The Strategic JOURNAL of Business & Change MANAGEMENT
ISSN 2312-9492 (Online), ISSN 2414-8970 (Print)
www.strategicjournals.com
Volume 3, Issue 4, Article 11

EFFECT OF STRATEGIC SECURITY MANAGEMENT PRACTICES ON FIRM PERFORMANCE: A CASE OF KENYA REVENUE AUTHORITY

PETER MURITHI MOFFAT, DR. JOYCE NZULWA (PH.D)

The Strategic JOURNAL of Business & Change MANAGEMENT
ISSN: 2312-9492 www.strategicjournals.com

Vol. 3, Iss. 4 (11), pp 201-218, Sept 29, 2016, www.strategicjournals.com, ©strategic Journals

EFFECT OF STRATEGIC SECURITY MANAGEMENT PRACTICES ON FIRM PERFORMANCE: A CASE OF KENYA REVENUE AUTHORITY

[1]Peter Murithi Moffat, [2]Dr. Joyce Nzulwa (Ph.D)

[1]Jomo Kenyatta University of Agriculture & Technology (JKUAT), Kenya
[2]Jomo Kenyatta University of Agriculture & Technology (JKUAT), Kenya

Accepted September 29, 2016

ABSTRACT

Over the past one century, the debates surrounding the issues of security have gained momentum tremendously. The general objective of this research was to establish the effect of strategic security management practices on the firm's performance. The goal of this study was to address the gaps in the literature and develop an understanding of how strategic security management in an organization drives firm performance. Three gaps had been identified. The areas of physical security and other forms of security had not been focused which became important with the increase in threat of terrorism. Lastly, there was a dearth of studies that incorporated security management as a strategic focus. This study was a descriptive cross-sectional survey. This study was carried out in Nairobi. The study population was 92 employees in the security department of Kenya Revenue Authority (KRA), Nairobi. The sampling frame that was applied in this study was a list of employees in the security department of KRA. This study was a census where all target respondents in the population participated in the study. Questionnaire was utilized as data collection instrument in the study. Analysis was through both descriptive and inferential statistics. Descriptive statistics used were frequencies, percentages and mean scores. Inferential statistics were correlation and regression analysis. The results established that security of ICT infrastructure, leadership coordination in security management and security of employee working conditions at KRA significantly influenced performance of the organization. The results however established that employee participation in security management did not have a significant influence on performance of KRA. From the study findings, the study recommended that, first, KRA should put in place reward systems where there are punishments and deterrents for observance of ICT security policies and strategy. Secondly, top leadership of KRA should be involved in leading security management and also in designing and implementing security strategy and policies in the organization. Third, employees should be always orientated on security management when they are recruited to ensure that they understand security issues and help in implementing the security strategy. Lastly, KRA should have a clear plan and log of the physical and ICT infrastructure in place and ensure that the infrastructure in place is functional at all times to enhance service delivery to employees and customers.

***Key Words**: ICT infrastructure, employee participation, employee working conditions*

INTRODUCTION

Security is an issue of concern for organizations at all levels and that organizations, whether small, medium or large, sole proprietorship, partnership or company, security remains a priority (Anderson, 2011). For companies to survive and remain competitive in the contemporary turbulent environment, management of security has to be done efficiently (Ndung'u, 2014). Despite the rapid changes and enhancements of security management practices, a number of firms still rely on old systems to manage their security (Kwon & Johnson, 2014).

Bodin (2015) explains that due to the constantly changing operational environment, security management is becoming more complex and broader in scope. Further, Cavusoglu, Raghunathan and Yue (2012) state that as contemporary business organizations are expanding beyond borders and competing globally, so does the threat posed by global insecurity. The pressure that managers face requiring them to ensure security is provided and their organizations in entirety are safe is overwhelming (Anderson, 2011). The question that remains is to what extent Kenyan firms have implemented strategic security management structures in the provision of their services to improve their effectiveness. In Kenya, increases in insecurity related to terrorism, robbery and cybercrime have been reported to affect business adversely (Katua, 2014). For organizations that have implemented strategic security management structures, the effect to the performance of the organization is always in question (Bose & Luo, 2014).

A study by Gordon and Loeb (2013) established that ICT security management affects employee productivity, reduces organizational losses and enhances organizational productivity. Kwon and Johnson (2014) on the other hand established that though there is no direct link between security management and firm performance, security management is a factor which plays an indirect role in enhancing the work environment.

There had been very few local studies focusing on strategic security management and firm performance. Katua (2014) sought to establish the role of information security management at Kenya Electricity Generating Company and established that through ISM strategy organizational competencies were developed and preserved for better performance of the Company. Ndung'u (2014) studied security management in top 100 midsized companies in Kenya and established that top management commitment, human-related information security issues and information security risk assessment were individually significant predictors of firm performance. The few local studies on security management and firm performance have mostly focused on information security whereas the current study will focus on security in general where information security will just be a sub variable. This study suggested that implementation of strategic security management practices is critical in providing security solutions that enhance firm performance.

