THE INFLUENCE OF STRATEGIC SECURITY PLANS ON ORGANIZATION MANAGEMENT: A CASE OF KENYA PORTS AUTHORITY

BY

LUKE N. NANDASAVA

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF ARTS IN PROJECT PLANNING AND MANAGEMENT DEGREE

DEPARTMENT OF URBAN AND REGIONAL PLANNING

MASENO UNIVERSITY

DECLARATION

Declaration by the Student

This Research project is my original work and has not been presented for a degree in any other University.

Sign: ..... Date:……

Luke N. Nandasava
Reg. No: EL/SPM/00522/2013

Declaration by the Supervisor

This research project has been submitted for examination with my approval as a University Supervisor.

Sign: ..... Date:……

Dr George G. Wagah
School of Planning and architecture,
Maseno University.

ACKNOWLEDGEMENT

The production of this research project was made possible by the assistance and support given to me in a variety of ways by various people. They were always enthusiastic, supportive and critical when I needed it most. I acknowledge and appreciate my University supervisor Dr. George G Wagah, for his insightful guidance and assistance at every stage of writing this project. I would like to acknowledge the enthusiastic support of all management of the Kenya Ports Authority for their support in facilitating my data collection. I am sincerely grateful to my family for their encouragement, support and constant prayers. Finally, all glory and honor goes to God for giving me good health and strength to carry on.

DEDICATION

I dedicate this research to my family who gave me great encouragement, devotion and to all my comrades, friends and fellow students together with whom we share the same opinion towards project planning and management.

ABSTRACT

Dynamic environments characterized by technological, economic, and political change increasingly requires organizational alertness among public organizations. The survival and success of an organization occurs when the organization creates and maintains a match between its strategy and the environment and also between its internal capability and its strategy. Kenya Ports Authority (KPA) envisions itself to be World class seaports of choice with a mission of facilitating and promoting global maritime trade through provision of competitive port services. Strategic security plans is the process of choosing the organization's security goals and ways to achieve them in response to the challenges posed by the operating environment. Organizations have to adequately and promptly respond to these challenges in the environment for them to be successful. The objective of this study was to determine the influence of strategic security plans to KPA management. The study was conducted within the Kenya Ports Authority in Mombasa. KPA has 32 departments with 7 division heads. This formed a target population of 39. Purposive sampling was further used to select key respondents for structured interviews. The study used primary data collected using questioners and interview guides on the departmental managers at KPA. The data obtained from the questionnaires and interview guide was analyzed using content analysis. The data was then presented in prose format. The study established that it is impossible to separate the concept of security transformation from the pragmatic day-to-day discipline necessary to achieve it. In order to transform security infrastructure, organization must ensure that each security project clearly maps back to the organization's strategic business objectives. KPA has successfully restructured its organization, there is need to focus on change management issues, proper organizational communication and adequate strategic security plans. Strategic security plans at KPA enabled the organization to redesign and improve business work processes radically but there is still need for initiatives that emphasize incremental improvement in the whole strategic security planning process and output to cope with changes in the ever changing business environment. In light of the findings, the study recommends that security awareness training be done regularly to enable both the management and employees understand system vulnerabilities and threats to organization operations that are present.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

KPA	:	Kenya Ports Authority
IMO	:	International Maritime Organization
CCTV	:	Closed Circuit Television
ISPS	:	International Ship and Port Facility Security
SOP	:	Standard Operating Procedure
EAC	:	East African Community
KCHSC	:	Kenya Cargo Handling Service Company
IT	:	Information Technology
EH&S	:	Emergency Health and Security Services
IPS	:	Integrated Physical security plan
ISMS	:	Integrated Security Management System
KPIs	:	Key Performance Indicators
IDS	:	Intrusion Detection Systems
NCSC	:	National Cyber Security Centre
PMAESA	:	Port Management Association of Eastern and Southern Africa
JICA	:	Japan International Cooperation Agency
CFS	:	Container Freight Stations
SAP	:	Systems Application Program
VTMIS	:	Vessel Traffic Management Information Systems
ISM	:	International Safety Management
NEMA	:	National Environmental Management Authority
KRA	:	Kenya Revenue Authority

OPERATIONAL DEFINITION OF TERMS

Security is defined as the measures taken to safe gourd the port against terrorism, sinking or grounding of the ships, theft of cargo and organizational assets, protection against cyber-crimes such as hacking of the systems, espionage, sabotage and security of the employees and the customers within KPA.

A strategy in this context is defined as a complete plan which specifies what choices an organization will make in every possible situation in order to reach a preset objective. It is a set of beliefs on how a firm can achieve success in a highly dynamic and competitive environment.

A strategic security plan is the process of choosing the organization's security goals and ways to achieve them.

Cyber Security Plan is the measures adapted by the organization, that comprise of body of technologies, processes and practices designed to protect network systems, computers, programs and data of the organization from attack, damage or unauthorized access.

Physical Security Plan is measures adapted by the organization to protect personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.

Personnel security plan is a system of policies and procedures which seek to mitigate the risk of employees exploiting their legitimate access to an organization’s assets for unauthorized purposes. People security is about shaping and controlling the environment to promote vigilance and an effective security culture, and to influence and deter those seeking to cause harm.

Organizational Management refers to the art of getting people together on a common platform to make them work towards a common predefined goal. It binds employees together and gives them a sense of loyalty towards Kenya Ports Authority. This is exercised through the functions of organizing, planning, staffing, controlling, and directing of resources and personnel towards achieving the vision of KPA.

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE: INTRODUCTION

1.1 Background to the Study

The iterative process of strategic security management includes predictions and forecasts on challenges that an organization is likely to encounter as a result of changes in the external environment (Sauer and Willcocks, 2003). However, this statement assumes a rational process and approaching strategy in the right way. Even if there were strong pointers to a possible right way, it is arguably difficult for strategists to make decisions without reference to their own views on how strategy should be determined (Frishammer, 2003). Strategic management involves strategy formulation, implementation evaluation and control.

The survival and success of an organization occurs when the organization creates and maintains a match between its strategy and the environment and also between its internal capability and its strategy (Grant, 2002). Ports are critical enablers of a country's competitiveness on the international market hence they need to be oriented towards supply chain to meet the changing needs of their customers. Kenya Ports Authority's mandate is to maintain, operate, improve and regulate all scheduled sea ports situated along the coastline (KPA, 2012). To be more responsive to customers' demands and keep abreast with global shipping trends, the Kenya Ports Authority has resorted to various strategies to uplift its services to the world-class level.

Kenya ports security has been tightened up considerably following the events of 11 September 2001 in United States and the sharp rise in terrorist incidents worldwide (African Center for Strategic studies, 2009). Kenya Ports Authority has responded positively to pressure from the international community by taking steps to increase the level of security checks and supervision in all sectors. Until recently, KPA was concerned mainly with cargo security, but now, in common with other port authorities around the world, KPA is focusing its attention on the security of physical properties, personnel and cyber network within its organization and beyond. The authority is determined to ensure that its ports comply with the security rules of the International Maritime Organization (IMO), (Sekomo, 2013). The influence of this security measures on the management of KPA have not been identified.

Several scholars have reviewed the subject of strategies developed by organizations in response to the changes taking place in the operating environment. Sanga (2012), concludes that strategy implementation at Kenya Maritime Authority faces many challenges which directly related to the reporting hierarchy and structure of the organization. Strategic security plans that forms an integral part strategies of Kenya Maritime Authority also faces the same challenges but how they influence decision making and the structure of the organization have not been identified in the study.

Flood, Marm and Young, (2010) concludes that for the success of any organizational strategy, it must be properly aligned to organizational management structures. Tai (2007) finds that there exists major barriers including how the management structure of the organization is designed and also there is lack of communication between the management and staff on the implementation of the organizational strategy. It is true that strategies as a whole must be aligned with organizational management structures; however, strategic security plans will as well influence manner in which the organization is structured.

Wilson (1990) observed that developing a holistic view for convergence issues requires a collaborative dialogue between multiple functions within an organization to better understand the common risk concerns, challenges, and possible solutions. This includes physical, personnel, and information security, business continuity, disaster recovery, disaster preparedness, emergency services, and safety. The focus of this is on getting security solutions integrated throughout the company's business architecture from operations to service delivery.

David (2005) argues that to protect the organizational assets, employees, and customers from security risks, organizations must analyze their security practices to identify the threats to their operations and protect themselves in the most cost-efficient way. Anderson (2011), argues that the strategic plans provides a framework for the management of the organization and that strategic planning system enables company shareholders and management to determine the direction and pace of business development. The direction and pace of the organization will be influenced either positively or negatively by the strategic security plans development.

Swaleh (2007) studied competitive strategies adopted by petroleum retail stations in Kenya using a case of Mombasa City and he concluded that they used reactive strategies but he did not mention anything on oil distribution. Mwarania (2008) conducted a study on strategic responses to changes in the external environment the case of Kenya Re Corporation and found that they mainly used focus strategies while Gichumbi (2008) did a study on strategic responses by NSSF to changing environmental conditions in Kenya and found that they mainly employed reactive and decisive strategies.

Agumba (2012) reviewed the competitive strategies in response to challenges of external environment by Water Resources Management Authority in Kenya. He established that in order to improve its competitiveness, the Authority needed to emphasis more on corporate social responsibility and create working relationships with corporate organizations that can sponsor the Authority in its efforts to protect the water catchments. Mwikali (2012) also looked at the response strategies adapted by Kenya Pipeline Company (KPC) Limited to the challenges of oil distribution in Kenya. He established that KPC devised several strategic security plans to counter the challenges emanating from the changes in its operating environment

1.2 Statement of the Problem

KPA envisions itself to be World class seaports of choice with a mission of facilitating and promoting global maritime trade through provision of competitive port services. To achieve these vision and mission, KPA is guided by five key objectives which include: improving managerial, operational and financial performance; developing, maintaining and sustaining port facilities and infrastructure to meet the customer needs; promoting the Port of Mombasa as a primary gateway to the great lakes region and also serve the horn of Africa; maintaining and promoting a clean, safe working and rewarding environment; integrating the functionality of the Port of Mombasa in the development vision of the republic of Kenya and the region; and instilling sound corporate governance practices.

KPA exist in complex and volatile commercial, economic, political, technological, cultural and social environments. The environmental changes occasioned by these factors are more complex for some organizations than others due to differences in economies of scale. For survival, KPA must maintain a strategic security fit within the environment. The environment is indispensable

and KPA has to respond to its dynamism, heterogeneity, instability and uncertainty. It is only through strategies developed by KPA that are able to achieve its vision and mission.

KPA is currently facing high level of insecurities as seen by the high levels of theft of containers at the port. The services at the Port have not been up to standard as the operations at the Port are way below the world class services. In the quest to improve service delivery, the management team at KPA developed a strategic security plan that aims at transforming the port into a world class sea port of choice. Risks to KPA are assessed based on their probability and impact (both quantitative and qualitative), and then security measures are implemented based on this risk analysis. KPA however, face particularly high levels of uncertainty. When planning fails to adequately account for high levels of uncertainty, the consequences can be costly.

