CYBER SECURITY RISK MANAGEMENT AND THREAT CONTROL MODEL (CSRM-TCM): A STUDY CARRIED OUT TO ENHANCE THE PROTECTION OF INFORMATION IN THE NAMIBIAN PUBLIC SERVICE

A THESIS SUBMITTED IN PARTIAL FULFILMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

OF

THE UNIVERSITY OF NAMIBIA

BY

JAMBEKO M. UUDHILA

200308581

MARCH 2016

Main Supervisor: Prof. Jameson Mbale

ABSTRACT

The persistent threats of the cyber environment drives organizations to adopt risk management as a crucial practice of minimizing dangers to their information assets. However, focusing on technology alone to address these risks is no longer sufficient. IT governance which enables senior managers to align and integrate technology with business strategies through clear policy development and good practice of IT control is essential.

The Namibian Public Service (NPS) currently lacks policy guidance on cyber security risk management. Consequently Offices/Ministries/Agencies (O/M/As) depend on technology to manage security risks facing them. However, this effort is not co-ordinated between various O/M/A. Therefore it presents security challenges to the government network as various systems continues to be interconnected.

To address these risks, the study investigated behaviors of different O/M/As in the NPS. The focus was predominantly on the management of information assets in the absence of standardized cyber security best practices. The study concluded that although there may be an abundance of technologies in the (NPS), the absence cyber security policies, standards and guidelines has led to a huge disparity regarding the way in which Information Systems (IS) are managed in various O/M/As. Hence, this poses security challenges.

The study further identified threats, vulnerabilities facing the NPS and developed the Cyber Security Management and Threat Control (CSRM-TC) model. The model is believed to assist IT officials and policy makers in the NPS to understand challenges facing their information assets. This would further assist them to make appropriate decisions when developing cyber security policies, standards, guidelines and procedures according to best practices.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

3G/4G - Third Generation/ Fourth Generation

BYOD – Bring Your Own Device

CCTV – Closed Circuit Television

CMSPSM – Common Minimum Standards of Protective Security Measures

CSRM-TC – Cyber Security Risk Management and Threat Control

DDoS – Distributed Denial of Service Attack

DPSITM – Department Public Service Information Technology Management

DoS - Denial of Service Attack

GRN – Government of the Republic of Namibia

HIPPSA – Harmonization of ICT Policies in the Sub-Sahara Africa

ICT – Information Communication Technology

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

IS – Information Systems

ISO – International Organization for Standardization

ISO/IEC - International Organization for Standardization/International Electro technical Commission

ISMS – Information Systems Management System

IT – Information Technology

ITU – International Telecommunication Union

NPS – Namibian Public Service

MICT – Ministry of Information and Communication Technology

MS – Microsoft

O/M/AS – Offices/Ministries/Agencies

PDA – Personal Digital Assistants

SPSS – Statistical Package for Social Sciences

USB – Universal Serial Bus

Wi-Fi – Wireless Fidelity

WSUS – Window Server Update Services

ACKNOWLEDGEMENT

I would like to express my sincere appreciation and gratitude to the following people:

First and foremost I would like to thank Father God, the Almighty for his love, protection and for blessing me with an undoubted health during the duration of my study. Secondly I would like to thank my supervisor, Professor Jameson Mbale for his remarkable support, guidance, encouragement and exceptional advice throughout this Thesis work. Thirdly, I must applaud all IT staff in the Namibian Public Service who availed themselves to participate in the study. I appreciate their passion and the proficient inputs they provided.

Fourthly, I should express gratitude to my fellow postgraduate students, at that time, for their encouragement, motivation and inspiration.

I do not want to forget to extend my heartfelt obligations to Telecom Namibia for providing me with the financial assistance through the Center of Excellence at the University of Namibia.

And finally, I would like to express my appreciativeness to my family and close friends for the unceasing support, understanding, love and patience throughout my study.

To anybody else who has helped me directly or indirectly.

I say thank you.

DEDICATION

I dedicate my Thesis to the Lord God Almighty, my father Heimo Twaloyendji Uudhila, my mother Terttu Ndunge Uudhila, my sister Uuyuni Ndeutala Iteeleni Ondinomukwathi Uudhila, my daughters Michelle Mutatwa Kavindja and Twapewa Omukwathi Nghidini Shawelaka.

DECLARATION

I, Jambeko M. Uudhila, declare that this study titled "**Cyber Security Risk Management and Threat Control Model (CSRM-TCM): A survey carried out to enhance the Protection of Information in the Namibian Public Service**" is a true reflection of my own research, and that this work, or part thereof has not been submitted for a degree in any other institution of higher education.

Full Name: **Ms. Jambeko M. Uudhila**

Signature: _____

Date: _____

1. INTRODUCTION

This chapter introduces the cyber security and risk management study carried out in the NPS. The statement of the problem, research questions, significance of the study, limitations and methodology are also discussed here. The chapter further presents the definitions of core terms used and an outline of the Thesis.