Objectives of the Research

The general objective of this research was to establish the effect of strategic security management practices on the firm's performance. **The** Specific Objectives were:

- To determine the effect of strategic ICT infrastructure on performance of KRA in Nairobi.
- To assess the effect of strategic leadership coordination on performance of KRA in Nairobi.

- To evaluate the effect of strategic employee participation on performance of KRA in Nairobi.
- To establish the effect of strategic employee working conditions on performance of KRA in Nairobi.

Empirical Review

Studies carried out on strategic security management and organization performance are reviewed in this section. Specifically, this section reviewed studies on security of ICT, leadership and coordination in strategic security management, employee involvement in security management and security of working conditions. The relationship between these sub variables on strategic security management and organizational performance was discussed.

Security of ICT Infrastructure

ICT security relates to an array of actions designed to protect information, information systems and ICT hardware (Gordon and Loeb, 2013). Therefore, ICT security does not cover only the information itself but also the entire infrastructure that facilitates its use. It covers hardware, software, threats, physical security and human factors, where each of these components has it is own characteristics. Consequently, a study by Kuhn, Ahuja and Mueller (2013) established that ICT security plays a major role in the internet age of technology and firm performance. Given that the number of organization security breaches is increasing daily, and the more accessible the information, the greater the hazards, it is inevitable that security will need to be tightened (Brown & Duguid, 2011).

A study conducted by Bharadwaj (2013) observed that as the number of employees, applications and systems increase, the management of the organization's ICT infrastructure becomes much more difficult and consequently vulnerabilities potentially increase. To determine secure use of hardware and software as well as facilitating and encouraging secure employee behaviour, organizations make use of ICT security policies. An ICT policy is a combination of principles, regulations, methodologies, techniques and tools that directs on how ICT should be used (Tryfonas et al., 2011) established to protect the organization from threats.

A study by Canavan (2013) established that these policies also help organizations to identify its information assets and define the corporate attitude to these information assets and have a role in ensuring that the firm continues to perform effectively. The effectiveness of ICT-related investments, measured in financial terms, has been a topic of research for quite a while now. However, researchers (Anderson, 2011; Bodin et al., 2015) have argued that ICT security investments, unlike other IT-related investments, additionally depend on political or regulatory decisions and not solely on financial decisions. In essence, ICT security investment must be analyzed using a holistic approach that combines different factors such as technical, financial, legal and policy. This study takes such a holistic approach to identify critical ICT security factors and their effects on firm performance.

Enterprise security governance is a firm's strategy for reducing the risk of unauthorized access to ICT systems and data. It ensures that security strategies are aligned with business objectives and consistent with regulations (Bose & Luo, 2014). In essence, security governance provides oversight and strategic planning, authorizes decision rights, enacts policy, specifies the accountability framework, and involves resource allocation. Security policies on the other hand are developed to enforce firm wide standardization and integration. The risk assessment and management function is involved in identifying, addressing, and minimizing, or even eliminating enterprise vulnerabilities. Security training, education and awareness programs alert employees to risks, make them aware of countermeasures that exist to mitigate these risks and drill into them the importance of security and awareness programs. This has been established to enhance not just preparedness of the organization but also the performance of the firm (Razi and Madani, 2013).

Regulatory compliance involves meeting the requirements of national and local legislations such as personal data privacy and security act, which is designed to prevent and mitigate identity theft, to ensure privacy and to provide notice of security breaches (Brody et al., 2012). ICT security has also been established to enhance criminal penalties, law enforcement assistance and other protections against security breaches, fraudulent access and misuse of personally identifiable information (Anderson, 2011). However, a study by Kwon and Johnson (2014) did not establish any significant effect of ICT security investments and firm performance though they observed that there can be indirect effects.

Cyber security insurance is not meant to be a substitute for protection of company data and security policies (Bharadwaj, 2013). Rather a firm that would purchase this insurance will also implement proper preventative measures to ensure that they will never have to use it. Most cyber security insurance policies provide two levels of coverage. First-party coverage accounts for the costs that the business would have to lay out to respond to a loss of clients' or employees' private information. Third-party coverage covers legal defense costs, including lawsuits filed by consumers and other businesses. Security personnel includes, but are not limited to, information security manager who reports to the chief information security officer, data security analysts, security business analysts, security engineer, security administrator, compliance officer, auditor, security officer – hardware, software and network − and physical security officer. Moreover, a study by Aral and Weill (2011) established that though buying insurance is a good risk management approach, mitigating cyber threats is really better and has a positive effect on cost management and firm performance.