The security challenges comprise of the cyber-crimes, personnel security issues and the physical security issues affecting the both the employees and the customers. KPA have to adequately and promptly respond to these challenges in the environment for them to be successful. The security plans developed are implemented by the management in the hope that they will mitigate the organization against the security challenges they face. In the process of implementation, the management makes decisions bearing in mind that the security challenges might hinder the organization from achieving its objectives.

It is in this light that the study sought to fill the existing gap in this area of sea port services bench-making in Kenya because there is no study which has been carried out in this area by answering the following the question: what has been the influence of strategic security plan on the management of the Kenya Port Authority.

1.3 Objective of the Study

The broad objective of this study was to investigate the influence of strategic security plans on the organization's management. Specifically the study sought to:

a. Determine the influence of cyber security plans on organization management at the Kenya ports authority.

b. Determine the influence of personnel security plans towards the KPA management.

c. Assess how physical security plans influence the overall organization management at Kenya Ports Authority.

1.4 Research Questions

The study sought to provide answers to the following research questions:

a. How does a cyber-security plan influence the organizational management at KPA?

b. What are the effects of personnel security plans to organization management at KPA?

c. How does the physical security plans influence the overall management of organizations at KPA?

1.5 Significance of the Study

This study would contribute to the theory on strategic management in organizations. In particular, the study will be useful to researchers and academia in the field of strategic security planning and responding to changes in the operating environment. They would be able to identify the changes that have taken place in the sea transport and see how they can improve service delivery to the standards of world-class sea ports. The study would further contribute to the practice of strategic security planning and in particular demonstrate the strategies developed by organizations to respond to challenges in the operating environment. It would therefore provide a framework upon which more efficient security strategy responses can be developed in organizations to effectively deal with the changing environment.

1.6 Scope and Limitation of the Study

The study focused on investigating the influence of security plans on organization management: a case of Kenya Ports Authority. It investigates on the key physical, information and personnel security measures that organisations chose to apply to reduce their vulnerabilities and how they have influence on the management of the organization. The study was conducted at KPA, focusing on Kenya pots authority management and the physical structures at the port.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter takes an in depth look at literature on the influence of security plans on organization management. This chapter provides a theoretical and conceptual framework of the study, explore what others have said and done on this topic. The chapter also provides a review on; the critical areas of the study and focused on: influence of cyber security plans, personnel and physical security plans on the overall organization management.

2.2 Cyber Security Plans to Organization Management

Almost every business relies on the confidentiality, integrity and availability of its data. Protecting information, whether it is held electronically or by other means, should be at the heart of the organisation's security planning. Dinicu (2014) points out that the key questions to keep under constant review are: Who would want access to our information and how could they acquire it? How could they benefit from its use? Can they sell it, amend it or even prevent staff or customers from accessing it? How damaging would the loss of data be? What would be the effect on its operations?

Fischer (2015) established that people who actually or potentially perform cyber-attacks are widely cited as falling into one or more of five categories: criminals intent on monetary gain from crimes such as theft or extortion; spies intent on stealing classified or proprietary information used by government or private entities; nation-state warriors who develop capabilities and undertake cyber-attacks in support of a country's strategic objectives; "hacktivists" who perform cyber-attacks for nonmonetary reasons; and terrorists who engage in cyber-attacks as a form of non-state or state-sponsored warfare. These findings form the core of organizational cyber security plan, and the management has to focus its attention in mitigating the risk associated with the five categories of cyber-attack.

Cyber security risks are a constantly evolving threat to an organization's ability to achieve its objectives and deliver its core functions. According to Centre for protection of National Infrastructure (2016), Cyberspace lies at the heart of modern society; it influence our personal lives, our businesses and our essential services. Cyber security applies both to the public and the

private sector and spans a broad range of issues related to national security, whether through terrorism, crime or industrial espionage. Dinicu (2014), in his research articles on Cyber threats to national security also concurs that Security is not something given for sure, nor easy to obtain, especially in the current era of globalization, when actors present in the international environment have become much more diversified and the security threats seem to continually reinvent themselves.

Cyberspace was once just a way to communicate but now pretty much everything depends on it. Fischer (2015) points out that critical infrastructures such as energy, healthcare, banking, transportation and water are dependent on how well organization protect and secure the systems and the data that controls them. He further notes that Cyber security in the maritime industry is a major concern, due to a lack of security awareness or accountability while increasing use of new, sophisticated communications technologies raises the threat level to high. Sharma (2012) is of the view that with the potential for sensitive customer data leaks, it is important that security procedures and processes are in place so that operators know how to identify a potential security threat or have been trained to respond when a cyber-attack is in process.

According to Marco (2012), the perpetrators active in the maritime industry are mostly interested in financial gain, looking to gain access, stay hidden and extract financial profit from their targets. However, accessing and extracting sensitive information or intellectual property can also help criminal or terrorist organizations whose motive is to use the industry to transport hazardous materials or weapons. In an advanced threat, the attacker will spend a large amount of time researching a list of potential targets, gathering information about the organization's structure, clients etc.

Sharma (2012) is of the view that social media activity of the people in the target company will be monitored to extract information about the systems and forums favored by the user and any technology vulnerabilities assessed. Once a weakness is found the next step the hacker will take is to breach the cyber security perimeter - the basic security most companies adopt - and gain access, which, for most attackers, is easily done (Fischer, 2015). These are the aspect the management has to constantly deal with in their daily duties. Information security plans have

different weaknesses, risks, and countermeasures than physical security plans. When people look at information security, they conspire how a person may penetrate the network using unauthorized means through wireless, software exploits or open ports.

Understanding company security must begin with an understanding of the basic laws, regulations, and legal liability issues to which the company must adhere to protect the company and its assets, as well as the employees and customers. Security policies and procedures are official company communications that are created to ensure that a standard level of security guidelines exists across the entire organization (Mark and Anderson, 2009). These policies define how the employees interact with company computer systems to perform their job functions, how to protect the computer systems and their data, and how to service the company's clients properly.

An information security strategic plan can position an organization to mitigate, transfer, accept or avoid information risk related to people, processes and technologies. An established strategy also helps the organization adequately protect the confidentiality, integrity and availability of information. According to Evans (2015), in his article on the importance of Building and information security strategic plan, says the business benefits of an effective information security strategic plan are significant and can offer a competitive advantage. These may include complying with industry standards, avoiding a damaging security incident, sustaining the reputation of the business and supporting commitment to shareholders, customers, partners and suppliers.

Harris (2013), in his studies on information security governance and risk management argues that, if computer users were isolated from one another, computer security management would be straightforward and rely primarily on personnel background checks and padlocks. But the benefits of networking are too great to ignore. Modern organizations require Internet connectivity. The trick is to find the right balance between functionality, performance, and security. It is impossible to optimize the equilibrium with respect to all attacks. He furthers observes that an enormous amount of attention has been drawn to cyber security. For example, in 2002,

Microsoft advertised its Trustworthy Computing Initiative, declaring that security would henceforth be at the forefront of Window's development (Dinicu, 2014).

Kenneth (2011), in his articles on Strategic cyber security argues that, a strategic challenge for cyber defense is that the Internet evolves so quickly it is impossible for any organization to master all of the latest developments. Over time, attackers have subverted an ever-increasing number of operating systems, applications, and communications protocols. Defenders simply have too much technical ground to cover, which is to a hacker's advantage and places a premium on defensive creativity, good intelligence, and some level of automated attack detection and response.

According to Evans (2015), Security failings in today's information-driven economy can result in significant long term expense to the affected organizations management and substantially damage consumer trust and brand reputation. Sensitive customer information, intellectual property, and even the control of key machinery are increasingly at risk from cyber-attack. The targeting of electronic assets has the potential to make a material impact on the entire organization and possibly its partners.

The Australian National Cyber Security Centre in their report on cyber security and risk management (2013) observes that, the topic of cyber security needs to move from being in the domain of the IT professional to that of the Executive and Board, where its consideration and mitigation can be commensurate with the risk posed. The traditional approach to thinking about cyber security in terms of building bigger walls (firewalls and anti-virus software) - while still necessary - is no longer sufficient. The report further recommends that a holistic approach to cyber security risk management – across the organization, its network, supply chains and the larger ecosystem – is required.

Further research has shown that effective information systems are critical to the success of any organization. Center for protection of National infrastructure (2015) concluded that secure management of intellectual property and confidential or sensitive information provides competitive advantage and helps protect corporate reputation. This is true whether that

information is in the form of a product design, a manufacturing process, a negotiating strategy or sensitive personal data. At the same time, the need to access and share information more widely, using a broad range of connecting technologies, increases the risk of that information becoming compromised or misappropriated. Compromise of information through, for example, staff error or the deliberate actions of an outsider could have a permanent or at least long-term impact on an organization management. A single successful attack could have a devastating impact upon an organization's financial standing or reputation (Harris, 2013).

The strategic cyber security management literature emphasizes the importance of protecting organizational knowledge and information, especially in terms of maintaining competitive advantage. After synthesizing several mechanisms from the literature that organizations could deploy to protect their knowledge and information. An Australian field study (2016) investigated how and to what extent these mechanisms were deployed in 11 knowledge intensive organizations. The study revealed surprising findings: firstly, there was no evidence of a systematic and comprehensive management approach to the identification and protection of knowledge assets. Secondly, concerns about confidentiality of organizations' operational data (e.g., client details), often crowded out managerial attention to protecting organizations' own knowledge and information assets. As a result of this, Information compromise can lead to material financial loss through loss of productivity, loss of intellectual property, reputational damage, recovery costs, investigation time, and regulatory and legal costs.

According to the survey conducted by the GFI software on the business and social impacts of cyber security issues (2015), 47 per cent of the respondents have been victims of at least one cybercrime in the last one year. The key findings were that 41 per cent believe that banks will be the main target for cybercrimes while 23 per cent were concerned that business institution will be targeted for crime and cyber espionage. The research revealed that almost all cybercrimes have noticeable, detrimental impacts on business and the management as a whole, 88 per cent of those surveyed believed that a cyber-attack against an organization would have measurable financial and productivity implications and might put the organization out of business completely. The survey further revealed that cyber-attacks have profound consequences for the business community, organizations being as a target, or victim of the attack elsewhere.

2.3 Personnel Security Plans to the Organization Management

Personnel security plans focuses on employees, their access to their organization's assets, the risks they could pose and the adequacy of existing countermeasures. According to the Centre for the Protection of National Infrastructure, (2015), risk assessment is crucial in helping security and human resources managers, and other people involved in strategic risk decisions, communicate to senior managers the risks to which the organization is exposed.

Although many organisations regard personnel security as an issue resolved during the recruitment process, it is a discipline that needs to be maintained throughout a member of staff's time in employment. It should also include a formal process for managing staff leaving the business (Mark and Anderson, 2009). When applied consistently, personnel security measures not only reduce operational vulnerabilities, they can also help build a hugely beneficial security culture at every level of an organisation. Wilson (1990) established that robust personnel security helps organisations to employ reliable people; minimise the chances of staff becoming unreliable once they have been employed; detect suspicious behaviour and resolve security concerns once they emerge.

Mark and Anderson (2009) established that security planning process of the organizational management structure is the first step for management. In the planning phase, a manager sets goals for his department and defines the actions that must transpire to reach those goals. This phase may involve plans for revenue and expense management, inventory control, labor and regular daily tasks for the department. On the other hand, Bryson (2004) points out that managers use the security plans created in this process as a foundation for all other aspects of the organizational management system.