1.1 Introduction

Cyber security has generally brought concerns among nations as they become increasingly dependent on Information Communication Technology (ICT), and Internet to operate their businesses and provide services to their customers. This situation has equally been realised in Namibia as the adoption of ICT has been on the rise among the different sectors of the country. This was confirmed by Xoagub (2014) when he stated that the need for cyberspace security in Namibia had grown with the increase in usage and dependence on ICT devices and gadgets. Imalwa also stated that Cyber security plays a fundamental role in the continuing development of Information Technology (IT) and Internet Services (IS) (Bennett, 2015). In addition, Bennett stated that in order to safeguard Namibia's security and economic wellbeing it is of utmost importance that cyber security is developed to protect information structures.

Therefore, based on the above sentiments, it is clearly evident that although ICT has brought recognizable benefits to the Namibian Public Service (NPS), its information

assets have also become vulnerable to various threats of the cyber environment. This condition highlights a need for the engagement of cyber security best practices to prevent the possibility of cyber incidents.

Atul et al. (2013) defined cyber security as the activity of protecting data and information systems with appropriate procedural and technological security measures. In addition, the International Telecommunication Union Report (ITU, 2014) defined cyber security as the collection of tools, policies, concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that could be used to protect the cyber environment, organization and user's assets.

In view of the above it could be noted that cyber security is a combined effort that requires organizations to collectively engage the right governance, processes and technology to address both technical and non-technical challenges. In this study, Cyber Security Risk Management and Threat Control model was introduced and abbreviated as CSRM-TC. The model presents foundational security building blocks that would place the NPS in the position to either block cyber intrusions or detect them and stop them from spreading further into the networks.

Daughton (2015) advised that in the face of ever more sophisticated criminals, the fight against cybercrime requires coordinated effort among all stakeholders, including governments, educational institutions, business organizations and law enforcement authorities. In view of the above, it is important that there is a strategy for each stakeholder to manage risks associated with cybercrime. Peltier (2002) described risk

management as the process of identifying risks, assessing the likelihood of their occurrences and then taking steps to reduce them to an acceptable level. The study was therefore carried out to assess effects of absence of cyber security and risk management best practices on the NPS with the aim of developing strategy in the form of a model.

1.2 Statement of the Problem

There is currently a lack of cyber security best practices in the NPS. This situation has made it difficult for IT staff to manage the security of different Information Systems (IS) and networks of various O/M/As in a standardized manner. Ogut et al. (2011) stated that an important challenge faced by governments is the management of national infrastructure security. Similarly, the NPS does not have cyber security best practices for the various O/M/As. The only security guidelines currently present are the Common Minimum Standards of Protective Security Measures (CMSPSM) that were developed for manual based systems of the Namibian Public Service (GRN, 1996). Since then, no other security standards or guidelines were developed to cater for the current electronic systems.

Therefore, with the evolvement of technology and the increasing dependency on ICT, there was a need for the NPS to initiate, adopt cyber security measures and standardize them across the whole public service. Geers (2009) stated that as dependence on IT and the Internet grow, governments should make proportional investments in network security, incident response, technical training, and international collaboration. Similarly, NPS has been investing on e-Government initiatives, which would require

proportional investments in network security framework. Therefore it is crucial that the cyber security best practices and proper technical trainings are developed for the NPS.

In this study, CSRM-TC aimed at identifying risks facing various O/M/As according to cyber security best practices. Furthermore, the study developed strategies to control threats and mitigate their impacts on the Namibian Public Sector information systems and networks. This was intended to assist the NPS to be proactive in terms of cyber security measures in terms of managing both targeted and widespread attacks.

1.3 Research Questions

During the study, the following research questions were answered:

1.3.1. How can cyber security risks be addressed to protect data and control threats in the Namibian Public Service?

1.3.1.1. What cyber security risks are facing the Namibian Public Service?

1.3.1.2. What strategies can be employed to mitigate risks facing the Namibian Public Service?

1.4 Significance of the Study

The study would encourage NPS senior officials to develop suitable security policies, standards and guidelines. This would also guide them when reviewing the current IT policies to improve cyber security in the NPS. The study would further aid IT officials to better understand and manage the cyber security risks facing the NPS.

1.5 Limitations of the Study

Access to certain data was difficult to obtain due to the sensitivity of information and fear of compromised security. Some of the targeted respondents were lacking the required knowledge and some were inaccessible. Some of the IT technical services rendered to the NPS were outsourced from foreign consultants. This limited availability of the sufficient data. Hence some figures provided were simply approximations.

1.6 Research Methodology

The study was designed to use qualitative research methods. A case study in the form of an exploratory qualitative research design was used to carry out an in-depth analysis of the behaviors of IT staff at different O/M/As when managing various information assets, in the absence of cyber security best practices. Surveys and face to face interviews were conducted to understand cyber security risks facing the NPS. Qualitative methods were used to classify features of different threats and vulnerabilities identified as well as to construct statistical models and figures to explain findings of the study.

1.7 Definition of Terms

This section consists of the core terminologies used in the Thesis. The terms may be defined differently in the literature, but for the purpose of this study, the following definitions applied:

Cybercrime: is referred to as any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them (Ayofe & Irwin 2010).