Network security technologies such as firewalls, demilitarized zone and data loss prevention protect the usability, reliability, integrity and safety of organizational networks and data. Platform security technologies include antivirus software and patching. Application security technologies include secure coding and secure socket layer (Razi and Madani, 2013). Mass storage security technologies include disk and backup tape encryption and shared storage access control. File and data security technologies include file and data encryption and enterprise rights management. Response to security attack or breach includes monitoring, intrusion detection and delivering proactive and reactive responses. A new trend is increasingly becoming popular in the business IT environment where many employees are using their personal devices at work (Aral & Weill, 2011). This mobile trend is called bring your own device (BYOD). Implementing a BYOD program requires the same security measures that one applies to any devices already on the network.

For example, enforcing strong passwords; installing antivirus protection and data loss protection software; having full-disk encryption for disk, removable media and cloud storage; application control; and mobile device management (MDM) to wipe out sensitive data when devices are lost or stolen. Observance of network security technologies was noted in a study by Razi and Madani (2013) to influence the working environment around ICT and hence affecting the productivity of employees and eventually the performance of the firm.

Leadership in Strategic Security Management

Business organizations increasingly are seeking leadership that emphasizes ethics, risk management and a concern for society, in part as a reaction to the numerous high-profile scandals involving greedy and selfish corporate management (van Dierendonck, 2011). Top leadership in every organization is central to this type of leadership. They set the tone for the organization via the vision they express, decisions they make, policies they implement, and what they pay attention to, measure, and reward (Finkelstein, Hambrick, & Cannella, 2014). Such choices and actions of the top management are critical to how well the members perform and to the firm's overall direction, performance, reputation, and stakeholder relationships (Boal & Hooijberg, 2011).

An examination of the relationship between leadership in strategic security management and firm performance is particularly important in light of the mixed results in prior empirical studies examining the effect of leadership in risk management on firm performance (for example Ling, Simsek, Lubatkin, & Veiga, 2013; Waldman, Javidan, & Varella, 2014). Undoubtedly, there are aspects of leadership relevant to firm performance that is not captured when a leadership in a particular field is under study. For instance, a study by Hambrick and Mason (2014) established that there is a positive link between executive leadership in security and ethical issues and firm performance.

The study noted that executives who constitute the top management team (TMT) make decisions and take actions that reflect their personality, orientations, values, and experiences. By providing a vision for the organization, the leader may chart a path of sustainability for the organization. Another study by Carpenter, Geletkanycz and Sanders (2014) established that top leadership influences the strategic decision-making processes and firm performance.

A recent study by Felekoglu and Moultrie (2014) on senior management and their involvement in risk management, health and safety initiatives suggested that there is a need for further theoretical development as regards how leadership in the organization in matters involving safety and ethics influence firm performance. Thus, this study seeks to advance research and theory by unraveling the context in which leadership in strategic security management helps to build and develop strategic capabilities and influence firm performance.

Waldman et al. (2014) noted that despite top managers' unique position in influencing organizational processes, relatively little is known about the ways organizational leaders build capabilities for and facilitate strategic security management practices. This is important as research points to the significant role played by senior management in facilitating cross-functional integration in the coordination of organizational activities.

Employee Participation in Strategic Security Management

Markos and Sridevi (2010) in a US study noted that consulting employees touches on almost every facet of the organization. They observed that employee consultation requites effective management of all parts of HRM so at to have employees feel that they are valued partners in the organization. Failure to engage employees would make them not to be psychologically involved with the organization leading to them being dissatisfied, less committed, and showing little organizational citizenship. The study established that employee engagement through consultations is a strong predictor of organization performance. The study further noted that improvement in employee engagement leads to enhancement of organizational performance. Organizations that consult their employees in security related issues make them to be psychologically attached hence increasing their involvement on the activities and operations of the organization.

Consulting employees in security issues is expected to build a climate of partnership and trust where the employees are enabled to take an active role in improving efficiency in the work undertakings (Sargeant, 2011). In a study in US, Sargeant determined that employee consultation can apply to both the team and the individual employee. Sargeant noted that this form of direct participation in decision making if carried out properly and regularly can have a positive impact on organization's economic performance.

Sun and Pan (2011) in a study in China observed that adopting high performance work practices in all facets of the organization including security management led to enhanced employee commitment in the surveyed firms. The study further, established that this involvement improved employee commitment which was stated by Sun and Pan to mediate in the effect of high performance work practices and organization performance. This agrees with findings of Amah and Ahiauzu (2013) that employee involvement had a significant influence on the overall organizational performance.

Kubaison, Gachunga and Odhiambo (2014) conducted a study aimed at assessing the association between employee participation schemes and organizational performance. This study was conducted in the state owned corporations in Kenya. The contribution of employee participation on the state owned corporations' performance was also sought in the study. The study revealed that state owned corporations had a variety of participation schemes employee surveys, work teams, and employee suggestion schemes. Additionally, the study revealed that suggestion schemes had a significant positive relationship with performance of the surveyed organizations. However, study results indicated that most of the surveyed organizations preferred work teams as the form of employee participation.