Wilson (1990) established that personnel security planning touches on the core values of the company management. Core values are the emotional engine that drives people and organizations forward. Being explicit about a strategic direction and how it links to the organization's core values and competencies helps everyone understand why the energy, focus, and costs are worth it. Values are the "how" an organization expects to conduct business

(Warner, 2002). When people understand the values that are at the heart of an organization, they have a better understanding of how to move toward realization of that vision.

The Security Awareness Program Special Interest Group (2014) denotes that one of the biggest risks to an organization's information security is often not a weakness in the technology control environment. Rather it is the action or inaction by employees and other personnel that can lead to security incidents—for example, through disclosure of information that could be used in a social engineering attack, not reporting observed unusual activity, accessing sensitive information unrelated to the user's role without following the proper procedures, and so on. It is therefore vital that organizations have a security awareness program in place to ensure employees are aware of the importance of protecting sensitive information, what they should do to handle information securely, and the risks of mishandling information.

Irwin (2014) argues that employees' understanding of the organizational and personal consequences of mishandling sensitive information is crucial to an organization's success. Examples of potential consequences may include penalties levied against the organization, reputational harm to the organization and employees, and impact to an employee's job. It is important to put potential organizational harm into perspective for personnel, detailing how such damage to the organization can affect their own roles.

For a company's security policies to be effective, they must be communicated properly to the employees to ensure companywide knowledge and compliance. Rules won't be followed if nobody knows they exist (Mark and Anderson, 2009). Many companies make use of consultants to create and draft security policies and procedures, but these policies often aren't communicated to the user community and aren't used. Employees need to be aware of security issues and procedures to protect not only themselves but also the company's services and data.

2.4 The Physical Security Plans to Organization Management

Harris (2013) established that physical security is often a second thought when it comes to information security. Since physical security has technical and administrative elements, it is often overlooked because most organizations focus on technology-oriented security countermeasures to prevent hacking attacks. Hacking into network systems is not the only way that sensitive information can be stolen or used against an organization.

Oriyano (2014) points out that physical security plans must be implemented correctly to prevent attackers from gaining physical access and take what they want. The challenges of implementing physical security plans are much more problematic now than in previous decades. The strategies to protect the organization's assets need to have a layered approach. It is harder for an attacker to reach their objective when multiple layers have to be bypassed to access a resource. Physical security plans over past decades has become increasingly more difficult for organizations.

Harris (2013) established that physical security measures aim to either prevent a direct assault on premises or reduce the potential damage and injuries that can be inflicted should an incident occur. For most organisations the recommended response will involve a sensible mix of general good housekeeping alongside appropriate investments in CCTV, intruder alarms and lighting that deter as well as detect – measures that will also protect against other criminal acts such as theft and vandalism and address general health and safety concerns (Centre for protection of national infrastructure, 2010). In some locations these measures may already be in place to some degree. However, external and internal threats to organisations (and their staff) will constantly evolve and so all procedures and technology should be kept under constant review.

According to Sekomo (2013), physical security policies are the first line defense for any organization. To provide effective security, security policy and procedure creation must begin at the top of an organization with senior management. These policies and procedures must then flow throughout the company to ensure that security is useful and functional at every level of the organization. To protect their assets, employees, and customers from security risks, organizations must analyze their security practices to identify the threats to their operations and protect themselves in the most cost-efficient way.

The concerns that come up with the growth of ports include theft of cargo, piracy, and acts of terrorism. David (2005), argued that to protect the organizational assets, employees, and customers from security risks, organizations must analyze their security practices to identify the threats to their operations and protect themselves in the most cost-efficient way. This is actually in line with the international best practices.

The International Ship and Port Facility Security (ISPS) Code, which came into force in 2004, prescribes responsibilities to governments, shipping companies, shipboard personnel, and port/facility personnel to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade. The International Maritime Organization's (IMO) ISPS Code applies to facilities serving cargo ships and it is the duty of governments to determine that port facilities comply with the code (Sekomo, 2013).

However, it is the duty of port authorities to ensure real compliance. One cannot talk about port security in Africa without mentioning the Horn of Africa. Piracy off the coast of Somalia escalated in 2008 causing significant disruption to the maritime industry resulting in the need to increase security in African waters (African Center for Strategic studies, 2009).

African ports are unhappy about plans to introduce a stringent new security system aimed at checking cargo being shipped into and from the United States. African authorities describe it as another burden for cash-strapped economies. The Maritime Transportation Security Act passed in the U.S. House and Senate, requires an assessment of security at foreign ports, and it allows the U.S. to block entry to vessels arriving from foreign ports that are found to lack effective anti-terrorism measures. U.S.-bound freight containers are expected to go through a tracking, identification and screening system, and foreign ports must enforce steps including restricting access to security-sensitive areas, background checks and the issue of security identification cards (CNSNews.com, 2008).

Elsewhere others have voiced concern that piracy activities have severely affected trade and tourism sectors. The Tanzania People's Defence Forces has claimed that the flow of cargo ships at the Dar es Salaam Port has also been affected since pirates invaded the region in 2005. Data from the Tanzania Port Authority (TPA) shipping traffic department has highlighted a marked drop in vessels making port calls. Now of course global trade itself has changed since 2005, but with Africa considered a new hope for investment it seems that security has played almost as much a role in this drop as the global recession (African Center for Strategic studies, 2009).

Port operators around the continent have not idly stood by but have strongly and vociferously voiced their concerns. Back in 2010 the Executive Secretary of Pan African Association of Ports Cooperation (PAPC) termed piracy as "a cankerworm that grossly militates against the growth of ports' operations". It seems the ensuing years have done little to change this view. The most obvious security issues have affected general and bulk cargoes, but the Somali piracy problem has also had a significant effect on cruise traffic. This has been particularly damaging to East Africa, as countries such as Kenya and Tanzania see tourism as a tool to drive further investment and bring revenue into the countries (Tommy, 2013).

Having lawless bandits operating off the coast looking to attack cruise ships or grabbing tourists from the beaches is far from ideal for any country. Then there is the issue of offshore exploration – it appears that the Somali basin is ripe for oil and gas exploration, however this is another major industry which is expressing concerns about the security risks in the region. Investing billions of dollars into a drilling program, only to see it ruined by Somali pirates is not something which the oil majors can contemplate (Bandari, 2010).

Oriyano (2014) re affirms that the physical element of security is often overlooked. The theft of hardware or vandalism could occur while working with administrative and technical controls. Organizations often focus on technical and administrative controls and as a result, breaches may not be discovered right away. Security professionals with physical security in mind are concerned about the physical entrance of a building or environment and what damages that person may cause.

Looking at the East Africa scenario and Kenya in particular, the Kenya Maritime Authority was established in June 2004 to regulate, co-ordinate, and oversee all maritime affairs in Kenya. The Authority holds that terrorism, maritime piracy, and armed robbery; arms trafficking; narcotics trafficking; human trafficking; illegal, unreported, and unregulated fishing; illegal immigration; and marine pollution are crimes that, if not put under control, may flourish and undermine the political stability and economic development of the region (Bandari, 2010). Mombasa is Kenya's principal port through which international seaborne trade is routed; it is also the economic lifeline of the rich agriculture hinterland countries of Uganda, Rwanda, Burundi, Democratic Republic of Congo, northern Tanzania, Southern Sudan, and Somalia. Consequently, port

authorities regularly update port security measures in compliance with the ISPS Code (African Center for Strategic studies, 2009).

Reports indicate that since the Kenya Ports Authority started implementing the IMO anti-terrorism inspired measures, crime incidents at the port have been reduced by 85 per cent. Kenya has formulated a national strategy on anti-terrorism, enacted maritime security legislation, and conducted security assessment at the port. Kenya is one of the countries in Africa that is rising to the challenges of security in the maritime industry. African countries are trying to take a leading role but still need international support especially due to general instability in some regions and the lack of maritime capacity. Through close dialogue, countries in Africa are forging partnerships and building positive relationships that will enhance maritime security on the continent (African Center for Strategic studies, 2009).

According to Tommy (2013), the major factors affecting port dwell and performance time as revealed by the survey conducted by International Peace Information Service and Trans Arms-Research include the following: System reliability for ports and customs authorities which is affecting the passing of customs entries and issuance of release orders, rigidity of the clearance process means that any errors in declarations and manifests are heavily punished as shippers who complete a form for rectifying such errors have to content with an average 7 days to have their entries passed, at which point their cargo has already started to incur storage and demurrage charges.

2.5. Study Gap

Despite the fact that the number of studies measuring ports performance is flourishing, several deficiencies still exist. The vast majority of the studies have a specific focus towards the assessment of operations productivity, in order to conclude on port efficiency. According to Mangan and Cunningham (2001), it has been argued that improved performance is partly due to revised handling procedures and focused management strategies as a result of private participation. Security personnel, operators, and all organization personnel including the management should be familiar with the information and procedures associated with the Security Plans put in place. Studies have been carried out relating to the organization management of Kenya Ports Authority but none of them has sufficiently focused on how of security plans

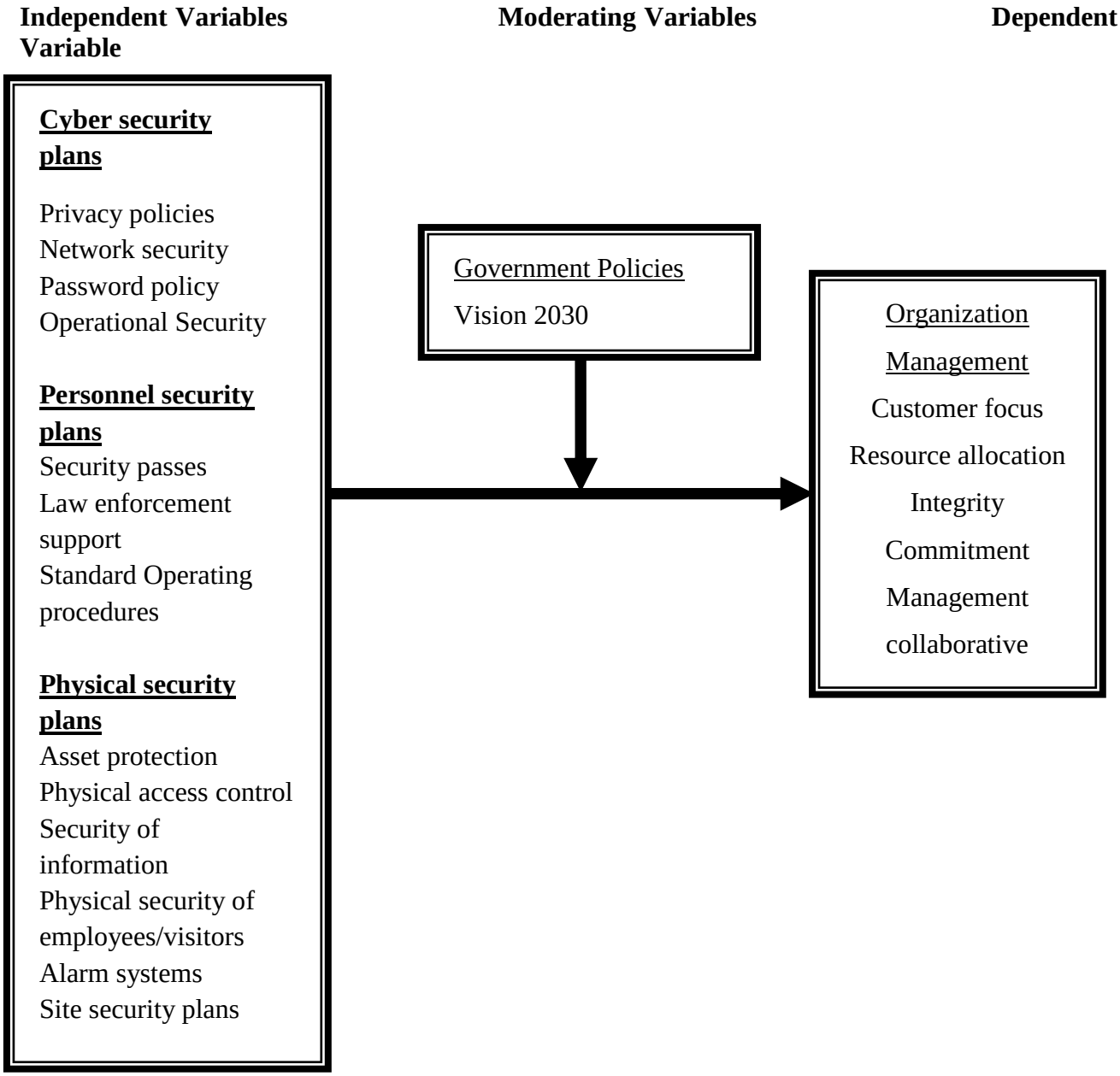
influence organization management. What change has the strategic security plans brought to the organization management at the Kenya ports authority? What relationship exists between the different security plans with the organization management? This study seeks to address the influence of strategic security plans to organization management.

