulnerabilities factor was measured using the Likert scale and the results, expressed as percentages, tabulated in Table 4.

Threats and Vulnerabilities Factors		SD	D	N	A	SA	Mean	Std.Dev
RSR1	%	1.1	0.0	0.0	72.3	26.6	4.23	0.557
RSR2	%	1.1	0.0	2.1	71.3	25.5	4.20	0.579
RSR3	%	1.1	1.1	11.7	62.8	23.4	4.06	0.700

Table 4 Response to threats and vulnerabilities
Source: Author

The results showed that majority (98.9%) of the respondents agreed to the opinion that their organization had in place an adequate risk assessment process and a few (1.1%) disagreed. Shedden et al. (2011) states that an inadequate risk assessment process could lead to severe

adverse consequences for organizations including financial losses. Resources, including financial capital, are the basis of firm differential performances in terms of wealth creation. The response was one of the highest indicating the severity of non-conformance.

On whether their organizations employed one of the popular ISRA methodologies, majority (96.8%) of the respondents agreed to the opinion, a few (1.1%) disagreed while 2.1% remained neutral. Dhillon (2007), posited that irrespective of the methodology employed by a firm, they generally start with context establishment, followed by risk identification and finally risk analysis. Dhillon in his study had identified a number of methodologies including CRAMM. On whether their staff were trained towards mitigating threats and vulnerabilities, majority (86.2%) of the respondents agreed, a few (2.2%) disagreed while 11.7% remained neutral. Al-Awadi (2009) emphasized that training enhances implementation of information security and make the implementation of security easier. Due to the dynamic nature of information technology training should be carried out in a continuous process in all firms. This is likely to raise the degree of entrepreneurship, leading to superior performance of medium-sized firms.

Measurement of Potential Impact Factor Amongst Top 100 Medium-sized Firms

Potential impact factor was measured using the Likert scale and the results tabulated in Table 5.

Potential Impact							
Factors	SD	D	N	A	SA	Mean	Std.Dev
RSR4 %	1.1	0.0	9.6	70.2	19.1	4.06	0.619
RSR5 %	1.1	0.0	6.4	73.4	19.1	4.10	0.588

Table 5. Response to potential impact
Source: Author

The results showed that majority (89.3%) of the respondents agreed to the opinion that their firms rated each risk according to potential impact, a few (1.1%) disagreed while 9.6% remained neutral. Rating of potential impact starts with the firm's most critical information assets followed by the identification of the threats and vulnerabilities of each of these assets (Visintine, 2003).

On whether risk assessment in their firms covered the consequences of a security incident in terms of lost revenues, lost customers and investor confidence, majority (92.5%) of the respondents agreed, a few (1.1%) disagreed while 6.4% were neutral. Shedden et al (2011) emphasized on this, and stated that any assessment falling short of this would be inadequate. Inadequate risk assessment could lead to severe adverse consequences for organizations including financial losses. The same consequences would be faced if firms failed to rate each risk according to potential impact. At this point no new innovative ideas would be forthcoming and the firm is likely to face closure.

Measurement of likelihood of occurrence factor amongst Top 100 Medium-sized firms

Likelihood of occurrence factor was measured using the Likert scale and the results tabulated in Table 6.

Likelihood of Occurrence Factors		SD	D	N	A	SA	Mean	Std. Dev.
RSR6	%	1.1	2.1	12.8	70.2	13.8	3.94	0.669
RSR7	%	3.2	2.1	3.2	78.7	12.8	3.96	0.732

Table 6. Response to likelihood of occurrence
Source: Author

The results showed that majority (84.0%) of the respondents agreed to the opinion that risk assessment in their firms considered whether the entity could continue to operate if critical information became unavailable, compromised or lost, a few (3.2%) disagreed while 12.8% remained neutral. Absence of some critical information would ground operations of a firm to a halt, and so it is incumbent upon the firms to rate and identify the information in question.