Cyber security: is the collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. (ITU, 2014)

Risk: is the potential loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability. A risk is a possibility that something unpleasant will happen.

Threat: is an object, person or other entity that represents a constant danger to an asset (Whitman & Mattord, 2008). It is anything that can exploit vulnerability, intentionally or accidentally and damage or destroy an asset.

Vulnerability: is a weakness or gap in our protection efforts. It is a defect or weakness in information asset, security procedure, technical design or control that a threat may exploit on purpose or even accidentally to breach security system. (Jounia et al., 2014)

1.8 Outline of the Thesis

The thesis is organized into seven chapters as follows:

Chapter 1: Introduction

Chapter 1 introduces the research by providing an overview of the research topic, orientation of the study, statement of the research problem, research questions, significance of the study, limitation of the study, research methodology, definition of core terms used in the study, and an outline of chapters of the Thesis.

Chapter 2: Literature Review

Chapter 2 addresses the review of related work carried out for the purpose of the study. It covers the literature on cyber threats identification, sources of cyber threats, the danger of cyber threats, need for cyber security in the NPS and their significance in an organization.

Chapter 3: Methodology

Chapter 3 discusses the research methodologies used in the study. It covers the research design, targeted population of the study, sample selected for the study, research instruments, research procedures used during the study and data analysis.

Chapter 4: Results

Chapter 4 presents the analyzed results of the data collected through questionnaires and interviews.

Chapter 5: Discussion

Chapter 5 presents the discussion of the results of the study in relation to the research questions posed in the Thesis.

Chapter 6: Proposed Framework

Chapter 6. Presents the proposed framework designed for the NPS.

Chapter 7: Conclusion and Recommendation

Chapter 7 presents the conclusion of the study and recommendations for further research.

The next chapter focuses on related work carried out to understand factors that need to be considered by the NPS to enhance effective cyber security.

2 LITERATURE REVIEW

This chapter presents a review of related work carried out for the purpose of this study. Security models similar to CSRM-TC were studied and summarized in terms of gaps that the proposed model is aiming to address. In addition, the chapter covers literature on the kind of information assets to be considered, ways in which information assets should be selected for protection, importance of cyber security policy and the key players.

2.1 Review of Related Models

The review of literature was conducted to inform this study. Two topics of literature were identified: cyber security and risk management. The focus of the review was to gain a better understanding of what others have done to secure their information assets from the risks emerging from the cyber environment and how they overcame the challenges according to best practices. The first section of this chapter describes existing models related to CSRM-TC. The gaps therein were discussed and summarized as presented below:

2.1.1 Information Security Policy: An Organizational-Level Process Model

Knapp et al. (2009) developed this model. The model illustrated a general, yet, comprehensive policy process in a distinctive form not found in existing professional standards of academic publications. The model went beyond the ones illustrated in the literature by depicting a larger organizational context that included key external and

internal influences that could materially impact organizational processes. It used a methodology involving qualitative techniques, based on responses from a sample of Certified Information Systems Security Professional (CISSP).

The qualitative methodology was largely based on grounded theory approach involving a series of structured steps that included the systematics comparison of units of data and the gradual construct of categories that described the observed phenomena. The description of the phenomena evolved directly from the data. After development of a model, a three phase validation process that led to improvement to the model was conducted.

The model reflected an information security policy process in modern organizations based on recommended practices from a sample of certified professionals. However this model only focused on the general information security policy development and did not explore down to the topic specific or IT device specific policies. Based on the conceptual framework CSRM TC found it necessary to consider both the high and low levels of the security policy framework in order to bring about effective cyber security in the NPS.

2.1.2 A Situation Awareness Model for Information Security Risk Management (ISRM)

Webb, Ahmad, Maynard and Shanks (2014) developed a Situation Awareness Model for Information Security Management (ISRM). The model addresses deficiencies in the practice of information security risk assessment that inevitably led to poor decision-making and inadequate or inappropriate security strategies. The three deficiencies are 1) information security risk: identification is commonly perfunctory, 2) information security risks are commonly estimated with little reference to the organization's actual situation and 3) information security risk assessment is commonly performed on an intermittent, non-historical basis. The deficiencies were addressed through an enterprise-wide collection, analysis and reporting of risk related information.

A single case study of the US IC using publically available documents was conducted. Seventy one (71) publicly available documents that included US laws intelligence community policy documents, military manuals US Government publications, US Government websites and authoritative works produced by subject matter experts.

Two rounds of axial and selective coding were conducted to: generate a process a description explaining which actors performed which functions in the intelligence community (round 1) and identify where efforts were concentrated at the highest intelligence community management (ODNI) level, in order to extrapolate from the key drivers of the enterprise (round 2). The adapted model was verified by comparing concepts from SA theory to the phases of intelligence cycle to identify points of analogy.