Muindi (2011) studied the relationship between employee participation in security management and job satisfaction in learning institutions and reported a strong positive relationship between employee participation and job satisfaction among the academic staff. Academic staff were more satisfied with the general conditions of their job when they participated in major issues in the organization including security. Other areas that showed positive relationship with employee participation were pay and promotion potential, use of skills and abilities, job design and job feedback. The conclusion made by the study was that employee performance can be improved through engaging the employees in decision making.

Security of Working Conditions

Providing amenities and facilities for the health, safety and welfare of employees is an important employer duty (Weiss, 2014). However, it is only one part of an employer's duty to provide and maintain a working environment that is safe and without risks to health. Amenities and facilities are integral to the health, safety and welfare of employees (Ogbo & Ukpere, 2013). This compliance code addresses duties to provide amenities and facilities. It does not provide guidance on other employer duties to provide the highest reasonably practicable level of protection against risks to health and safety. Workplace amenities and facilities are things provided for the health, safety, welfare and personal hygiene needs of employees. They include toilets, shelter, seating, drinking water, personal storage, washing facilities and ensuring that the work place is secure for employees to work effectively. They also include work environment facilities such as workspace, temperature and air quality, lighting and flooring.

It is evident in the research findings of Patterson et al. (2013) that the more satisfied workers are with the safety of their work environment; the better the company is likely to perform in terms of subsequent profitability and particularly productivity. Sekar (2011) argues that the relationship between work and security of the workplace becomes an integral part of work itself. The management that dictate how, exactly, to maximize employee productivity center around two major areas of focus: personal motivation and the infrastructure of the work environment (Sekar, 2011). There are various literature works that defines different factors that influence the performance of the employees. Haynes (2013) explains the behavioral office environment behavioral components of the secure office environment that have the greatest impact on office productivity. In all of the work patterns, it was found that interaction was perceived to be the component to have the most positive effect on productivity, and distraction was perceived to have the most negative. As people are the most valuable resource of an organization, and that the management of people makes a difference to company performance (Patterson et al., 2013).

To achieve high levels of employee productivity, organizations must ensure that the physical environment is conducive to organizational needs facilitating interaction and privacy, security, formality and informality and functionality.

The physical environment is a tool that can be leveraged both to improve business results (Mohr, 2016) and employee well-being (Huang, Robertson & Chang, 2014). Ensuring adequate and safe facilities are provided to employees, is critical to generating greater employee commitment and productivity. The provision of inadequate equipment and adverse working conditions has been shown to affect employee commitment and intention to stay with the organization (Weiss, 2014).

Research conducted by Roelofsen (2012) has also yielded indications suggesting that improving working environment results in a reduction in a number of complaints and absenteeism and an increase in productivity. The indoor environment has the biggest effect on productivity in relation to job stress and job dissatisfaction. Providing working conditions that promote the safety of employees is therefore becoming a major management concern (Ogbo & Ukpere, 2013).

A study by Estes and Wang (2012) established that the safety of the workplace environment impacts employee morale, productivity and engagement, both positively and negatively. The work place environment in a majority of industry is unsafe and unhealthy. These includes poorly designed workstations, unsuitable furniture, lack of ventilation, inappropriate lighting, excessive noise, insufficient safety measures in fire emergencies and lack of personal protective equipment. People working in such environment are prone to occupational disease and it negative impacts on employee's performance. Thus productivity is decreased due to unsafe workplace environment. It is the quality of the employee's workplace environment that most impacts on their level of motivation and subsequent performance. How well they engage with the organization, especially with their immediate environment, influences to a great extent their error rate, level of innovation and collaboration with other employees, absenteeism and ultimately, how long they stay in the job. Creating a work environment in which employees are safe and productive is essential to increased profits for your organization, corporation or small business.

Research Methodology

This study used a descriptive cross-sectional survey design. Thomas (2011) noted that a descriptive survey is a study designed to collect data or information on some given units or observations without influencing the study environment.

This study was carried out in Nairobi. The study involved 92 employees in the security department (KRA HR Department, 2016). The target respondents in this case were these security department's employees since they were the ones who understood the security strategy, policies and practices in the organization.

The sampling frame that was applied in this study was a list of employees in the security department of KRA. This sampling frame which was sourced from the HR department had all the employees who were in the department at the time of the study. This sampling frame was selected as it included all employees of interest in this study and hence provided a good basis for selecting the study participants.

This study did not employ any sampling as the target population was small. Babbie (2011) argued that when one is dealing with a small population, there is no need for sampling as this introduces sampling error which can be material in studies focusing on small populations. This study hence applied census where all the members in the target population participated in the study.

Questionnaire was utilized as data collection instrument in the current study. Gillham (2008) noted that a questionnaire is efficient for data collection as it ensures standard responses to prepared questions from the study respondents. The questionnaire was employed due to its economy, ability to get standard responses and the lesser effort required to collect the data in comparison to other methods such as interviews.