On whether their organization rated each risk according to likelihood of occurrence, majority (91.5%) of the respondents agreed, a few (5.3%) disagreed while 3.2% remained neutral. Likelihood of occurrence being one way of rating the criticality of risks is an indication that risks to organizational assets are organized and then prioritized according to criticality for whatever further action (Alberts & Dorofee, 2004). Likelihood of occurrence should be mitigated by carrying out satisfactory information security risk assessment. Repeated occurrences would disrupt creativity and innovation in a firm. When this happens, entrepreneurial intensity levels decrease resulting into firm closure. Same consequences would be suffered if critical information became unavailable in the firm.

DATA ANALYSIS AND RESULTS

The main objective here was to provide results of the analyses, interpretation of the results and findings. Several steps were undertaken towards ensuring building of a good quantitative model, as well as key general guidelines for structuring a quantitative model. As a general approach, the analysis of the descriptive data were presented as the first step to understanding the data structure. This was followed by univariate analysis, necessary for uncovering the one-on-one relationship. Factors which were significant univariately were further subjected to a rigorous multivariate analysis, and the steps carried out in a hierarchical manner.

Case screening was undertaken through the examination of the missing data by running the cases counts in excel, using the standard deviations to access the level of engagement of the respondents. The few records with missing cases were dropped. The variables with missing data were mainly in the section where the respondents were required to indicate the average growth for indicators of performance in their firms: average pre-tax profits, Return on Equity, Return on Assets, employment growth and sales turnover from year 2010 to 2012. The respondents in question found the section sensitive.

Variable screening was also done. In this case the missing data was generated using central

tendencies where the most appropriate central tendency measure was adopted. For the cases, median was adopted as it is least affected by the outliers. It is instructive to note that missing data can pose a serious modeling challenge, more so with SEM. For the Likert scales, median was the appropriate statistics to use while with the continuous variates the mean was appropriate. To ensure that there was no violation of the assumptions, this study tested for outliers, normality, linearity, homoscedasticity, multicollinearity, non-response bias and common method variance. The results of the tests conformed to the respective thresholds for each test.

In general, analyses were conducted using a two-phase process consisting of confirmatory measurement model and confirmatory structural model. This is in line with the two-phase process suggested by Anderson and Gerbing (1988). The first phase involved confirmatory factor analysis (CFA) that evaluates the measurement model on multiple criteria such as internal reliability, convergent, and discriminant validity. Prior to this was the exploratory factor analysis (EFA) whose key steps included the computation of pattern matrix, communalities and principal components analysis (PCA). EFA is used when you have a large set of variables that you want to describe in simpler terms and you have no a priori ideas about which variables will cluster together (Tabachnick & Fidell, 2013), thus necessitating carrying out of the analysis at the early stages of the research (Bordens & Abbot, 2014).

EFA is preceded by two statistical tests: Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's Test of Sphericity. These tests were conducted to confirm whether there was a significant correlation among the variables to warrant the application of EFA (Snedecor & Cochran, 1989). The KMO statistics vary between 0 and 1 (Argyrous, 2005). A value of zero indicates that the sum of partial correlation is large relative to the sum of correlations indicating diffusions in the patterns of correlations, and hence that factor analysis likely to be inappropriate (Costello & Osborne, 2005).

A value close to 1 indicates that the patterns of correlations are relatively compact and so factor analysis should yield distinct and reliable factors (Cooper & Schindler, 2011). Bartlett's Test of Sphericity tests the hypothesis that one's correlation matrix is an identity matrix, which would indicate that the variables are unrelated and therefore unsuitable for structure detection. Small values ($p < 0.05$) of the significance level indicate that a factor analysis may be useful with one's data. The results of the two tests are shown in Table 7, with indications of appropriateness of application of EFA.