A situation awareness (SA-ISRM) process model was proposed to complement the information security risk management process. This model however did not incorporate the necessary risk management best practices in terms of governance required as well as key players involved. CSRM-TC therefore found it necessary to address this issue based on ISO/IEC 27000 series of best practices.

2.1.3 Information Security Management: An Information Security Retrieval and Awareness Model for Industry (ISRA)

Kritzinger and Smith (2008) developed an Information Security Retrieval and Awareness Model for Industry (ISRA). The model consists of three parts namely 1) the ISRA dimension (non-technical information security issues, IT authority levels and information documents), 2) information security retrieval and awareness, and 3) measuring and monitoring. The model focused exclusively on the non-technical issues. The primary reason was that much research had already been done regarding the implementation of technical information security issues in the industry. This model could be used by industry to enhance information security awareness among employees. However, the model only focused on the non-technical information security matters but did not show how this influences the technical issues. CSRM had therefore addressed this gap in the NPS by carrying out an assessment to identify how the non-technical information security issues have impacted the effective utilization of technical measures while focusing at both internal and external influences. The ISRA study was general but CSRM was a specific case study for the NPS.

2.1.4 IT Security Auditing: A Performance Evaluation Decision Model

H.S.B Herath and C. Herath (2014) developed the Performance and Evaluation Decision Model. This model was developed on the basis that information security and systems audits are important for providing compliance, however they were not mandatory to all organizations. The model considered the question of whether or not to carry out an IT security audit by developing a performance evaluation decision model. The model also considered investments and their relationship to IT audits. The model incorporated agency costs to determine the incentive payment for managers to conduct an audit. However this was a non-mandatory security initiative that would still give room to be overlooked. CSRM-TC on the other hand has incorporated the IT Audit and compliance model that is made compulsory to all.

2.1.5 COBIT 5 Information Security

According to (ISACA, 2014), COBIT 5 Information Security is an extended view of COBIT5 that explains each component from info security perspective. It aimed to be an umbrella framework to connect other information security frameworks, good practices and standards. The major drivers for the development of COBIT 5 for Information Security included the increasing need for enterprises to keep risk at acceptable levels, maintain availability to systems and services, connect and align with other major standards and frameworks and comply with relevant laws and regulation.

The benefits of using COBIT 5 for Information Security includes improved integration of information security in the enterprise, informed risk decisions and awareness,

improved prevention, detection and recovery, reduced impact of security incidents and better understanding of information security.

Information security policies, principles, and frameworks, processes, information security-specific organisational structures, factors determining the success of information security governance and management, people, skills and competencies specific for information security are also part of this framework.

Similarly, CSRM-TC will also look at the NPS from a security perspective of information systems considering that in each activity that is undertaken there is a security risk. It was crucial that CSRM-TC considered both the governance and management of IT services within the NPS and adopt a characteristic of being able to connect and align with other major standards and frameworks.

2.1.6 The ITU Conceptual Framework

According to the (ITU, 2015) report, the ITU conceptual framework was developed through the Global Cybersecurity Index (GCI) project which was aimed at effectively measure each nation state's level of commitment to cybersecurity. The ultimate goal was to help foster a global culture of cybersecurity and its integration at the core of ICTs. The project was launched by the ITU and private sector company ABI Research.

Rooted in the ITU Global Cybersecurity Agenda, the GCI looked at the level of commitment in five areas: legal, technical, organizational, capacity building and international cooperation. The result was country-level index and a global ranking on

cybersecurity readiness. The GCI did not seek to determine the efficacy or success of a particular measure, but simply the existence of national structures in place to implement and promote cybersecurity.

The project was a result of intensive primary and secondary research by both ITU and ABI Research. Country level surveys, complemented by in-depth qualitative research, were sent out to all ITU Member States. Information was collected on laws, regulations, CERTs and CIRTs, policies, national strategies, standards, certifications, professional training, awareness raising, and cooperative partnerships.
The aim of the GCI was to provide a snapshot of where countries stand in their cybersecurity engagement at the national level. The visions as seen by ABI Research and ITU was to promote cybersecurity awareness and the important role governments had to play in integrating appropriate mechanisms to both support and promote this crucial discipline. In this project, Namibia was among the countries that were ranked at twenty nine (29) on the "Global Cybersecurity Index & Cyberwellness Profiles" on the scale of 1- 29 with one (1) being good and twenty nine (29) being poor.

The CSRM-TC model was designed to operate at a government level unlike the ITU framework that was aimed at addressing cybersecurity risks at a national level. The focus of ITU was purely an assessment to develop a wellness profile for the different countries globally while the CSRM-TC was both an assessment and recommendation for cyber security strategies by the NPS. It was confirmed from this report that the ECOWAS legislation was being transposed into the Namibian legal System and specific legislations were already being mandated through the use of Electronic

Transaction and Communication Act and the Cybercrime bill (draft). This therefore highlights a need for the NPS to develop and enforce cyber security risk measures to be able to successfully secure electronic evidence that may be used as evidence in the court of law.