Two types of validity that the questionnaire was tested on were content and face validity. Expert reviews of the questionnaire were done with the help of a few strategic security personnel from the organization. Secondary review of data and information about organizational performance was done to collaborate the data from the respondents.

Findings

Strategic Security Management Practices and Firm Performance

The general objective of the study was to establish the effect of strategic security management practices on firm performance with a focus on KRA. Specifically, the study sought to establish the effect of ICT infrastructure security, leadership coordination in security management, employee participation in security management and employee working condition on performance of KRA in Nairobi. This section provided the analysis of the results in relation to these specific objectives.

Effect of Strategic ICT infrastructure security on Performance

The study had an objective of establishing the effect of ICT infrastructure security on performance of KRA. Some statements on ICT infrastructure security were provided and respondents were asked to indicate their level of agreement to the statements.

The study indicated that respondents agreed to the statement that the organization had put in place strategy and policies to safeguard ICT infrastructure and also agreed that the organization had enough safeguards to ensure security of ICT software and hardware. Respondents also agreed that KRA observed enterprise security governance aimed at reducing the risk of unauthorized access to IT systems and data. More results indicated that respondents agreed that there were network security technologies such as firewalls, demilitarized zone and data loss prevention protection at KRA and also agreed that the organization made it clear that ICT infrastructure security was very important to employees and to the company. Respondents however, were neutral on a number of statements in ICT infrastructure security at KRA.

Respondents were neutral to the statement that the organization had effective punishments and deterrents that ensured ICT security policies and strategy were observed and also the organization had effective reward systems to ensure adherence to ICT infrastructure security. Respondents also indicated neutrality to the statements that and also that the KRA has cyber security insurance aimed at indemnifying it in case of a loss related to cybercrime and that KRA continually monitored use of ICT invading intrusion detection and delivered effective proactive and reactive responses.

This indicates that there were some weaknesses in ICT security policies, reward systems for adherence to ICT security, and cyber security insurance. There were also weaknesses in monitoring of ICT security risks and responses thereof.

Strategic Security Leadership and Coordination

The study had an objective to determine the effect of security leadership coordination on performance of KRA in Nairobi. Statements that related to security leadership coordination were provided and respondents were required to indicate their level of agreement to the provided statements.

Results as presented indicated that the respondents agreed to the statement that the security strategy and policies were well communicated to employees and employees understood them. Further, respondents also agreed to the statement that KRA had policies with clear instructions on every single aspect of security and how someone should be acting in facing any incident.

However, findings indicated that respondents were neutral to other statements listed. These included statements that the top leadership of KRA were at the forefront of security management ensuring that matters of security were coordinated effectively, that KRA had a security strategy that laid down the vision and mission of the organization regarding security and that security strategy and policy were presented in an attractive way and displayed in strategic places for employees and visitors to remember them. These findings indicate that KRA had a security policy which was well communicated to employees. However the organization had weaknesses in top management involvement in security issues, security strategy and communication of policies to employees and visitors.

Strategic Employee Participation in Security Issues and Performance

The study further sought to establish the effect of strategic employee participation in security management and its effect on performance of KRA in Nairobi. Statements regarding employee participation were listed and respondents were required to indicate their level of agreement. The results indicate that the respondents disagreed to the statement that employees were taken through security management when they were recruited into the organization. This implied that employees were not orientated on security management upon recruitment at KRA.

Study results further revealed that the respondents were neutral to the statements that views and opinions of employees were continually sought to inform strategy and policies in security management at the organization and that there was a disciplinary strategy of reward and sanction procedures that motivated employees to comply with security strategy and policy. Moreover, study results indicated that respondents were neutral to the statements that employees got feedback and updates regarding security management and that KRA employees got regular communication regarding security management and progresses in the organization. These results revealed that there were gaps in employee involvement in security management at KRA. There were gaps in seeking employee opinions, reward strategy, feedback to employees and communication.

Strategic Security of Employee Working Conditions

The study sought to determine the effect of strategic security of employee working conditions on performance of KRA in Nairobi. Respondents were asked to indicate their level of agreement to statements provided. Study results revealed that the respondents agreed that the work environment did not present any harm physically or health wise to the employees while they also agreed that employees at KRA were effectively secured from threats that could come out of the premises. Further, the respondents agreed that property of employees at the workplace was always secured as practically as possible while they also agreed that there were enough mitigating measures taken to ensure effective response against disasters such as fire.

Respondents also agreed that KRA had provided amenities and facilities that were good for the health, safety and welfare of employees and also agreed that KRA had provided and maintained a working environment that is safe and without risks to employees. Respondents were however neutral to the statement that management at KRA had effectively managed the infrastructure of the work environment. These results pointed that KRA had good working conditions but could improve on management of the workplace infrastructure.