The studies have focused on effectiveness of strategic management, structural implication in strategic implementation, logistical challenges at the Kenya ports authority, privatization of the ports and its socio-economic impacts among other. But the growing security challenges in the recent parts has had the management change their way of thinking and thus security plans of the organization effect the management of the port in a way or the other. This paper focuses its attention on the influence of strategic security plans to the organization management with focus on the Kenya ports authority.

2.6 Conceptual Framework

Strategic security planning ensures that resources, decision making, and activities are aligned with the common goal of the institution. Assessing goal attainment however does not necessarily reveal whether the institution is having the impact it wants or needs to have. For that, the institution needs to examine its actual outcomes or results. The chart illustrates the conceptual framework for organizational management, the relationship between the independent variables and dependent variables.

Figure 2.6: Showing the Model of program impact



Source: Johns Hopkins University

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the methodology that was used to gather and analysis data. First it describes the study area where the focus of the research was conducted and with an account of the methods applied in carrying out the research study. It is organized under the following sections: study area, research design, data collection, data analysis and ethical considerations.

3.2 The Study Area.

The Kenya Ports Authority (KPA) is a state corporation charged with the responsibility of managing the Port of Mombasa, and all other ports along the Kenyan coastline. KPA is one of the leading parastatals in the Country and a major facilitator of sea-borne trade within the East and Central African region. (www.kpa.co.ke).

KPA envisions itself to be World class seaports of choice with a mission of facilitating and promoting global maritime trade through provision of competitive port services. To achieve these vision and mission, KPA is guided by five key objectives which include: improving managerial, operational and financial performance; developing, maintaining and sustaining port facilities and infrastructure to meet the customer needs; promoting the Port of Mombasa as a primary gateway to the great lakes region and also serve the horn of Africa; maintaining and promoting a clean, safe working and rewarding environment; integrating the functionality of the Port of Mombasa in the development vision of the republic of Kenya and the region; and instilling sound corporate governance practice(www.kpa.co.ke).

3.3 KPA Strategic Security Plan.

KPA strategic security plan has been developed to mitigate the emerging security challenges facing the organization. Security planning is one of the core functions of strategic management, which outlines the KPA's security goals and ways to achieve them. KPA strategic security plans provides the basis for all management decisions, functions of the organization, motivation, and control which are focused on the formulation of strategic plans towards achieving its vision. The strategic security plan is composed of three main components each with its own objective. The components include the cyber security, personnel security and physical security plans.

The cyber security plan at KPA is composed of several sections namely: Policy development and management, Privacy and Data security, Scams and Fraud, Network Security, Website Security, Email, Mobile devices and Employees, Facility Security, Operational Security, Payment Cards, Incident response and reporting,. Under the policy development and management, the cyber security plan outlines the security roles and responsibilities of each department, the employee's internet usage policy, the social media policy and potential reputation risks within KPA. Network security section outlines the secure internal networks and clouds, the KPA password polices, encryption policy, web browsing rules and remote access policy. The incident response and reporting section, outlines how the employees are to behave in the event of breach of cyber security. The operation security outlines how to identify critical information within KPA network and website, analyze the threat and vulnerabilities, and assesses the risks and how to apply counter measures to mitigate the risks.

The personnel security plan within the strategic security plans mainly deals with employee hiring and security of assets. The personnel security sub section contains five sections namely: Personnel hiring and vetting, Background checks and credentials, Third party engagement policy, access control for the employees and security training for KPA employees. The Security training focuses on understanding and complying with policies and procedures, training on rules and behaviors for the systems and applications to which they have access to, working with management to meet the training needs and being aware of action to take to better protect KPA information.

The physical security plan of KPA is divided into five sections, namely: purpose, the responsibilities of different departments, policies established by KPA, access control measures and security aids. The responsibility section, list the persons responsible for physical security and what their specific responsibilities related to physical security of the installations or facility. The policies section outlines the area security which defines the areas, buildings and other structures considered critical and establishes priority for protection, and the four categories of security levels within KPA. Section four states the access control measures within KPA which include personnel access, Material control and vehicle control. While section five provides the security aids installed within KPA perimeter such as CCTV, Barriers and Intrusion Detection systems (IDS).

3.4 Research Design

This study adopted a case study design meant to investigate the of strategic security plans adopted by Kenya Ports Authority on organizational management. Kothari (2000) define a case study as a description of a situation involving problems to be solved. A case study is also an in-depth investigation of an individual, group, institution or phenomenon (Mugenda &Mugenda, 2003).The study chose to use a case study because of its ability to collect in-depth information on a subject because case studies are more detailed.

3.5 Target Population and Sample Size

The choice of study area was purposive because Kenya Ports Authority is a complex organization which therefore requires the management to adopt and implement effective security plans. Kenya Ports Authority has 32 departments with 7 division heads. This formed a target population of 39 as shown in annex A. On the other hand, purposive sampling was further used to select key respondents for structured interviews. This is because they were deemed to possess the relevant information that the study seeks to get.

3.6 Methods of data Collection

The study used primary data. The primary data was collected on the influence of strategic security plans adopted by Kenya Ports Authority in transforming the Port into a world – class sea port. The primary data was collected using questionnaires and interview guides. Interviewing was chosen for it allows for flexibility in the direction of question hence comprehensive data collection is ensured and the interviewer can direct the interviewees in case of difficulty in answering a question. Structured interviews were used to collected information from key respondents.

The researcher used one research assistant who assisted in collecting data by distributing and later picking the duly filled questionnaires. The main advantage of the instrument was that it allowed the researcher to control and focus responses to the research objectives. Thus, enhancing relevancy of data collected.

3.7 Data Analysis Procedures

The data obtained from the questionnaires and interview guide was analyzed using content analysis. Nachmias and Nachmias (1996) define content analysis as any technique used to make inferences through systematic and objective identification of specified characteristics of messages. Kothari (2004) explains content analysis as the analysis of the contents of documentary and verbal material, and describes it as a qualitative analysis concerning the general import of message of the existing documents and measure frequency. The researcher analyzed the information provided by the respondents against known strategic management concepts and implementation models to describe and determine the influence of strategic security plans developed by Kenya Ports Authority on its management. Content analysis also enabled the researcher to identify, interpret and make a scholarly judgment.

3.8 Validity and Reliability of Data Collection Instruments

3.8.1 Validity

Validity refers to the degree to which results obtained from the analysis of the data actually represent the phenomenon under study (Mugenda and Mugenda , 2003). To determine and improve the validity of the questionnaires, a pilot study was carried out with 7 questionnaires from a different organization other than KPA. The researcher then corrected ambiguity of questions with the assistance of the supervisors. This allows the preparation of the final questionnaire.

3.8.2 Reliability

The reliability of the questionnaires' test refers to the ability of that test to consistently yield the same results when repeated measurements are taken of the same individual under the same conditions. To test reliability, the researcher will use test re-test method after which a reliability index will be noted before data collection processes commence.

3.9 Ethical Considerations

Permission to carry out the study was sought from the management of the Kenya Ports Authority and from the respondents themselves. The nature and the purpose of the research were explained to the respondents by the researcher. The researcher respected the individuals' rights to safeguard their personal integrity. During the course of the data collection, the respondents were assured of

anonymity, confidentiality and they were assured also of their ability to withdraw from the study at any time if they want to do so. No names or personal identification numbers were reflected on the questionnaires except the numbering for questionnaires, which was for the purposes of identification of data during data editing. The results of the study would be availed to the KPA management and to those participants who are interested in knowing the results. All participants in the study were provided with an informed consent form which they all agreed and signed.

CHAPTER FOUR: FINDINGS AND DATA ANALYSIS

4.1 Introduction

This chapter presented analysis and findings of the study as set out in the research objectives and methodology. The results are presented on the influence strategic security plans adopted by Kenya Ports Authority management. The data was gathered exclusively from questionnaires and interview guides as the main research instrument which was designed in line with the objective of the study. The study targeted the 32 departmental heads and 7 divisional heads at KPA out of which 26 departmental heads responded to the questionnaires and 4 divisional heads scheduled interviews and provided responses used to complete this study, giving a response rate of 76.9%. This commendable response rate was made a reality after the researcher made personal visits to book appointment for the interview and remind them of the timings. This response rate was excellent and conforms to Mugenda and Mugenda (1999) stipulation that a response rate of 50% is adequate for analysis and reporting; a rate of 60% is good and a response rate of 70% and over is excellent

4.2 General Information

The study sought to establish the number of years that the interviewees had worked at KPA, the study established the respondents that had worked at KPA for the longest time was there for 15years while the respondents that had worked at KPA for the least period of time had been there for 3 years. This shows that the respondents were credible enough to give sufficient information on the research topic. On the role that the interviewees play in strategic security plan formulation the study established that they drafted the initial strategy draft at departmental level.

The study sought to determine how is the process of setting goals, objectives and milestones undertaken at KPA. It was established that every department undertakes its goals (internal targets) and the government sets its goals for KPA too. On how the feedback mechanism in monitoring the achievement of the strategic security goals and objectives conducted, the study found out that KPA has a balanced scorecard tool kit that performs this function and the government has introduced performance contracting and annual reviews which monitor performance at KPA.