2.2 Information Assets to be Considered for Cyber Security

In the presence of cyber security challenges, it is mostly important to understand exactly what needs to be protected. Solm and Niekerk (2013) highlighted that the most defining characteristic of cyber security is the fact that all aspects that should be secured are protected against vulnerabilities that exists as a result of ICT, that forms the basis of cyber space. Maskun et al. (2013) emphasized that both protection of hardware and software are the main point of cyber security. In addition, the ITU (2011) highlighted that the general security objectives comprises of availability, integrity and confidentiality of information. They explained that cyber security strives to ensure the attainment and maintenance of properties of an organization and user's assets against relevant risks in the cyber environment. They further clarified that organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

In agreement to the previous paragraph, the NPS hosts majority of IT systems that forms part of the national critical infrastructures. These include amongst others, security, health, transport services and financial systems. Therefore it was important

that CSRM-TC identified that all information assets of the NPS that needed to be protected and considered to be secured against cyber threats.

Another aspect that also needs to be considered in CSRM-TC security efforts is the protection of outsourced services. Ernst and Young (2006) noted that as businesses moved toward increasingly decentralized business models through outsourcing and other external partnerships, it became even more difficult for them to retain control over the security of their information and for senior management to comprehend the level of risk to which they were exposed. In the same vein, the researcher had learned that some of the ICT solutions in the NPS are outsourced to local private or foreign companies. After implementation, IT members of staff were not trained to take ownership of the systems in terms of providing technical support or adding new functionalities based on user requirements. The systems remain fully supported by the service providers throughout its life and one would not guarantee that the level of security at that particular organization is acceptable. This situation had made it equally difficult for IT staff and senior managers to realize the level of risk they were exposed to when outsourcing IT solutions. CSRM-TC therefore found it necessary that the NPS addressed the security concerns of outsourced ICT solutions.

Atul et al. (2013) stated that recent surveys on cyber security trends identified mobile devices and application, social media networking, cloud computing and a practice of protecting systems rather than information as new sources of cyber vulnerabilities. Calder and Watkins (2012) also observed that there is an unstoppable trend towards mobile computing. They added that the use of laptop computers, Personal Digital

Assistants (PDAs), mobile and smart phones, digital cameras, portable projectors, mp3 players and iPad has made working from home and while travelling relatively straightforward with the result that network perimeters had become increasingly porous. They further concluded that these practice means that the number of access points to networks and the number of accessible end-point devices, had increased dramatically, and this has increased the opportunities for those who wish to break into networks and steal or corrupt information.

In view of the above authors, the NPS was equally faced with similar vulnerabilities since social networking sites such as Facebook, LinkedIn and Twitter are widely used in the Public Service. Cloud computing has also been adopted by some O/M/As through various models namely Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Nowadays staff members also prefer to connect to the corporate networks and access official information and systems using smart phones, iPad or tablets that may be personal or official. Therefore it was crucial that the CSRM-TC considered security measures in the areas of cloud and mobile computing as well as social networking in the NPS.

Shackerford (2012) observed that while huge effort and resource is spent in securing the perimeter, threats within company networks often go unnoticed. Slay and Koronois (2006) also observed that businesses often focused on protection against external attacks, but internal attacks were more common and often more damaging. They added that businesses needed to have access control that limited the extent to which a particular employee could access IT resources so that employees only access the

resources required for performing their job. Jaccard and Nepal (2014) also supported this with evidence from a research conducted by McCue (2008) which, indicated that 70% of fraud is perpetrated by insiders rather than by external criminals but that 90% of security controls in organisations are focused on external threats. On the contrary, CSRM-TC proposed that the NPS addresses both internal and external threat prevention and management against information assets.

2.2.1 Ways in Which Information Assets are Managed for Protection

The literature has shown three possible ways by which security threats could be managed for protection.

2.2.1.1 Threat and Assets Identification

Jaccard and Nepal (2014) stated that threats come from different sources, like employees' activities or hacker's attacks. He added that to find these threats, their sources and specific areas of the system that may be affected should be known, so the information security assets could be protected in advance. He advised that, managers needed to know the threats that influenced their assets and identify their impact to determine what they needed to do, in order to prevent attacks by selecting appropriate countermeasures. Pant et al. (2006) also observed that the relevance of a threat to a particular network had to be determined in the context of a network's underlying technology, the applications being used, and the design of the network. In favour of the above statement, CSRM-TC found it necessary to study and investigate the underlying technologies of the NPS ICT infrastructure to determine the possible risks

and impacts associated with them. This process was aimed to assist in deciding on the appropriate countermeasures.

Tudose (2012) also emphasized that identifying the types of threats is an extremely important aspect for creating the security policy, because it allowed the creation of a set of measures destined to remove these dangers. In support of the above, CSRM-TC had considered the identified threats and vulnerabilities and decided upon appropriate countermeasures that could be used as inputs to the security policy framework development.

2.2.1.2 Threat Classification

Jaccard and Nepal (2014) highlighted that, effective security classification was necessary to understand and identify threats and their potential impacts. They added that security threats could be observed and classified in different ways by considering different criteria like source, agents, and motivations. They further added that classification helps identify and organize security threats into classes to assess and evaluate their impacts, and develop strategies to prevent, or mitigate their impacts on the systems.