KMO Measure of Sampling Adequacy	**Bartlett's Test of Sphericity**	
0.871	Approx. Chi-Square	3349.637
	df	528
	Sig.	***0.000***

Table 7. Results of the test for suitability of structure detection
Source: Author

The second phase involved latent variables structural equation modeling (SEM) to test the hypothesized relationships and to fit the structural model. Normality test on the factors produced Skewness values between -1 and +1. The outliers were tested for each of the

observations, with observations farthest from the centroid, Mahalanobis distance, being taken into consideration. There were no outliers detected. The values obtained in testing the model fit indices were within the thresholds as shown in Table 8.

Model	CFI	GFI	AGFI	RMSEA
Default model	.993	.978	.916	.050
Saturated model	1.000	1.000		
Independence model	0.000	.673	.509	.412

Table 7. Results of the test for suitability of structure detection
Source: Author

The structural equation modeling (SEM) for the study objective was as shown in Figure 2, showing there was a positive relationship (regression weight = 3.77) between information security risk assessment and firm performance. Therefore, H1a was rejected. The significance test result for the hypothesis is shown in Figure 3. Therefore this model was statistically significant at 95% significant level with t=3.224.

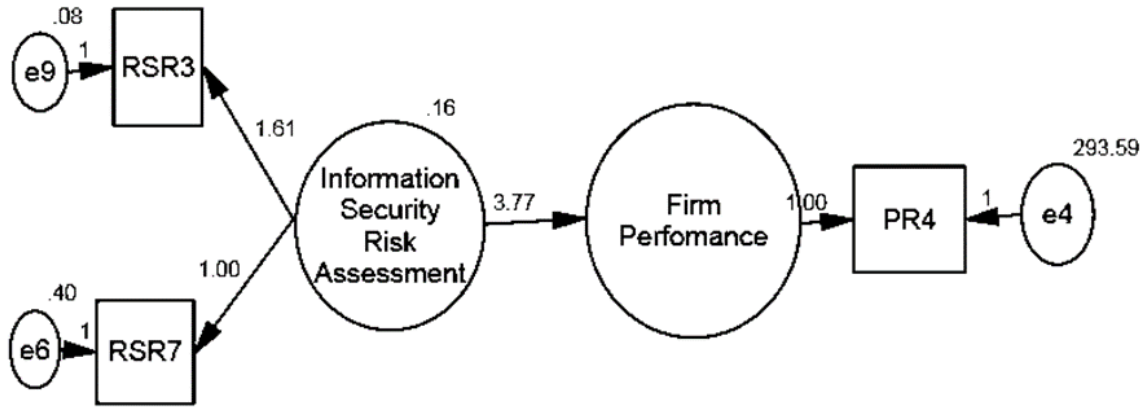

Figure 2. SEM for the objective
Source: Author

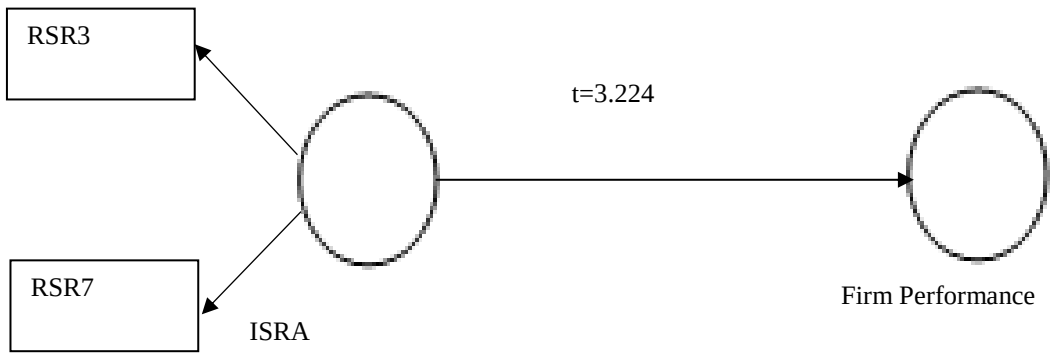

Figure 3. Significance test result for effect of ISRA on firm performance
Source: Author

Structural Equation Modeling (SEM) with moderation was carried out. Prior to moderation, a bootstrapping procedure (Hesterberg, 2003) to evaluate the statistical significance of path coefficient was carried out, resulting in the initial model in Figure 4. The t-statistics indicate that Information Security Risk Assessment (ISRA) was significant at 10% α level (t-statistics > 0.842). This finding was corroborated during the testing of the hypothesized relationships, where the factor was found to be statistically significant.