4.3 The strategic security plans formulation within the authority

The study sought to establish the one in charge of strategic security plans formulation and implementation in the Kenya Ports Authority. It was established that most respondents (53%) stated that it was the divisional heads that are in charge of strategic security plans formulation and implementation in the authority, 30% stated that it was the heads of departments while 17% said it was all managers who are involved in the strategic security plans formulation and implementation. However, it should be noted that some respondents gave more than one response and therefore the n-value here was more than the sample size. Table 4.1 below presents the study findings on the strategic security plans formulation and implementation.

Table 4.1: Participation in strategic security formulation

Heads	**Departmental Heads**	**Divisional Heads**	**All Managers**
No. of Respondents	**9**	**16**	**5**

Source: Survey Data 2016

The study established that the formulation of the strategic security plan at the KPA is the responsibility of the divisional heads with consultation of the departmental heads. The division heads spearhead the process of the development of the various security plans within their respective divisions in line with the organizations goals and objectives. The departmental heads produce the draft of the security plans and have it approved by the divisional heads. However, the cyber security plans are developed by the corporate service division, with the Information Technology (IT) department being the lead in formulation of the plans. The safety and security department also support the IT department in formulation and implementation of the cyber security plans.

In public sector organizations, however, those in executive positions often have their powers constrained by statute and regulation which predetermine, to various degrees, not only the very purpose of the organization but also their levels of freedom to make strategic security decision that would affect the organization behavior and performance.

4.4 Strategic Plans Adopted and Challenges Faced within the Organization

The interviewees outlined some of the strategies that KPA has adopted in its quest to achieve world class standards. These strategies included benchmarking how best performing port operate, carry out comprehensive port improvement planning, preparation of port master plan, high level organization structuring, Cargo handling equipment improvement, Investment in IT both in operations and port security, Licensing of Container freight stations (CFS) to improve capacity of cargo storage, Capacity expansion – additional berth and Stakeholder consultation.

The study sought to establish the challenges that KPA faced in the adoption of strategic security plans. These challenges included, Resistance to change, Political interference, financial constraints, Changes in technology and the Government bureaucracy which causes delay in implementation of strategic security plans. In order to improve the speed with which these strategies are implemented, change of regulatory framework which may involve the review of KPA Act to streamline the Act with vision 2030.Secondly they ought to engage in seeking external funding from Trademark East Africa, World Bank, JICA over and above income generated by the company and finally there is need to Involve internal stakeholders.

The study established that KPA made use of information technology in its operations through automation of all their process, System application program (SAP), Integrated security services (ISS), Vessel Traffic Management Information System (VTMIS) and IP Telephony. By automating all its operations KPA has become paperless, linkage with KRA, clearance of cargo is on-line/automated. Internally all the modules are automated finance. The study found out that KPA benchmarked its services to other world class ports – port of Singapore, Shanghai, and Durban. Further the interviewees indicated that KPA has achieved certifications including – International safety management (ISM), ISO, Lloyds Certification for the marine craft NEMA, ISPS.

4.5 Situational Analysis is Done before a Strategic Security Plan is Formulated

Furthermore, when respondents were asked to state whether situational analysis is done before a strategy is formulated, (89%) of the respondent confirmed that Kenya ports authority conducts a situational analysis before formulation of its strategic security plans while 11% pointed out that much of the information needed for formulation of the security plans is learned over time with

the changing operating environment. Table 4.2 below presents the findings on weather situational Analysis is conducted before formulation of strategic security plans.

Table 4.2: Situational Analysis done before formulation of Security plans.

Heads	**YES**	**NO**	**NOT SURE**
No. of Respondents	**26**	**4**	**0**

Source: Survey Data 2016

Before formulation of any strategy, it is prudent that an assessment on the ground is done. This is to allow the identification of areas that need improvement and for the management to know the kind of security strategy that fits the situation at hand.

4.6 The influence of Cyber Security Plans to organization management

The first objective of the study was to determine the impacts of cyber security plans to the organization management at Kenya Port Authority. This objective was measured by analyzing the cyber security plans developed, the challenges of cyber security to the organization and the influence of this cyber security to the management of the KPA as an organization.

4.6.1 KPA cyber security challenges

On some of the cyber challenges KPA is facing, 27% of the respondents said that employees of the organization are the greatest challenge in managing cyber security. The study established that employees are the major risk since there are high chances of security breaches done by employees in their day to day activities. The study also established that closely followed by employees are the cyber criminals and hackers who want to steal or sabotage KPA. This was represented by 24% on cyber criminals and 20% on cyber hackers. It was further established that terrorism was also another major challenge to KPA as this was represented by 17% of the respondents. Table 4.3 shows the security challenges that KPA is exposed to.

Table: 4.3: The Cyber security challenges facing KPA

Cyber Threats	Hackers	Terrorism	Employees	Criminals	Competitors
No. of Respondents	6	5	8	7	4
Percentage	20%	17%	27%	24%	12%

Source: Survey Data 2016

Those respondents from the KPA security and IT departments noted that many attempts to compromise information involve what is known as the skillful manipulation of people and human nature. They said that it is often easier to trick someone into clicking on a malicious link in an email that they think is from a friend or colleague than it is to hack into a system, particularly if the recipient of the email is busy or distracted.

Respondents noted that there are also many well documented cases of hackers persuading IT support staff to open up areas of a network or reset passwords, simply by masquerading as someone trusted. Such threats pose a challenge to the Kenya ports authority management as they try to come up with policies and plans to curb cyber-crimes within the organization.

4.6.2: Cyber Security Plans adopted by the organization.

On the cyber security plans, the respondent were to state some of the security plans that have been adopted in the Kenya ports authority. From the respondents there were three main cyber security policies that have been adopted and this include regulatory (These policies are cyber security policies that KPA must implement due to compliance, regulation, or other legal requirements), advisory (policies that strongly advises employees on the behaviors and activities which should not take place within the organization), and informative cyber security policies (policies that exist simply to inform the employees and the KPA customers).

On network security policies the respondent were asked to state whether the KPA as an organization has in place network security policies for its management and employees at various departments. It was established that 80% of the respondent confirmed that there are strong network policies for the management and even other employees such as password policies and

levels of access. While 20% of the respondents noted that network security policies have not been adopted within the organization especially with the current security threats that the organization is facing. In this case, the study established that the organization is taking too long to develop and implement security policies to curb much of the cyber threats available within their operating environment. Table 4.4 below shows the response on cyber security plans adopted by the KPA. They respondent also stated that the management have put in place an integrated security management systems that is meant to track all security related incidences with the organization.

Table 4.4: Cyber Security Plans adopted by the organization

Heads	YES	NO	NOT SURE
No. of Respondents	24	6	0

Source: Survey Data 2016

Cyber security has never been more essential, for various reasons. The management noted that KPA have more digital assets than it had 10 years ago, and these assets are worth more than they were before. They include customers' personal, financial and transaction information; proprietary assets, including source code for products; automated business processes; sensitive communications with suppliers and partners; and other data. The security around these assets varies greatly depending upon the perceived (as opposed to the actual) financial and strategic value to the business, as well as the effectiveness of the security technologies and processes in place.

4.6.3 Trends of organization cyber security plans review

On the trends of the organizational change of cyber security plans, it was established that the cyber security plans have been increasing with 62% confirming that for the last four years, the organization has been reviewing the plans yearly to accommodate the new emerging security challenges. However, 13% of the respondents were of the opinion that cyber security plans have been stagnant and little has been done to improve the plans for a period of about three years, this group of respondents cited the increase in hackers in cyber space and that the organization has to

tighten its cyber security so that they do not fall into this trap. Figure 4.1 summarizes the findings on trends of organization change in cyber security plans within KPA.

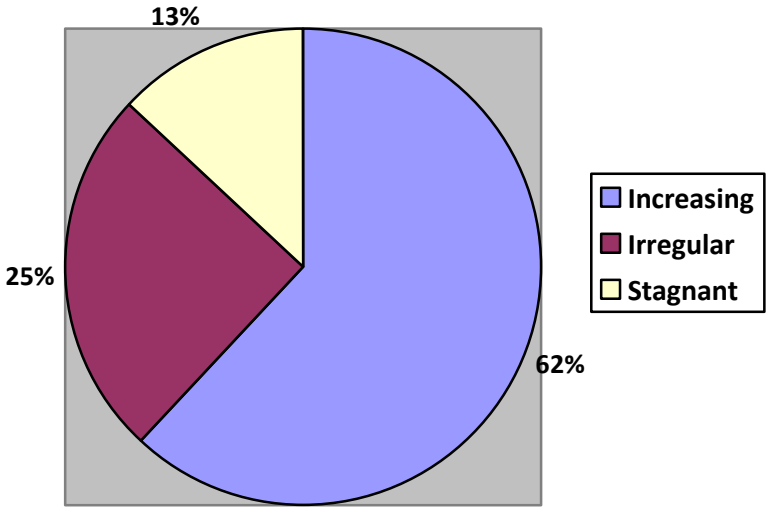
The other 25% of the respondents noted that though there have been changes in the cyber security plans but the changes or updates have been done irregularly. This group of management said that the policies have given powers to only one department to update security plans but other organization have lagged behind or it's because of ignorance.

Table 4.5: Trends of Organization Cyber Security Plans

Trends	Increasing	Irregular	Stagnant	Decreasing
No. of Respondents	32	13	6	0

Source: Survey Data 2016

Figure 4.1: Trends of Organization Cyber Security Plans



4.6.4 Influence of Cyber security plans to overall organization management

The research sought to establish there has been difference in cyber security within KPA after the cyber security plans were adopted by the organization. 83% of the respondents said that since the introduction of the cyber security plans in the organization, most of the cyber-crimes have tremendous reduced and that this is attributed to the introduction of cyber security plans in place. 17% of the respondent noted that despite there are numerous cyber security plans within the

organization. Table 4.6 below shows the respondents feedback on change in cyber-crimes at KPA.

Table 4.6: Change in cyber-crimes within KPA

Heads	**YES**	**NO**	**NOT SURE**
No. of Respondents	**24**	**6**	**0**

Source: Survey Data 2016

In addition, when respondents were asked to state whether KPA has developed a set of key performance indicators or some other form of accountability to track the success of cyber security initiatives, majority (73%) agreed while only 17% of the respondents denied the statement. This therefore implies that some managers are not aware of the performance indicators put in place to monitor the success of cyber security plan initiatives. It is therefore a challenge for the top management and administration to ensure that performance indicators are made known to all managers as well as other stakeholders in order to promote the organization's cohesiveness. Table 4.7 below summarizes the findings on development of performance indicators for cyber security within KPA.

Table 4.7: Development performance indicators for cyber security plans

Performance Indicators	Yes	No	Not sure
Respondents	22	5	3
Percentage	73%	17%	10%

Source: Survey Data 2016

The study established that KPA is having a tougher time mitigating cyber security breaches, and average financial impact of each breach on the organization is increasing. Often, clients or regulatory agencies require KPA to disclose breaches; in other cases, attackers themselves distribute the pilfered information online. In many cases, the consequences on KPA have been devastating in terms of lost revenue, impugned reputations and financial repercussions. The immediate consequences for a KPA dealing with a customer data breach are severe and may include negative press, the threat of lawsuits from customers and partners, and long legal investigations.

4.7 The Influence of Personnel Security plans on Organization Management

The second objective of the study was to determine how personnel security plans affect organization management at Kenya Ports Authority. This was assessed through both closed and open ended questions as well as structured interviews to key respondents. The objective was measured by determining the personnel security challenges facing KPA, determining the kind of personnel security plans adopted by KPA and what have been the impacts of these personnel security plans on the management of KPA.