Similarly, the manual of Guidelines for Common Minimum Standards of Protective Security Measures for Government Ministries/ Public Offices and Agencies of the Republic of Namibia classified security levels of manual records in three categories mainly: Top Secret, Secret and Confidential where Top Secret referred to information that required high degree of protection and confidential being the least sensitive (GRN,

1996). In view of the above, CSRM-TC proposed for the classification of data stored by O/M/As to control the identified cyber security risks in the NPS.

2.2.1.3 Security Management Controls

After the cyber threats were identified and classified, they needed to be managed and controlled. Calder and Watkins (2012) highlighted that organizations needed an information security management system to be able to make informed, practical decisions about what security technologies and solutions to deploy. They further advised that a risk management plan with the objectives of eliminating or reducing them to an 'acceptable' levels either by living with them while exercising carefully the controls that keep them acceptable or by transferring them, by means of insurance, to some other organizations was crucial. In the same vein, CSRM-TC incorporated a cyber-security risk management framework for the NPS. It further developed strategies as road maps that would enable O/M/As to move from where they are now to the proposed stage.

According to Ifinedo (2012) researchers had noted that organizations that paid attention to technical as well as non-technical means of protecting their information assets and resources were likely to be more successful in their attempts to protect their key information system assets. He therefore advised organizations to utilize multi-perspective approaches for protecting their IS assets and resources. Similarly, CSRM-TC adopted a multi-perspective approach by considering both technical and non-technical means of addressing cyber security risks. The model had considered the fact

that information security was not just a technology concern but the management of user behavior of was essential for cyber security.

2.3 The Key Players in Cyber Security

Jaccard and Nepal, (2014) stated that weaknesses in network protocols were complicated when both System Administrators and users had limited knowledge of the networking infrastructure. They clarified that weaknesses in security efforts simply resulted when System Administrators did not use efficient encryption scheme, did not apply recommended patches on time, or forgot to apply filters or policies. Pilling and Works (2013) observed that one pitfall in many organizations was the lack of knowledge and understanding between the IT managers and employees, which resulted in a poor defensive posture. CSRM-TC also found it essential to identify gaps related to security updates and patches during the study.

According to Mclean (2013) cyber incidents could be caused by a variety of factors including vulnerable IT systems and networks, insecure email, lost and stolen devices, social engineering, employee actions, system errors and organized crime gangs.

Based on the above, evident that IT members of staff and all other users at different levels were responsible for protecting information systems. Therefore, with that in mind, it was crucial that CSRM-TC ensured that the relevant training needs for all individuals were studied. Appropriate training would enable them to be technically conversant with IT systems or devices in place, and to be competent in configuring them or operating them safely.

2.4 The Significance of Cyber Security Policy in an Organization

Knapp et al. (2009) indicated that the development of an information security policy was the first step toward preparing an organization against attacks from internal and external sources. They further highlighted that other researchers assured that managerial polices may be more effective at reducing computer security incidents than many electronic devices. Similarly, the NPS requires policies to enhance a better protection effort against cyber security threats in addition to the available technologies.

According to Von Solms (as cited in Knapp et al., 2009) policies were especially important to information systems security as they provided the blueprints for an overall security program and created a platform to implement secure practices in an organization. The objective of policy is to provide management direction and support for information security in agreement with business requirements and relevant laws and regulations (ISO/IEC, 2005). Similarly the development of cyber security policies in the NPS would create a platform to all O/M/As to implement secure practices on information assets.

Jirasek (2012) emphasized that network security should be based around formal security policies. He clarified that they should be available from high-level natural language non-technical policies created by management, down to device and vendor specific policies, or configurations, written by network system administrators. In view of this, it was vital that CSRM-TC adopts a cyber security policy framework that

encompasses policies, standards, guidelines and procedures to guide O/M/As execute their duties as expected.

Kritzinger and Solms (2010) stated that information security awareness, education and training is one of the most important aspects to enforce information security in an organization. Similarly, the CSRM-TC model addressed the training aspects for all staff members at different levels.

Moore (2012) outlined that to solve problems of growing vulnerability and increasing crime, policy and legislation must coherently allocate responsibilities and liabilities so that the parties in a position to fix problems have an incentive to do so. In support of the above, CSRM-TC policy framework had considered the national cyber security legal framework draft that was developed with assistance of the International Telecommunications Unit (ITU) through the Harmonization of ICT Policies in Sub-Sahara Africa (HIPSSA) project. The framework was developed to address electronic communications, cybercrime and data protection in Namibia (HIPPSA First Mission Report, 2013). The draft bill was being studied for endorsement by cabinet (Kaze, 2014). However the security policy aspect needed to be addressed in order to give directives to IT officials on how to manage risks associated with the growing vulnerabilities.