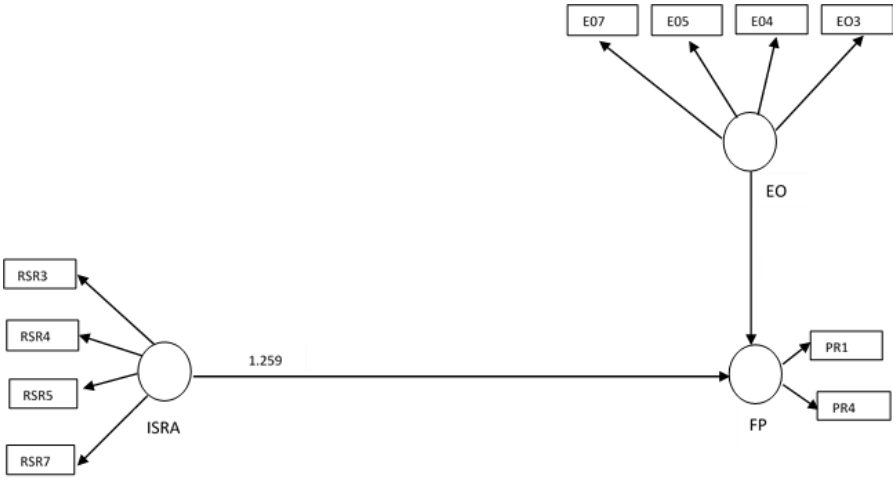

Figure 4. Weights initial model with bootstrapping
Source: Author

First Order Construct using the t-statistics through bootstrapping produced insignificant interaction, that is, ISRA*EO, which had t<0.842 (Fisher, 1926) at 10% α level. The next step involved testing the significance for the synergies of the factors at a higher level. This was done at second order level, where ISRA was combined with Information Technology Competence (ITC) factor to form Technical factor. When run with the interaction term, the Technical*EO interaction was statistically significant at 10% α level. This is shown in Figure 5.