Regression Results

A multiple linear regression analysis was performed to test the cause and effect relationship between the independent and the dependent variables. The average ratings for the four independent variables (ICT infrastructure, leadership coordination, employee participation and working conditions) were used as the indicators for input into the regression model. Three measures of performance (employee satisfaction, tax collection and customer satisfaction) were used.

The coefficient of determination and standard error of the regression model is indicated in Table 1. Results in Table 1 indicate that the adjusted r^2 was 0.581 indicating that the independent variables explained 58.1% of the change in performance at

KRA was explained by the independent variables. This indicates that the model had good explanatory power.

Table 1: Regression Model Parameters

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.762	.581	.547	.603

Further, the regression output in Table 2 presents the source of variance, mean of variances and the f value. The results indicates that the overall model was significant (f value = 24.530; p < 0.05) and could provide important results. This indicates that the model could provide some predictive significance and was a good fit.

Table 2: Analysis of Variance of the Regression

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	21.881	4	5.470	24.530	.000
Residual	15.803	71	.223		
Total	37.684	75			

KRA provided secure work environment where security against internal and external threats was provided. KRA also had enough mitigating measures to ensure effective response against disasters such as fire and terrorism.

Summary of Findings

The study had four specific objectives. These were to establish the effect of ICT infrastructure security, leadership coordination in security management, employee participation in security management and security of working conditions on performance of KRA in Nairobi. The summary results of the study are provided in this section based on the study objectives.

Effect of ICT Infrastructure security on performance

The results established that security of ICT infrastructure significantly and positively affected performance of KRA. Results further revealed that the organization had put in place strategy and policies to safeguard ICT infrastructure and that the organization had enough safeguards to ensure security of ICT software and hardware. Similarly, results revealed that KRA observed enterprise security governance aimed at reducing the risk of unauthorized access to IT systems and data and that there were network security technologies such as firewalls, demilitarized zone and data loss prevention protection at KRA. The organization also made it clear that ICT infrastructure security was very important to employees and to the company. However, results established weaknesses on punishments and deterrents for ICT security policies and strategy, reward systems to ensure adherence to ICT infrastructure security, cyber security insurance aimed and continuous monitoring and of ICT intrusion detection.

Effect of Security Leadership Coordination and Performance

Leadership coordination in security management positively and significantly influenced performance of KRA. Study results also revealed that the security strategy and policies were well communicated to employees and employees understood them. Further, results indicated that KRA had policies with clear instructions on every single aspect of security and how someone should be acting when facing a security incident. The study results also noted that there were weaknesses in top leadership involvement in security issues, having an effective security strategy that laid down the vision and mission of the organization and effective communication of the security strategy to employees and visitors.

Effect of Employee Participation in Security Management on Performance

Employee participation in security management did not have a significant influence on performance of KRA. The results also indicated that employees were not orientated on security management when they were recruited. Study results further revealed that there were weaknesses in seeking views and opinions of employees to inform strategy and policies in security management. The organization also lacked an effective disciplinary strategy of reward and sanction procedures to ensure adherence to security strategy and policy. Moreover, study results indicated that there was no effective feedback mechanism on security management. The organization also was not effective in provision of regular communication regarding security management and progresses in the organization.

Effect of Security of Working Conditions on Performance

Security of employee working conditions at KRA significantly influenced performance of the organization. Study results revealed that the work environment did not present any harm physically or health wise to the employees. Employees at KRA were effectively secured from threats that were external to the organization whereas their property was always secured as practically as possible. Results also established that there were enough mitigating measures taken to ensure effective response against disasters such as fire. Results also established that KRA had provided amenities and facilities that were good for the health, safety and welfare of employees and also that KRA had provided and maintained a working environment that is safe and without risks to employees. However, there were weaknesses noted in effectively managing the infrastructure of the work environment.

Conclusion

From the study findings, the following conclusions are made. First, security of ICT infrastructure significantly and positively affected performance of KRA. KRA also had put in place strategy and policies to safeguard ICT infrastructure which indicated the important role of ICT to the organization. KRA had challenges in formulating punishments and deterrents for ICT security policies and strategy, implementing reward systems to ensure adherence to ICT infrastructure security and having cyber security insurance. The organization also had gaps in continuous monitoring of ICT policies and practices.

Secondly, leadership coordination in security management positively and significantly influenced performance of KRA. KRA’s security strategy and policies were well communicated to employees and had policies with clear instructions on every single aspect of security. However, KRA had challenges in top leadership involvement in security issues and its security strategy had gaps in laying down the vision and mission of the organization.

Third, employee participation in security management did not have a significant influence on performance of KRA. KRA did not orientate employees well on security management. There were also gaps in incorporating employees' views and opinions in security management, gaps in feedback mechanisms on security management and also gaps in communication regarding security management.

Lastly, security of employee working conditions at KRA significantly influenced performance of the organization. KRA provided secure work environment where security against internal and external threats was provided. KRA also had enough mitigating measures to ensure effective response against disasters such as fire and terrorism.