4.7.1 The personnel security challenges in KPA

KPA faces a number of challenges concerning personnel security. Majority of the responded focused their answers on four key aspect that pose a great challenge to the organization as with regard to personnel security measures as shown in table 4.8 below.

Table 4.8: Personnel security changes in KPA

Personnel Security challenges	Recruitment	Staffing	Data control	Large Numbers (customers)
No. of Respondents	28	26	29	27

Source: Survey Data 2016

The study established that recruitment process is one of the biggest security challenges to the management of KPA. The respondents interviewed and the response from the questionnaires showed that 90% of the respondents reaffirmed that recruitment is the biggest challenge to the management. In this case the organization places itself at risk in employing persons with different motives such as spies and persons with malicious intent.

The study also established that KPA as an organization has a large number of workers who are not directly employed by the organization but work there on behalf of other secondary organizations such as clearing and forwarding companies. The shipping companies as well have a large work pool of personnel working within the organization. This has posed a security challenge to the organization given that, identification of such a large workforce at sometimes is difficult.

It was also established that staffing of security personnel has posed a challenge in KPA. Staffing with access control of personnel within the KPA has been mentioned by the responded as a challenge to the management. The staffing of personnel from different background and different specialty in the implementation of personnel security plans has affected personnel relationship especially with management and the employees.

4.7.2 Personnel security plans adopted within the organization

The study established that the departmental heads had adopted vetting of personnel especially the newly employed personnel while some respondents also confirmed that vetting has been there but the most current personnel security plans is the personnel supervision and accountability by the division heads and departmental heads. Table 4.9 below shows the respondents rating on a scale of 1-5 on the personnel plans adapted by KPA (1 being the lowest and 5 being the highest).

The respondents pointed out that background screening for candidates or employees whose job responsibilities require that they have elevated system user privileges or access to sensitive and confidential information.

Table 4.9: Personnel security plans adopted by KPA

Personnel Security strategies within KPA	**Rating (1-5)**
Personnel Vetting	5
Personnel supervision	4
Screening procedures for new personnel and visitors	4
Law enforcement agency cooperation	4
Third party provider rules and regulations	5
Movement control within KPA	3

Source: Survey Data 2016

It was also established that testing and background screening to determine or validate a candidate's qualifications, past performance and appropriateness for a particular position is part of the policies that have been developed by KPA. They further stated that the organization should define the conditions where initial screening in required, conditions requiring rescreening, and the frequency of such re-screening.

On the availability of other law enforcement agencies, all respondents confirmed that there are other agencies assisting and working together with the organization in enforcement of the personnel security plans. The management confirmed that in matters of security management they require other agencies to assist in safeguarding there personnel and this influence on how they make their decision. The respondents further noted that the organizations have established personnel security requirements, including security roles and responsibilities, for third-party providers. This includes, for example, contractors and other organizations providing services, outsourced applications, and network security management.

It was also established that all employees are given identification numbers and staff numbers for ease of identification while in various offices. The overall use of personally identifiable information has not changed with the introduction of the ISMS update. These security risks within the Kenya ports authority are mitigated by the same measures that were outlined in the cyber security controls above. The study established from the interviews that KPA has developed, disseminated, and constantly reviewed, documented personnel security policy and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with recommended safeguards pertaining to personnel security. These responsibilities are outlined in the standard operating procedures of the KPA.

4.7.3 Personnel Security Influence on the KPA management

With the introduction of the strict vetting measures in the recruitment stages, the confidence level between the management and the employees has gone high since they have embraced the values of KPA. There are three areas that were noted that the organization management needs to focus on. This involves the people side of the issue and the summery of the response is as shown in table 4.10.

Table 4.10: The influence of personnel security plans on KPA management.

Management element	Commitment	Integrity	Transparency
% of respondents strongly agree	77%	83%	68%
% of respondents agree	23%	17%	32%

Source: Survey Data 2016

The study established that based on the personnel security plans that have been established and in light with the security challenges facing KPA, there has been improved organization commitment by the management. From the questionnaires, 77% of the respondents noted that physical security plan is so diffused and impacts everyone, the KPA management has taken into count on all employees to play multiple roles in ensuring safety and security within the KPA. However, 23% of the respondents observed that employees' have become vigilant in observing risks within the organization premises and then report what they see to the proper contacts.

Personnel security measures also have brought the issue of integrity to question. The study established that 83 % of the respondents were of the opinion that even if employees are willing to play a role in aiding the organization's physical security plans, they may find it too confusing to do so. There has been noted improvement on the integrity of the KPA management since it is observed that is their responsibilities in formulation and implementation of such security measures. While 17% of the respondents noted that of coherence among the various internal departments have improved and there is a key role played by each department in the improvement of the overall performance of KPA management.

The study established that personnel security plans have brought about transparency in management and implementation of various security strategies. Among the respondents, 68% observed that, personnel security matters are managed in a visible manner and that it has contributed to the improvement of organization's culture. Only the 32 % of the respondents were uncertain how transparency in matters of personnel security affect the management since they were of the opinion that matters to do with security is a collective responsibility.

The study established that the issues relating to personnel security plan at KPA is the most challenging to KPA management. Interviewees indicated that in a culture where employees feel

disgruntled, apathetic, confused, ignored and disengaged, policies and procedures concerning facilities and security will be ineffective and this has led to increased theft and smuggling of goods within the KPA. It's not surprising that most respondents were reluctant to comment of personnel security plans of the organization, given the complexity of the challenges faced by the organization.

4.8 The Influence of physical security plans on organization management

The third objective sought to assess how the physical security plans affect the overall organization management. This was assessed by looking how the adequate physical security measures and asset identification measure are in protection of the organization assets. The researcher also assessed how the surveillance system impact on the leaders in effective management of the port and assessing the organizational awareness of the physical security plans as well as how they impact on management of the port. This objective was mainly measured through observation and structured interviews on specific key responders.

4.8.1 Physical security challenges faced by the KPA

There are various aspects of physical security that the port has to contend with and this 85% of the respondents noted that the growing volume of containerized maritime trade also provides opportunities for smuggling illicit drugs and the precursor chemicals used in the manufacture of drugs such as cocaine and heroin. Concealment of illicit shipments manifested as legitimate commercial cargoes, and diversion of legal chemicals following legitimate transactions by unscrupulous shippers is a problem. Table 4.11: shows some of the challenges KPA face in its day to day operations.

Table 4.11: Physical challenges to KPA

S/No.	Physical security challenge	Rating (Scale of 1-5)
1	Smuggling of Cargo	5
2	Theft of KPA assets and Cargo	3
3	Vandalism of the KPA properties	2
4	Fire Risks	2
5	Environmental Failures	1
6	Physical Intrusion	4
7	Terrorism	4

Source: Survey Data 2016.

When asked on a scale of 1-5, to rate the physical security challenges to the organization. The study established that KPA has both internal and external challenges and this emanate for the employees. The study revealed that employees are considered internal threats and can utilize their knowledge of building layouts and where assets are located to steal or vandalize assets. It was also established that at KPA employees have the ability to gain access to areas unobserved because of their job duties. The study established that predicting attacks from insiders is difficult for KPA to detect because of their access permissions.

The study also established that fire, water, and environmental failures are also internal threats. An example of insider threat that was given by the KPA safety department could be a security guard working off hours with access into all areas decides to commit crimes without alarming other employees. The study also established that employees should have background checks conducted when hired to protect KPA assets. Government agencies and organizations that work with them have access to classified data.

4.8.2 Physical Security Measures adopted by KPA

To determine the kind of physical security have been put in place, observation method was used to gather information. The physical security plans adopted by the KPA include the installation of the Electric Perimeter fence, security lighting within the compound, and installation of CCTV Cameras within the office premises and along the fences as well as at strategic location. The construction of automation systems at the entry points, electrically operated gates and barriers at the entry points. All this is controlled from one central room and other secondary central station which are managed by different level of managers. Figure 4.2 below shows the automated gate A at KPA.

Figure 4.2: Automation of access control at Gate A

The study established that if the equipment is relocated without approval, intrusion detection systems (IDSs) can monitor and notify of unauthorized entries. IDSs are essential to security because the systems can send a warning if a specific event occurs or if access was attempted at an unusual time. KPA Guards are a significant part of an intrusion detection system because they are more adaptable than other security aspects. It was further established that security officers are fixed at one location or make rounds patrolling the premises. While making rounds, guards can verify doors and windows are locked, and vaults are protected. KPA Guards are accountable for watching IDSs and CCTVs and can react to suspicious activity. They can call for backup or local police to help capture a suspect if necessary.

The study also established that KPA has automated its access point and also installed screening equipment at the main entrance. There are security cameras at the main entrance, security lights, traffic lights as well as physical security personnel in collaboration with the Kenya police. There are also physical barriers at the main entrance to control movement of vehicles and personnel with clearly marked signs. Figure 4.3 shows the access gate to the KPA

Figure 4.3: Main entrance to Gate A at KPA

The study found out that the automation of the access points have a direct bearing on employee and visitor's behavior as they enter or exit from the port. Obstacles have been placed in the way of potential attackers and sites have been hardened against accidents and environmental disasters. Such measures include multiple locks, fencing, walls, fireproof safes, and water sprinklers.

The study established that adequate controls are not present to control the physical environment without a plan in place. Most of the respondents noted that KPA must create a team that is responsible for designing a physical security program when planning for security. The organization has put in place an electric fence around it premises as part of the physical security plans. Along the fence also there are security cameras installed at strategic position and they can be able to cover the entire compound and are monitored from a central location: control room.

Figure 4.4: The perimeter wall and electric face at KPA

Besides Electric fence and Security cameras, the organization has reinforced this measure with installation of solar powered security lights and observation towers which are manned by the security guards within the institution as shown in figure 4.4 and figure 4.5.

Figure 4.5 The electric fence at the KPA headquarters

The study established that the control tower is the highest observation post as shown in figure 4.6 below. It provides a clear view of the entire port and also as far as 12 miles into the sea, to monitor approaching vessels. Kenya Ports Authority has put in place flood lights and CCTV that enables the organization to conduct 24 hours operation within its harbor. This security plans has enabled the management to double its operation given the increase of ships docking at the port.

Figure 4.6: The watch control tower and CCTV within KPA

The study further revealed that surveillance and notification systems have been put in place, such as lighting, heat sensors, smoke detectors, intrusion detectors, alarms, and cameras as shown in

figure 4.7 below. This again is complimented by the automated cargo clearance and scanning which has improved efficiency and thus the management can be able to achieve their strategic goals.

Figure 4.7: The CCTV control systems at main entrance Gate B

It was further observed that closed-circuit television or surveillance systems utilize cameras and recording equipment to provide visual protection. In areas that cameras monitor, having enough light in the right areas is essential. It might be too dim for the camera to capture decent video quality necessary to prosecute or identify persons of interest without enough light.

4.8.3 Physical security influence to the management of KPA

The study established that in light with the security challenges that face the organization, the physical security is still inadequate at the moment. The respondent when asked to state how the physical security measures have influenced the management functions, the respondent's feedbacks is summarized in table 12 below.