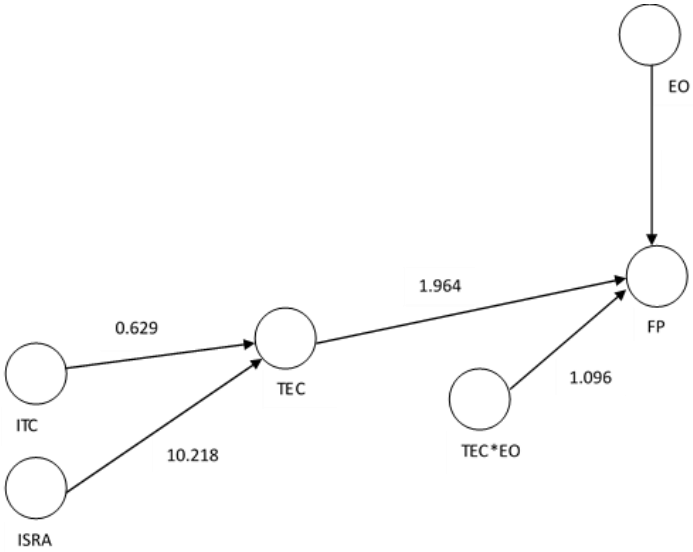

Figure 5. Second order SEM with moderation
Source: Author

DISCUSSION AND CONCLUSION

ISRAs are important for organisations as they are the means by which critical information assets are identified, their threats and vulnerabilities assessed and a level of risk assigned and prioritized for future action. ISRA methodologies, however, mostly adopt an asset-based focus. In this study, information security risk assessment had a relationship with performance of medium-sized firms and all the three factors of information security risk assessment, namely threats and vulnerabilities, potential impact and likelihood of occurrence contributed significantly to the effect of information security risk assessment on performance of medium-sized firms in Kenya. Thus the hypothesis that there is no relationship between information security risk assessment and firm performance in Kenya was rejected. This is in line with the findings of Gerber and von Solms (2005). In their study on Management of Risk in the Information Age, they identified information security risk assessment as one of the success factors in information security management leading to firm performance.

Information Security Risk Assessment also had a statistically significant influence on performance of top 100 medium-sized firms in Kenya. Hong, Chi, Chao and Tang (2003) in their study on An Integrated System Theory of Information Security Management, identified Information Security Risk Assessment as one of the success factors of information security management. In line with this, risk management theory suggests that through organizational risk analysis and evaluation, the threats and vulnerabilities regarding information security could be estimated and assessed, and the evaluation results used for planning information security requirements and risk control measures, with the ultimate goal of reducing or minimizing information security risk to an acceptable level in an organization. In this regard, through information security risk assessment a medium-sized firm could take appropriate measures to protect information cost-effectively, in turn leading to better performance. In light of this it can be concluded that information security risk assessment is a cornerstone of information security management implementation that could lead to superior performance of the top 100 medium-sized firms.

At second order structural equation modeling with moderation, the synergy between the technical factors, that is, information technology competence and information security risk assessment produced significant interaction. This is insightful considering that this study is advancing technological entrepreneurship. The top 100 medium-sized firms advancing technology entrepreneurship should adopt entrepreneurial orientation philosophy for superior performance. Undoubtedly, the interplay of information technology competence and information security risk assessment as moderated by entrepreneurial orientation could be said to be the face of technological entrepreneurship.

The decision to act entrepreneurially occurs as a result of interactions among organizational characteristics, individual characteristics, and some kind of precipitating event (Morris, Kuratko & Covin, 2008). Competition which is considered as an external trigger has made Top 100 medium sized firms in Kenya behave entrepreneurially. They have embraced EO to cope with a dynamic, threatening, and complex external environment. The external environment and considerations

within these organizations has made the owners/managers to respond creatively and act in innovative ways. This entrepreneurial behavior is well described by the Schumpeterian theory. It should also be noted that, Top 100 medium sized firms have planned programmes for innovation regardless of what is happening in the external environment at a given point in time, or they have created an entrepreneurial culture which allows initiation of open innovation. Thus Risks to assets are identified in terms of confidentiality, integrity and availability (Shedden, Scheepers, Smith & Ahmad, 2011), and the criticality of each risk is an important internal trigger that can only take place in an entrepreneurial culture.

This study also fills the gaps identified at the literature review stage where it was revealed that limited attention has been paid to the effect of entrepreneurial orientation on the relationship between information security management and firm performance. Moreover, the few studies that have been done on the area of information security risk assessment fail to relate information security risk assessment on firm performance. This study therefore has added value to existing literature by providing empirical information security risk assessment measures that small and medium enterprises in Kenya can adopt in order to improve on their performance. The ability to encourage entrepreneurship on an ongoing basis requires that owners/managers first identify the types of triggers that are prevalent in the firm, and determine if any key triggers are not occurring for particular reasons.

Lastly, the findings presented in this study are based on evidence gathered from SMEs that participated in the 2013 Top 100 Survey. Future research should be extended to financial institutions whose allure to cyber criminals are the millions of financial transactions carried out every day.