Recommendations

From the study findings, the following recommendations are made. First, KRA should put in place reward systems where there are punishments and deterrents for observance of ICT security policies and strategy. Moreover, KRA should ensure that its security strategy should be aligned to the overall corporate strategy. The organization should also put in place a monitoring and evaluation program aimed at ensuring that the organization is safe and secure at all times.

Secondly, top leadership of KRA should be involved in leading security management and also in designing and implementing security strategy and policies in the organization. This strategy should also be well communicated to employees where their involvement would be sought to ensure that the strategy was implemented effectively.

Third, employee participation in security management had various challenges. Employees should be always orientated on security management when they are recruited to ensure that they understand security issues and help in implementing the security strategy. Moreover, the study recommends that the suggestions and views of employees should be continually sought to ensure that the human element is effectively included in security management.

Lastly, KRA should have a clear plan and log of the physical and ICT infrastructure in place. KRA should also ensure that the infrastructure in place is functional at all times to enhance service delivery to employees and customers. There should be an effective maintenance plan to ensure that any infrastructure involved in security is functional so as to reduce the risk to the organization.

Areas for Further Research

The study focused on strategic security management and performance of KRA in Nairobi. The study focused on leadership coordination, employee participation, security of ICT infrastructure and security of employee working conditions. The study recommends that a similar study be conducted in other KRA branches mostly Mombasa which deals with good entering and leaving the Kenyan borders where security management is paramount.

Moreover, a study on strategic security management in other types of businesses such as SMEs, private companies and multinational corporations is suggested. This is because the current study was focused on a public entity whose findings may not be generalizable to other forms of business.

Lastly, a study could focus on areas that were not focused on this study including security management concerning terrorism, security issues brought about by employees and security concerns regarding theft, fraud and misappropriations that emanate from the workforce of the organization.

REFERENCES

Ahammad, M. F., Lee, S. M., Malul, M., & Shoham, A. (2015). Behavioral Ambidexterity: The Impact of Incentive Schemes on Productivity, Motivation, and Performance of Employees in Commercial Banks. *Human Resource Management, 52* (2), 156 – 171.

Amah, E., & Ahiauzu, A. (2013). Employee involvement and organizational effectiveness. *Journal of Management Development, 32* (7), 661 – 674.

Anderson, R. (2011), "Why information security is hard: an economic perspective", Proceedings of the 17th Annual Computer Security Applications Conference, Los Alamitos, CA, pp. 358-365.

Aral, S. and Weill, P. (2011), "IT assets, organizational capabilities, and firm performance: how resource allocations and organizational differences explain performance variation", Organization Science, Vol. 18 No. 5, pp. 763-780.

Aronson, S.L. (2013). Kenya and the Global War on Terror: Neglecting History and Geopolitics in Approaches to Counterterrorism. African Journal of Criminology and Justice Studies, 7 (1&2), 24-34.

Babbie, E. (2011). *The Practice of Social Research* (13th ed). Belmont: Wadsworth Thomson.

Bandura, R. P., & Lyons, P. R. (2014). Situations-vacant fall where employees are engaged: Involvement boosts various aspects of organizational performance. *Human Resource Management International Digest, 22* (5), 22 – 25.

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management, 17*, 99-120.

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, *17*, 99 - 120.

Bharadwaj, A.S. (2013), "A resource-based perspective on information technology capability and firm performance", MIS Quarterly, Vol. 24 No. 1, pp. 169-196.

Boal KB, Hooijberg R. (2011). Strategic leadership: Moving on. The Leadership Quarterly , 11, 515–550.

Bodin, L.D., Gordon, L.A. and Loeb, M.P. (2015), "Evaluating information security investments using the analytic hierarchy process", Communications of the ACM, Vol. 48 No. 2, pp. 79-83.

Bose, R., & Luo, X.R. (2014). Investigating security investment impact on firm performance. International Journal of Accounting & Information Management, 22 (3), 194 – 208.

Brown, J. S. and Duguid, P., (2011). The Social Life of Information. Boston: Harvard Business School Press.

Brown, S., McHardy, J., McNabb, R., & Taylor, K. (2011). Workplace Performance, Worker Commitment, and Loyalty. *Journal of economics and management strategy, 20* (3), 925 – 955.

Calas, B. (2008). From rigging to violence. Lafargue, J. (Ed.). The general elections in Kenya, 2007. (pp. 165-185). Dar es Salaam: Mkuki na Nyota Publishers, Ltd.

Carty, M. , Pimont, V. and Schmid, D.W. (2012), “Measuring the value of information security investments”, IT@Intel White Paper, Intel Corporate, Santa Clara, CA.

Cavusoglu, H. , Raghunathan, S. and Yue, W.T. (2012), “Decision-theoretic and game-theoretic approaches to IT security investment”, Journal of Management Information Systems, Vol. 25 No. 2, pp. 281-304.