2.5 Good Practices by other countries

Mauritius has defined a risk assessment methodology for the Civil Service. The IT Security Unit was leading the implementation of ISO/IEC 27001 Information Security standard in the Civil Service as part of National Information and Communication Technology Strategic Plan (NICTSP) of 2007-2011 and 2011-2014.

In Rwanda the Ministry of Education introduced different Information Security Course Modules in the overall IT or Computer Engineering program in higher education. In the ICT skills development plan, an IT Security Training and Certification Program was developed. In addition, a National Cyber Security Awareness and Training Program was developed. The aim of this was to promote cyber security awareness for internet users and to promote the development of security professionals that support the public and private institutions to protect their critical systems against cyber threats.

In Brazil the ABNT defines the Brazilian versions of ISO IEC standards (e.g. ABNT NBR ISO/IEC 27000 series). Through that, the CEPESC – Research and Development Center for the Security of Communication Developed scientific and technological research applied to projects related to the security of communications including technology transfer. CAIS RNP also developed the Security Incident Response Team to acts in the detection, solution and prevention of security incidents in the Brazilian academic network, besides creating, promoting and spreading security practices in networks. There is also a CGI.br - the Brazilian Internet Steering Committee that was responsible for recommending technical standards and good practices related to the Internet, and promoting security best practices.

Korea on the other hand developed a National cyber security measures for a systematic government-level response to various cyber threats to national security, including four strategies established with a goal to realize powerful cyber security: To strengthen promptness of cyber threat response system, to establish smart cooperative system for relevant agencies, to reinforce robustness of cyber space security measures, to build creative basis for cyber security.
The Personal Information Protection Normalization Plan was also developed to promote a general approach for information management and protection of system, technology & rights.

National Information Security Index: An objective and quantitative measure for assessing the information security level of the private sector (enterprises and individual internet users)
in Korea. In 2013, the e-Governance Academy of Estonia and the e-Government Center of the Republic of Moldova implemented a cybersecurity project with 3 main components: The first component consisted in developing a Cyber Security Roadmap for Moldovan government institutions. The second component consisted in developing minimum requirements for digital information security for government institutions, or what governments should do in order to secure digital information and the third component was more generally responsible for, raising awareness among government officials and Moldovan citizens on current risks and threats in relation to cyber security.

It is evident from the practices by other countries above that different initiatives were developed in order to address the issue of cyber security. These included, technical measures, legal measures, organizational measures, cooperation and capacity building. Similarly, the CSRM-TC could consider similar measures and lessons learned to develop a suitable framework for the NPS.

The next chapter will focus on the methodology employed for the purpose of this study.

2 RESEARCH METHODOLOGY

This chapter outlines the methodology used for the study. The population and sample size, design of the research instruments, procedure and an overview of data analysis were also presented. The chapter further highlighted the ethical consideration adhered to throughout the study.

3.1 Research Design

The study was designed to use qualitative research methods. A case study in the form of an exploratory qualitative research design was used to carry out an in-depth analysis of the behaviors of IT staff at different O/M/As when managing various information assets, in the absence of cyber security best practices. Surveys and face to face interviews were conducted to understand cyber security risks facing the NPS. Qualitative methods were used to count and classify features of different threats and vulnerabilities identified as well as to construct statistical models and figures to explain findings of the study.

2.2 Population

The population of the study comprised of all IT Managers, Systems Administrators and Analyst Programmers from the twenty-nine (29) O/M/As of the NPS. This population was selected because it consisted of all people that were directly responsible for managing the security of various information assets within the NPS.

2.3 Sample

Probability and non-probability sampling techniques were used to select the sample from the targeted population. Fourteen (14) O/M/As were randomly selected and two (2) O/M/As were purposively selected namely: the Office of the Prime Minister (OPM) and the Ministry of Information and Communication Technology (MICT). Note, the sample also consisted of one (1) IT Manager, one (1) Systems Administrator and one (1) Analyst Programmer from each selected O/M/As.

The OPM was purposively selected because it consisted of the Department of Public Service Information Technology Management (DPSITM), a unit that is mandated to co-ordinate all informatics activities on behalf of all O/M/As in the NPS. On the other hand, the MICT was selected because it is the custodian of ICT in the country.

2.4 Design of Research Instruments

Data was collected from various O/M/As through semi-structured interviews and mixed questionnaires where both open and closed questions were asked. In order to appropriately address the research questions posed for the study, the questionnaire was divided into three (3) sections namely Section A, B and C. Each section covered questions that were targeted at a specific group of IT staff members that were trusted to provide required information. Section A was targeted at IT managers, and high-level questions that demanded for strategic views were asked. Section B was targeted Systems Administrators, and high-technical operational information was required. The

last section, Section C was targeted at Analyst Programmer where by information relating to application development security was collected.

2.5 Research Procedures

After pilot testing and adapting the questionnaire, it was administered to all targeted forty eight (48) respondents from the three (3) groups namely, IT Managers, Systems Administrator and Analyst Programmer from the selected O/M/As. Data was collected, coded and processed using the Statistical Package for Social Sciences (SPSS) while charts and graphs were generated in Microsoft (MS) Excel. Data cleaning process was further conducted through random selection of entries and cross checking with questionnaires in order to ensure the integrity of the data set.