REFERENCES

Alberts, C. J., & Dorofee, A. J. (2004). Rethinking Risk Management. Pittsburgh, PA: SEI

Abu-Musa, A. A. (2010). Information security governance in Saudi organizations: an empirical study. Information Management & Computer Security, 18(4), 226-276.

Al-Awadi, M., A. (2009). A study of Employees' Attitudes Towards Organisational Information Security Policies in the UK and Oman. (Published Doctoral dissertation, University of Glasgow). Retrieved from http://theses.gla.ac.uk/860/.

Amancei, C. (2011). Practical Methods for Information Security Risk Management. Informatica Economică. 15(1), 151-159.

Anderson, B. S., Kreiser P. M., Kuratko, D. F., Hornsby, J. S., & Eshima Y. (2015). Reconceptualizing entrepreneurial orientation. Strategic Management Journal, 36, 1579-1596.

Anderson, J. C. & Gerbing, D. W. (1988). Structural equation modeling in practice: a review and recommended two-step approach. Psychological Bulletin, 103(3), 411-423.

Argyrous, G. (2005). Statistics for research: With a guide to SPSS. London: Sage

Basso, O., Alain, F., & Bouchard, V. (2009). Entrepreneurial orientation: The making of a concept. International Journal of Entrepreneurship and Innovation, 10(4), 313-321.

Bordens, K. S., & Abbott, B. B. (2014). Research design and methods: A process approach (9th ed.). San Francisco: McGraw Hill.

Chang, H. J., & Lin, S. J. (2011), Entrepreneurial intensity in catering industry: A case study on Wang Group in Taiwan. Business and Management Review, 1(9), 1-12.

Cooper, D. R., & Schindler, P. S. (2011). Business Research Methods. (11th ed.). New York: McGraw-Hill.

Covin, J. G., & Lumpkin, G. T. (2011). Entrepreneurial orientation theory and research: Reflections on a needed construct. Entrepreneurship Theory and Practice, 35(5), 855-872.

Covin, J. G., & Slevin, D. P. (1988). The influence of organization structure on the utility of an entrepreneurial top management style. Journal of Management Studies, 25(3), 217-234.

Covin, J. G., & Slevin, D. P. (1991). A conceptual model of entrepreneurship as firm behavior. Entrepreneurship Theory & Practice, 15(1), 7-24.

Cresswell, J. W., & Clark, V. L. P. (2011). Designing and conducting mixed methods research. Los Angeles: Sage.

Dhillon, G. (2007). Principles of Information Systems Security: Text and Cases. Hoboken, NJ: Wiley.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007). Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia. 15th European Conference on Information Systems (pp. 1560-1571). St. Gallen, Switzerland.

Dzazali, S., & Zolait, A. H. (2012). Assessment of information security maturity. Journal ofSystems and Information Technology, 14(1), 23-57.

Frazier, P. A., Tix, A. P. & Barron, K. E. (2004). Testing moderator and mediator effects in counseling psychology research. Journal of Counseling Psychology, 51(2), 115-134.

Fu S., & Xiao, Y. (2012). Strengthening the research for Information security risk assessment. International Conference on Biological and Biomedical Science Advanced in Biomedical Engineering, 9, 386-392.

Gerber, M., & von Solms, R. (2005). Management of risk in the information age. Computers & Security 24, 16-30.

Graham, D. J. & Midgley, N. G. (2000). Graphical representation of particle shape using triangular diagrams: an Excel spreadsheet method. Earth Surface Processes and Landforms, 25(13), 1473-1477.

Hesterberg, T. (2003). Bootstrap methods and permutation tests. New York: W. H. Freeman and Company.

Hitt, M., Ireland, R., Camp, S. & Sexton, D. (2001). Guest editors' introduction to the special issue strategic entrepreneurship: entrepreneurial strategies for wealth creation. Strategic Management Journal, 22, 479-491.

Hong, K., Chi, Y., Chao, L. R. & Tang, J. (2003). An integrated system theory of information security management. Journal of information management & computer security, 11(5), 243-248.