Table 4.12: Factors affecting organization management at KPA

Factors affecting organization management	Respondents	Percentage	Rank
Management Collaborative	9	30%	1
Team Cohesion	4	13%	4
Leadership Support	4	13%	4
Resource Allocation	6	20%	3
Customer Focus	7	24%	2

Source: Survey Data 2016

The study established that physical security can differ from facility to facility, with myriad factors playing into what exactly is implemented, including budget and the assets that are being protected. Most of the management observed that KPA now accept that physical security is a standard thing, 30% of the responded noted that management collaborative is the most important aspects that is influenced by the implementation of the physical security plans.

The study also revealed that 24% of the respondents confirmed that customer focus has a great bearing in terms of implementation of the physical security plans. It was also noted that physical security plans implementation require much of the resources to be dedicated in meeting the demands posed by the physical security challenges within KPA. Leadership support and team cohesion was rated at 13% by the respondents. The two factors were seen to be equally of importance when implementing physical security plans.

The study established that with the need for the physical security plans, the organization management has established a crisis management plan and have constantly up dated this plans according to the interview feedback from the respondents. It was also established that physical security plan has become the responsibility of each departmental head with supervision from the safety and security department. The organization management is constantly working with assumptions of what the security breach would be and in most cases fail to take into consideration the current threat that the organization is facing.

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Introduction

The purpose of the study was to investigate the influence of the strategic security plans on the organization's management. This chapter therefore presents a summary of findings and discussion, conclusion and recommendations for the study findings.

5.2 Summary of the Study Findings and discussion

5.2.1 Influence of Cyber Security plans

The first objective of this study was to determine the influence of cyber security plans on KPA management. The study established that KPA as an organization faces so many cyber security challenges which conform to the study of Fischer (2015) who established the five categories of the cyber-attack. Which include cyber criminals, hacktivists, organization employees and terrorism. The cyber security plans adopted by KPA include that of advisory, regulatory and informative to the employees. The study also revealed that KPA has a network policy in place including password policies that regulate employees and visitors accessibility to the computer systems.

The study established that KPA is having a tougher time mitigating cyber security breaches, and average financial impact of each breach on the organization is increasing. The findings concur with the findings of Harris (2013) that a single successful attack could have a devastating impact upon an organization’s financial standing or reputation. The immediate consequences for a KPA dealing with a customer data breach are severe and may include negative press, the threat of lawsuits from customers and partners, and long legal investigations.

5.2.2 Influence of Personnel security plans

The second object was to determine the influence of personnel security plans on the management of KPA. The study established that based on the personnel security plans that have been established and in light with the security challenges facing KPA, there has been improved organization commitment by the management. The study established that 77% of the respondents noted that physical security plan is so diffused and impacts on everyone at the management level. However, 23% of the respondents observed that employees’ have become

vigilant in observing risks within the organization premises and then report what they see to the proper contacts.

Personnel security measures also have brought the issue of integrity to question with 83% of the respondents affirming that the management has observed the need of including the employees in aiding organization's physical security plans. There has been noted improvement on the integrity of the KPA management since it is observed that is their responsibilities in formulation and implementation of such security measures.

The study established that 68% of the respondents observed that, personnel security matters are managed in a visible manner and that it has contributed to the improvement of organization's culture. Only the 32 % of the respondents were uncertain how transparency in matters of personnel security affect the management since they were of the opinion that matters to do with security is a collective responsibility.

The study established that the three factors of transparency, commitment and integrity formed part of the core values of KPA management. Wilson (1990) established that personnel security planning touches on the core values of the company management. The influence of these measures has been established that, KPA has an improved commitment by both the employees and the management in enforcement of the personnel security plans. This also had contributed to an improved transparency in vetting of personnel and staffing as well as implementation procedures of their various strategies within KPA. The study also established the integrity of the management has since improved as a result of the implementation the personnel security plans.

5.2.3 Influence of Physical Security Plans

The study established that smuggling, theft of KPA assets, vandalism, intrusion and terrorism are the main challenges that the organization faces. It was found out that KPA has adopted various physical security measures to curb on these challenges. The study established that the management has established automated security measures at the access points; they have also the physical security face and the CCTV camera to monitor movement of cargo, location of the organization assets. It has also established liaison with other law enforcement agencies to improve on the security and monitoring of the operations at the KPA.

It was established that 30% of the responded noted that management collaborative is the most important aspects that is influenced by the implementation of the physical security plans. That management has over time embraced collaboration among the departments in formulation and implementation of the physical security plans. The study also revealed that 24% of the respondents confirmed that customer focus has a great bearing in terms of implementation of the physical security plans. Leadership support and team cohesion was rated at 13% by the respondents. The two factors were seen to be equally of importance when implementing physical security plans. In light the security challenges experienced by KPA, leadership support and team cohesion has been embraced more and more in strategic security implantation within KPA. Resource allocation has considerably gone high in implementation of this security plans and thus impact on other operational activities within the organization.

Sekomo (2013) pointed out that physical security policies are the first line defense for any organization. KPA as the management has invested heavily in physical security so as to mitigate the challenges emanating from the operating environment. The study established there have been reduced cases of smuggling of cargo from KPA, there have been reduced cases of theft to KPA assets and this has increased the confidence level of the customers to the organization. The study established that the management has improved on budget allocation in response to the rising cases of physical security and also there has been improved management collaboration in implementation of this physical security plans with a more focus on customers and leadership support.

The study contradicts with the findings of Oriyano (2014) who re affirmed that the physical element of security is often overlooked. KPA management has endeavored to comply with the International Ship and Port Facility Security (ISPS) Code, which came into force in 2004. The management has made physical security a priority by improving leadership support and management collaborative measures within the organization.

5.3 Conclusion

It is clear that Kenya Ports Authority has adopted various strategic security plans which are aimed at improving the management of the port. Furthermore, the Authority has a clear intention of expanding its infrastructure in order to improve service delivery to its clients. Strategic security plans formulation and implementation is mainly done by divisional heads, and heads of departments. The increasing trend of the improved KPA management is a clear sign of positive influence of strategic security plans on the organization.

The respondents have re-affirmed that Cyber Security plans have had a great influence on Kenya Ports Authority and that it should develop, maintain clear and robust policies for safeguarding critical organization data and sensitive information, protecting their reputation and discouraging inappropriate behavior by employees. Many of these types of policies already exist, but may need to be tailored to suit the organization needs and updated to reflect the increasing influence of security plans, both professional and personal.

The personnel security plans have the greatest influence since they reflect on the personnel relationship with the managements. Most of the management would want to reflect a good impression to the customers and employees at the expense of security breaches. The study has established that it is impossible to separate the concept of security transformation from the pragmatic day-to-day discipline necessary to achieve it. In order to transform your security infrastructure, you must ensure that each security project clearly maps back to the organization's strategic business objectives.

The physical security plans have an influence on the organization management by influencing their way of decision making on the security structures required on the organization. Physical security procedures supplement the security plan and, while they may form part of the plan, can be used as standalone advices to management. However, the management is faced with challenges as they continual to implement this physical security plans. The challenge is twofold. The first challenge is to reach an agreement that something needs to be done. This involves altering mindsets; building consensus and getting senior management buy in. The second

challenge is in developing and implementing an effective and tailor-made integrated physical security (IPS) plan.

5.4 Recommendations

Kenya Ports Authority has set very many strategies that need to be implemented. The management of the Port needs to prioritize these strategies and tailor resources for the implementation of these strategies. Since some managers complained of not being involved in the formulation of strategies, there is need for the Authority administration to reconsider involving all the managers. This will enhance speedy implementation because the managers will feel involved.

From the findings and conclusions, the study recommends that the management engage various strategies to survive in a dynamic and highly competitive business environment. The study recommends that further training and study tours be used to allow the exchange of ideas among KPA employees and the management. This way, the staff will be able to learn the best ways of improving service delivery. The study further established that the strategic security plans also has an effect on the organization behavior. The researcher recommends further studies to be carried out to determine the impacts of this security plans to the organization behavior.

REFERENCES

Africa Centre for Strategic Studies. (2009).*Security Ports in Africa*; http://africacenter.org/2009/06/security-ports-in-africala-securite-portuaire-en-afrique/ retrieved on 12 Oct 14.

Agumba, J. (2012).Competitive strategies in response to challenges of external environment by Water Resources Management Authority in Kenya. Unpublished MBA Thesis, University of Nairobi

Ansoff H. I. and McDonnel E.J. (1990), Implementing Strategic Management, 2nd Edition, Prentice Hall, Pearson Education International.

Bandari Magazine. (2010, March 4). *Kenya Ports Authority Internal Magazine*: Pp 2, Pp5.

Bryson J.M. (2004). Strategic Planning for Public and Nonprofit Organization A Guide to Strengthening and Sustaining Organizational Achievement. Jossey-Bass.

Center for protection of national infrastructure. *Personnel security risk assessment: A Guide; 4th Edition.* Retrieved from http://www.cpni.gov.uk/documents/publications/2010/2010037-risk_assment_ed3.pdf?epslanguage=en-gb on 23 August 2016

David F.R. (2005). Strategic Management: Concepts and Cases, Tenth Edition. Prentice Hall, Pearson Education International.

Dinicu A. (2014). Cyber Threats to National Security. *Specific Features and Actors Involved*. http://www.armyacademy.ro/buletin/bul2_2014/DINICU.pdf accessed on 03 Oct 16

Evans B. (2015).*The importance of building an information security strategic plan*. Retrieved from https://securityintelligence.com/the-importance-of-building-an-information-security-strategic-plan/ on 20 July 2016.

Flood P.M, Marm W.J and Young C.T (2010), Success in Coin: Aligning Organizational Structure with Strategy. Published MSc Thesis, Naval Postgraduate School (US)

Frishammar, J. (2003). Information use in strategic decision making. *Management Decision, Vol.4, no.4: 318-326*

Gichumbi, N. (2008). Strategic responses by NSSF to changing environmental conditions in Kenya. Unpublished MBA Thesis, University of Nairobi

Grant, R. M. (2002). Contemporary Strategic Analysis, 4th edition, Balckwell Publishers Inc. Massachusetts.

Harris S. (2013). Physical and Environmental Security. *In CISSP Exam Guide* (6th ed., pp. 97, 98, 157- 277). USA McGraw-Hill

Harris, S. (2013). Information Security Governance and Risk Management. In CISSP Exam Guide (6th ed., pp. 21-141). USA McGraw-Hill.

https://www.connectsmart.govt.nz/assets/NCSC-Cyber-security-risk-management-Executive.pdf accessed on 23 July 2016

Irwin S. (2014). *Creating a Threat Profile for your Organization*. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492 on 19 July 2016

Kenneth G. (2015). Strategic Security Plan. NATO Cooperative Cyber Defence Centre of Excellence. CCD COE Publication; Estonia. Retrived from url: https://ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF accessed on 30 September 2016

Kenya Ports Authority (2012, August 15), *Master Plan Study of the Port of Mombasa.*

Kenya Ports Authority website: http://www.kpa.co.ke/security/Pages/default.aspx accessed on 03 Oct 14.

Kenya Ports Authority, *STRATEGIC PLAN; 2013 – 2018*

Mangan J. and Cunningham J. (2001) Irish Ports: Commercialization and Strategic Change. Business strategy review; Newyork.