Coolican, H. (2004). *Research methods and statistics in psychology*. London: Hugh Coolican.

Creswell, J. (2009). *Research Design; Qualitative and Quantitative and Mixed Methods Approaches*. London: Sage.

Easterby-Smith, M., Thorpe, R. & Lowe, A. (1999). *Management Research: An introduction*. London: SAGE Publication Ltd.

Estes, B. & Wang, J. (2012). Workplace Incivility: Impacts on Individual and Organizational Performance. Human Resource Development Review, Vol. 7, June 2008, pp.218-240.

Finkelstein S, Hambrick DC, Cannella AA, Jr. (2014). *Strategic leadership: Theory and research on executives, top management teams, and boards* . Oxford , UK : Oxford University Press.

Gillham, B. (2008). *Developing a questionnaire* (2nd ed.). London: Continuum International Publishing Group Ltd.

Gordon, L. A. & Loep, M. P. 2006. Budgeting Process for Information Security Expenditures. Communications of the ACM, Vol. 49, No. 1, pp. 121-125.

Gordon, L.A. and Loeb, M.P. (2012), “The economics of information security investment”, ACM Transactions on Information and System Security, Vol. 5 No. 4, pp. 438-457.

Hesket, J. L., Jones, T. O., Loveman, G.W., Sasser, W. E., & Schlesinger, L. A. (1994). Putting the service-profit chain to work. *Harvard Business Review*, 164 – 174.

Heskett, J. L., Jones, T. O., Loveman, G. W., Sasser, W. E., and Schelsinger, L. A. (1994). Putting the Service Profit Chain to Work. *Harvard Business Review*, (March- April), 164 – 174.

Israel, G. D. (2013). *Determining Sample Size*. Florida: University of Florida.

Katua, F. S. (2014). Information security management strategy implementation challenges at Kenya Electricity Generating Company. MBA Project, University of Nairobi, Nairobi.

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

Kuhn, JrJ.R. , Ahuja, M. and Mueller, J. (2013), “An examination of the relationship of IT control weakness to company financial performance and health”, International Journal of Accounting and Information Management, Vol. 21 No. 3, pp. 227-240.

Kurpius, S. E. & Stafford, M. E. (2006). *Testing and measurement: A user-friendly guide*. Thousand Oaks: Sage.

Kwon, J. and Johnson, M.E. (2014), “Proactive versus reactive security investments in the healthcare sector”, MIS Quarterly, Vol. 38 No. 2, pp. 451-472.

Leblebici, D. (2012). Impact of workplace quality on employee‘s productivity: case study of a bank in Turkey. Journal of Business, Economics & Finance, Vol.1 (1)

Ling Y, Simsek Z, Lubatkin MH, Veiga JF. (2014). The impact of transformational CEOs on the performance of small- to medium-sized firms: Does organizational context matter? Journal of Applied Psychology, 93, 923–934.

Lounsberya, M.O., Pearson, F. & Talentino, A.K. (2011). Unilateral and Multilateral Military Intervention: Effects on Stability and Security. Democracy and Security, 7 (3), 227-257.

Maupeu, H. (2008). Revisitng post-election violence. Lafargue, J. (Ed.). The general elections in Kenya, 2007. (pp. 187-223). Dar es Salaam: Mkuki na Nyota Publishers, Ltd.

Mugenda, O. and Mugenda, A. (2003). *Research methodology: qualitative and quantitative techniques.* Nairobi: Acts Press.

Muindi, F. K., (2011). The Relationship between Participation in Decision Making and Job Satisfaction among Academic Staff in the School of Business, University of Nairobi. *Journal of Human Resources Management Research*, 22, 1 – 34.

Ndung’u, S. I. (2014). Moderating role of entrepreneurial orientation on the relationship between information security management and firm performance in Kenya. PhD Thesis, Jomo Kenyatta University of Agriculture and Technology, Nairobi.

Ogbo, A.I. & Ukpere, W.I. (2013). Management of Designed Safety Adherence Model for the Nigerian Work Environment. Journal of Human Ecology, 41(3), 183-191

Oppenheim, A. N. (2000). *Questionnaire design, interviewing and attitude measurement* (New ed.). London: Continuum International Publishing Group Ltd.

Porter, M. E. (1985). *Competitive Advantage*. New York: The Free Press.

Reid, R. C. & Floyd, S. A. (2001). Extending the risk analysis model to include market insurance. Computers & Security, 20(4), 331-9.

Rucci, A. J., Kirn, S. P. & Quinn, R. T. (1998). The Employee-Customer-Profit Chain at Sears. *Harvard Business Review, 76* (1), 65 – 71.

Thomas, G. (2011). *How to do your Case Study: A Guide for Students and Researchers*. Thousand Oaks: Sage.

van Dierendonck D. (2011). Servant leadership: A review and synthesis. Journal of Management, 37, 1228–1261.

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