Hughes, M. & Morgan, R. E. (2007). Deconstructing the relationship between entrepreneurial orientation and business performance at the embryonic stage of firm growth. Industrial Marketing Management, 36, 651-661.

Information Technology Governance Institute (ITGI) (2006). Information Security Governance, Guidance for Boards of Directors and Executive Management (2nd ed.). Rolling Meadows, IL: IT Governance Institute.

Institute of Certified Public Accountants of Kenya (ICPAK) (2015, 11 05). Top 100 Mid-sized Companies - What Top 100 is all about. Retrieved 12 07, 2016, from ICPAK: https://www.icpak.com/top-100-mid-sized-companies-what-top-100-is-all-about/

Ireland, R. D., Hitt, M. A., & Sirmon, D. G. (2003). A model of strategic entrepreneurship: the construct and its dimensions. Journal of Management 29(6), 963-989.

Israel, G. D. (2012, 06 12). Sampling: Determining sample size. Retrieved 05 13, 2013, from University of Florida IFAS Extension: http://edis.ifas.ufl.edu/pd006

Ivan, I., Noşca, G., & Capisizu, S. (2005). Auditul sistemelor informatice. Bucureşti: Editura ASE.

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of mixed methods research. Journal of mixed methods research, 1(2), 112-133.

Jourdan, Z., Rainer, R. K., Marshall, T. E. & Ford, F. N. (2010). An investigation of organizational information security risk analysis. Journal of Service Science, 3(2), 33-42.

Kothari, C. R. (2009). Research Methodology: Methods and Techniques (5th ed.). New Delhi: New Age International.

Kroon, B., Voorde, K., & Timmers, J. (2013). High performance work practices in small firms: a resource-poverty and strategic decision-making perspective. Small Business Economics, 41(1), 71-91.

Kuratko, D. F., & Hodgetts, R. M. (2001). Entrepreneurship: A Contemporary Approach. Texas: Harcourt College Publishers.

Lee, M. (2014). Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method. International Journal of Computer Science & Information Technology (IJCSIT), 6(1), 29-45.

Liang, T., You, J., & Liu, C. (2010). A resource-based perspective on information technology and firm performance: a meta-analysis. Industrial Management & Data Systems, 110(8), 1138-1158.

Lumpkin, G.T. & Dess, G.G. (1996). Clarifying the entrepreneurial orientation construct and linking it to performance. Academy of Management Review, 21(1), 135-172.

Lumpkin, G. T, & Dess, G. (2001). Linking two dimensions of entrepreneurial orientation to firm performance: The moderating role of environment and industry life cycle. Journal of Business Venturing, 16(5), 429-451.

Mertens, D. M. (2010). Research & Evaluation in Education and Psychology: Integrating

Diversity with Quantitative, Qualitative & Mixed Methods. London: Sage Publications.

Miller, D. (1983). The Correlates of Entrepreneurship in three Types of Firms. Management Science. 29(7), 770-791.

Montgomery, D. C., Peck, E. A., & Vining, G. G. (2001). Introduction to Linear Regression Analysis (3rd ed.). New York: John Wiley.

Morris, M. H., Kuratko, D. F., & Covin, J. G. (2008). Corporate entrepreneurship and innovation. Cincinnati, OH: Thomson/SouthWestern Publishers.

Muchiri, M., & McMurray, A. (2015). Entrepreneurial orientation within small firms: A critical review of why leadership and contextual factors matter. Small Enterprise Research, 2(1), 17-31.

Mugenda, A. (2008). Social Science Research: Conception, Methodology and Analysis. Nairobi: Kenya Applied Research and Training Services.

Ndung'u, S. I. (2014). Moderating role of entrepreneurial orientation on the relationship between information security management and firm performance in Kenya. (Unpublished doctoral dissertation, Jomo Kenyatta University of Agriculture & Technology). Retrieved from http://ir.jkuat.ac.ke/handle/123456789/1577.