Mark L.F and Anderson R. J. (2009). *Strategic Risk Assessment – A first step for improving risk management and governance.* December 2009. Retrieved from http://www.rims.org/resources/ERM/Documents/StrategicRiskAssessment_StrategicFinance_December2009.pdf on 23 July 2015.

Mugenda, O. M. and Mugenda, A. G. (2003). Research Methods: Qualitative and Qualitative approaches, African centre for technologies Studies, Nairobi, Kenya

Mwarania. J (2008). Responses by reinsurance companies in Kenya to changes in the environment. The case of Kenya Reinsurance Corporatione. Unpublished MBA Thesis, University of Nairobi

Mwikali, M. C. (2012). Response strategies adapted by Kenya Pipeline Company Limited to the challenges of oil distribution in Kenya. Unpublished MBA Thesis, University of Nairobi.

Marco G. (2012). Understanding Cybercrime: Phenomena, Challenges and Legal Response: ITU, Newyork.

Marco G. (2011). Understanding Cybercrime: A Guide for Developing Countries: ITU, Newyork

Niyazi Onur B. (2007)"A Brief Analysis of Threats and Vulnerabilities in the Maritime Domain". Non-published Research Reports. Paper 5.

Oriyano S. (2014). Physical Security. In Cehv8: Certified Ethical Hacker Version 8 Study Guide (pp. 393-409). Indianapolis, IN USA: Wiley

Pearce, J. A. and Robinson, J. B., (2005). Strategic Management: Formulation, Implementation and Control, 3rd edition, Richard D. Irwin

Richard P. J, Devinney T. M, Yip G. S, Johnson G. (2009). 'Measuring Organizational Performance: Towards Methodological Best Practice'. *Journal of management 35: 3; p718-p804*.

Ruto W. K. & Datche, E. (2015) Logistical Factors Influencing Port Performance A Case of Kenya Ports Authority (KPA). *International Journal of Current Research and Review, 7 (12), 52-59.*

Ravi Sharma, (2012). Study of Latest Emerging Trends on Cyber Security and its challenges to Society, *International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012.*

Scheuing, E. E. (2004). Delivering World Class Service, A paper presented at the Purchasing and Supply Leadership Emeritus, St. John's University, New York.

Sanga W. M. (2012). Strategy Implementation at Kenya Maritime Authority. Unpublished MBA Research Project, University of Nairobi.

Swaleh, A. (2007). Competitive strategies adopted by petroleum retail stations in Kenya. Case of Mombasa City. Unpublished MBA Thesis, University of Nairobi.

Sekomo, A. (2013). Workshop Report "African Approaches to Maritime Security" Africa Centre for Strategic Studies: Johannesburg, University of the Witwatersrand.

Sauer, C. and Willcocks, L. (2003). Establishing the business of the future: the role of organizational architechture and information technology. *European Management Journal, Vol. 21, pp. 497-508.*

Tai J.K (2007). Strategy Implementation in Kenya Ports Authority. Unpublished MBA research project, University of Nairobi.

Tommy N. J (2013). Structural implications in strategy implementation at the Kenya Ports Authority. Unpublished MBA project, university of Nairobi.

Warner, M.E. and A. Heifetz. (2002). "Applying Market Solutions to Public Services: An Assessment of Efficiency, Equity and Voice," Urban Affairs Review, 38(1): 70-89.

Woods, A. and Joyce, P. (2003). Owner-Managers and the Practice of Strategic management, *International Small Business Journal, London 21 Issue 2.*

Wilson, P. (1990). *Strategic planning in the public sector, Practicing Manager, Vol. 10, No.2, pp. 23-24.*

APPENDICES

Appendix I: Letter to the Respondent

Maseno University
School of Planning and Architecture
Department of Urban and Regional Planning

TO WHOM IT MAY CONCERN

Dear Sir/ Madam,

RE: REQUEST FOR RESEARCH DATA

Mr Luke Nandasava is a student at Maseno University undertaking a Master Degree. As part of the requirement of Master of Arts in Project Planning and Management, he is undertaking a research study entitled "The impacts of strategic security plans on the organization Management: A case of Kenya Ports Authority". The study is expected to provide useful information that will be beneficial to managers on the impact of strategic security plans on the organizational management. You have been identified as one of the respondent to provide information for the study. This is therefore to request you to complete the questionnaire as honestly as possible. All information that you provide shall be treated with utmost confidentiality and will be used for the purpose of this study only.

Yours sincerely,
Dr George G Wagah
Dean

Appendix II: Questionnaires to the Respondents

MASENO UNIVERSITY
SCHOOL OF PLANNING AND ARCHITECTURE
DEPARTMENT OF URBAN AND REGIONAL PLANNING
QUESTIONNAIRE SERIAL NUMBER ……

SECTION A: GENERAL INFORMATION

1. How long have worked at the Kenya Ports Authority?

---

2. What role do you play in formulation of strategic security plans of KPA?

---

3. Do KPA have monitoring and evaluation/feedback mechanism to monitor achievements is strategic goals and objectives?

Yes [ ]
No [ ]

3. What are some of the strategies that have been adopted at KPA in achieving its vision?

---
4. What are some of the challenges that KPA has faced in the adoption of this strategies?

---
5. Does KPA conduct situational analysis before formulation of the strategic security plans?

Section B: Cyber Security Plans

6. What are some of the cyber security challenges that KPA has faced in the recent past?

---
7. What are some of the strategies that have been adopted by KPA in countering these challenges?

---
8. What has been the impact of cyber security plans to the management of KPA?

---

9. Does KPA management have a network policy for the employees?
   Yes [ ]
   No [ ]

10. What has been the trend in the organization cyber security plans in the last five years?
    a. Increasing [ ]
    b. Decreasing [ ]
    c. Irregular [ ]
    d. Stagnant [ ]

11. Has the authority developed a set of key performance indicators or some other form of accountability to track the success of cyber security plans initiatives?

---

12. How the cyber security does plans impact on the management of KPA?

……
……

Section C: Personnel Security Plans

13. What are some of the personnel security challenges that KPA has faced?

---

14. What strategies that have been developed by KPA to counter the challenges of personnel security plans?

---

15. On a scale of 1-5 (1being lowest and 5 being the highest) how do you rate the following strategies in management of the personnel security challenges?

Personnel Security strategies within KPA	**Rating (1-5)**
Identification numbers for the staff of KPA and visitors	
The use of Standard operating procedures	
Screening procedures for new personnel and visitors	
Law enforcement agency cooperation	
Third party provider rules and regulations	
Movement control within KPA	

16. What has been the impact of personnel security plans to the management of the KPA?

Section D: Physical security Plans

19. What are some of the physical security challenges that KPA has faced?

---

20. What are some of the physical security plans that have been adopted by KPA?

---

21. What has been the impact of the physical security plans to the management o the organization?

---

22. On a scale of 1-5 (1 being the lowest and 5 being the highest), how do you rate the following measures in curbing the physical security challenges?

Physical security factors	**Rating (1-5)**
Physical access control	
Asset protection	
Physical security of employees and visitors	
Alarm systems	
Physical security of information	
Site security plans	

Appendix III: Guide to Structured Interviews

1. Do the physical security plans provided by the organization adequate enough to secure the whole organization assets?

2. Does the asset identification measure put in place by the management adequate in protection of the facilities?

3. Do the surveillance systems within the organization assist the leaders in effective management of the port?

4. Do the employees and customers aware of the physical security measure provide within the organization?

5. How does the physical security plans assist the management in their normal running of the organization?

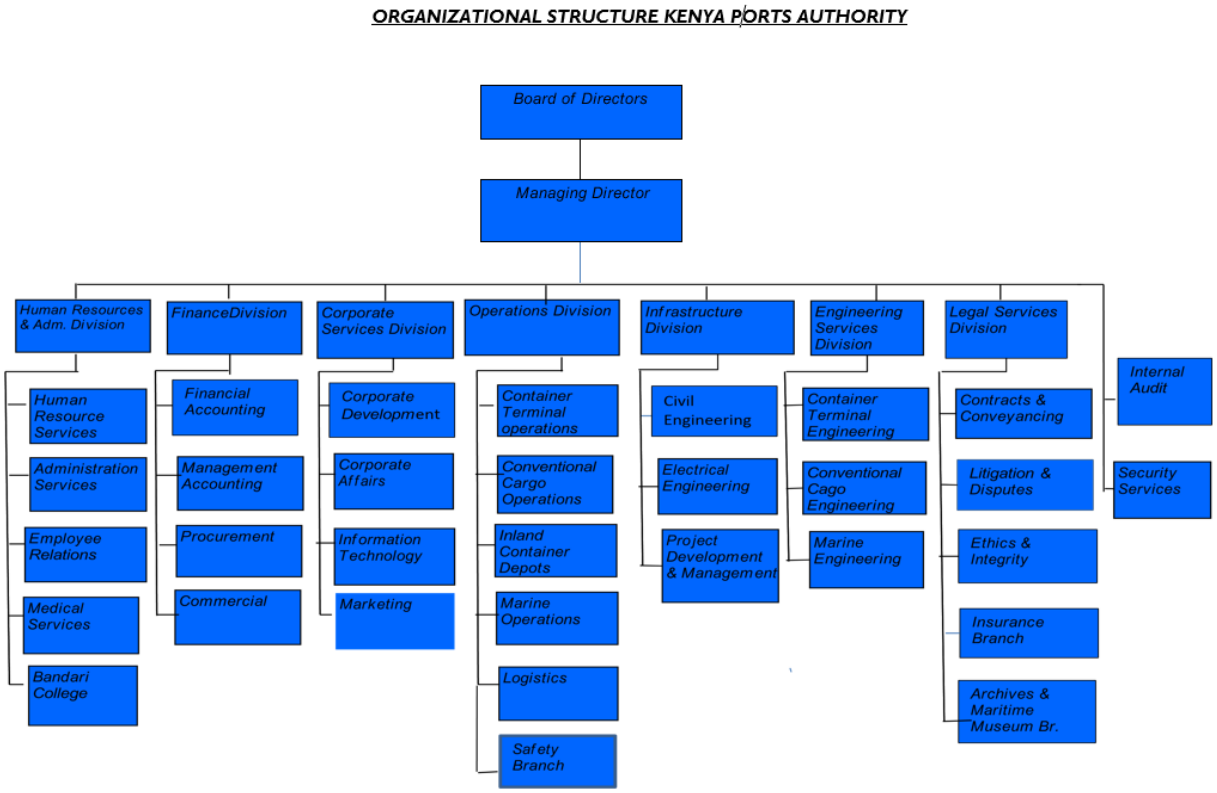
6. How does the personnel security plans adopted by the management affect the overall management of the organization?

7. Does the organization have in place the network security policies for the employees and management?

8. How the cyber security does plans impact on the management of organization?

ANNEXES

Annex A: Sample Size



Annex B: Observation Checklist

SN.	Items	External access	Physical security	Personnel security	Cyber security	Detection	Security plan
1	Fencing and gates						
2	CCTV						
3	Exterior lighting						
4	Electronic access control						
5	Intrusion alarms						
6	Security guards						
7	Emergency Procedure manuals						
8	Law enforcement Observation posts						
9	Identification barges						
10	Control room						