Ndung'u, S. I., Wanjau, K. L., Gichira, R., & Mwangi, W. (2014). Moderating Effect of Entrepreneurial Orientation on the Relationship between Human-Related Information Security Issues and Firm Performance in Kenya. Asian Academic Research Journal of Social Sciences & Humanities, 1(26), 311-334.

Pathak, J. (2005). Information Technology Auditing: An Evolving Agenda. Berlin: Editura Springer.

Pramod, D., Raman, R., & Bharathi, S. V. (2013). An Aspect Oriented Process Based Approach to Information Risk Management. International Journal of Engineering and Technology (IJET), 5(3), 2262-2267.

Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. Applied Computing and Informatics, King Saud University, 9(2), 107-118.

Schiendel, D. E., & Hitt, M. A. (2007). Issues in Strategic Entrepreneurship. Strategic Entrepreneurship Journal, 9(3), 425-453.

Schumpeter, J. A. (1942). Capitalism, Socialism and Democracy. New York: Harper & Bros.

Shamala, P., Ahmad, R. & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). Journal of Information Security and Applications, Elsevier Ltd, 18(1), 45-52.

Shamala, P., Ahmad, R., Zolait, H. A., & Sahib, S. (2015). Collective information structure model for Information Security Risk Assessment (ISRA). Journal of Systems and Information Technology, 17(2), 193-219.

Shedden, P., Scheepers, R., Smith, W., & Ahmad, A. (2011). Incorporating a knowledge perspective into security risk assessments. Journal of Information and Knowledge Management Systems, 41(2), 152-166.

Slevin, D. P., & Terjesen, S. A. (2011). Entrepreneurial orientation: Reviewing three papers and implications for further theoretical and methodological development. Entrepreneurship Theory and Practice, 35(5), 973-987.

Snedecor, G. W. & Cochran, W. G. (1989). Statistical methods (8th ed.). Ames, Iowa: Iowa State University Press.

Söderström, E., Åhlfeldt, R., & Eriksson, N. (2009). Standards for information security and processes in healthcare. Journal of Systems and Information Technology, 11(3), 295-308.

Stam, W., & Elfring, T. (2008). Entrepreneurial orientation and new venture performance: The moderating role of intra- and extra-industry social capital. Academy of Management Journal, 51(1), 97–111.

Tabachnick, B. G., & Fidell, L. S. (2013). Using multivariate statistics. (6th ed.). Boston: Pearson.

Tang, J., Tang, Z., Marino, L. D., Zhang, Y., & Li, Q. (2008). Exploring an inverted U-shape relationship between entrepreneurial orientation and performance in Chinese ventures. Entrepreneurship Theory and Practice, 32(1), 219-239.

Vij S., & Bedi H. S. (2012). Relationship between entrepreneurial orientation and business performance: A review of literature, Journal of Business Strategy, 9(3), 17-31.

Visintine, V. (2003). An Introduction to Information Risk Assessment. Denver, CO: SANS Institute.

von Solms, S. H. (2005). Information security governance compliance management vs operational management. Computers & Security, 24, 443-447.

Wales, W., Gupta, V. K., & Mousa, F. (2011a). Empirical research on entrepreneurial orientation: An assessment and suggestions for future research. International Small Business Journal, 31(4), 357-383.

Wiklund, J. & Shepherd, D. (2003). Knowledge-based resources, entrepreneurial orientation, and the performance of small and medium sized businesses. Strategic Management Journal, 24, 1307–1314.

Wójcik-Karpacz, A. (2016). The Researchers' Proposals: What is the Entrepreneurial Orientation? Managing Innovation and Diversity in Knowledge Society Through Turbulent Time (pp. 247-255). Timisoara, Romania: TIIM.

Wright, M. (1999). Third generation risk management practices. Computers and Security, 1999(2), 9-12.