3.6 Data Validation and Synthesis

The challenge throughout the data collection and analysis was to make sense of data and derive meaning necessary to construct a framework. The researcher developed graphs and tables from the data collected through questionnaires. The data from the interviews was used to validate the data collected from questionnaires. The researcher shared the summary of questionnaire data and scripts from interviews with fellow IT colleagues who were also IT staff members at the Office of the Prime Minister at the Department of Public Service Information Technology Management. This Department consisted of highly trained officials responsible for overseeing and coordinating the IT operations of the NPS (IT Policy, 2004). Discussion from colleagues confirmed the

researcher's designations. The scripts from the interviewees were helpful in cross-checking the data and served as a secondary analysis.

The data from interviews and questionnaires was combined for enriching and explaining purposes. The study developed a new theory by developing a conceptual framework. Thereafter recommendations based on the findings were developed.

3.7. Research Ethics

All questionnaires were anonymous so that the identities of the participants was not disclosed. Appointments for interview were made in advance with the selected IT Managers. The purpose of the study was explained before commencing the interviews and administering the questionnaires. Respondents were also assured that the information provided would be treated with confidentiality and anonymity. The data collected was purely used for academic purposes.

3.8 Data Analysis

Descriptive statistics (frequencies and percentages) were used to analyze the responses in MS Excel. SPSS was used to calculate frequency counts of the responses. Tables, graphs and charts were further constructed in Excel to illustrate the frequencies of the responses in percentages. An Impact/Probability Chart was used to analyze the probability of cyber security risk occurrences and their possible impacts on the NPS.

4. RESULTS

This chapter presents the results of data collected during the study. The data was collected from the targeted sample using questionnaires and interviews. This was, therefore further grouped, summarized and presented in the form of graphs, charts, tables and themes.

In order to appropriately address the research questions posed in this study, the responses from questionnaires were divided into three (3) sections namely Section A, B and C. Section A was targeted at IT managers, and high-level questions that demanded for strategic views were asked. Section B was targeted at Systems Administrators, and highly-technical operational information was required. The last section, Section C was directed at Analyst Programmers in order to get an insight on the application development aspect of information security.

The questions were designed to look at operational and strategic security gaps in various O/M/As of the NPS.

4.1 Section A: IT Managers

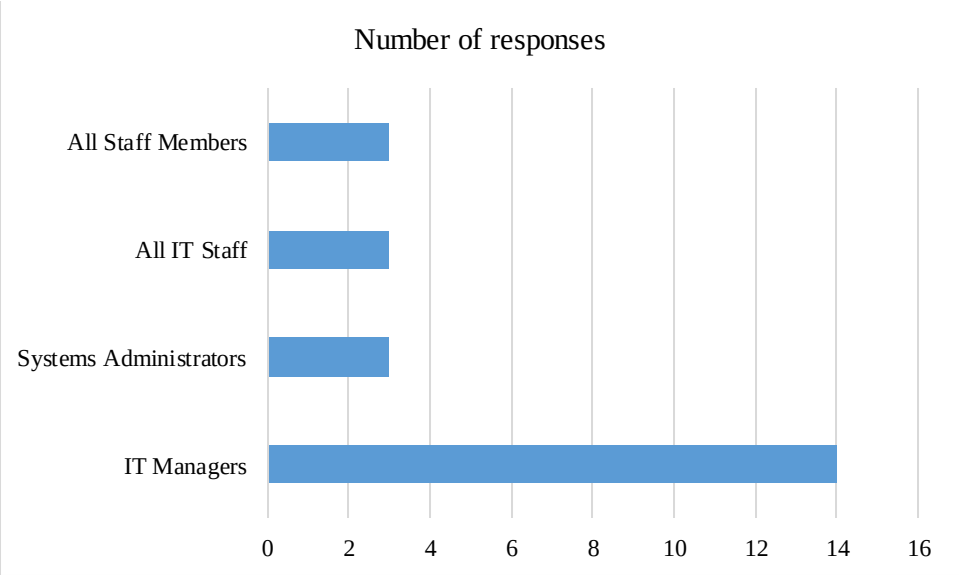


Figure 4. 1: *Accountability for information systems security*

IT Managers were asked to express their views on who they considered as being accountable for the information systems security in their O/M/As. Four options were provided namely; IT Manager, Systems Administrators, All IT staff and staff members. About fourteen (14) managers indicated that they should be held accountable for all information systems security concerns in their O/M/As, while all the other felt that they were not accountable.

Table 4. 1 *Order of priority for effective security*

	Advanced security equipment	**Qualified IT security staff**	**User education and training**
1st Priority	4	16	4
2nd Priority	12	5	7
3rd Priority	9	2	13

The participants were asked to prioritise among the three options on what they consider as significant towards effective information security. The options were advanced security equipment, qualified security staff and user education and training. Qualified IT security staff was rated as first, followed by advanced security equipment while user education and training was regarded as least important by the majority of respondents.

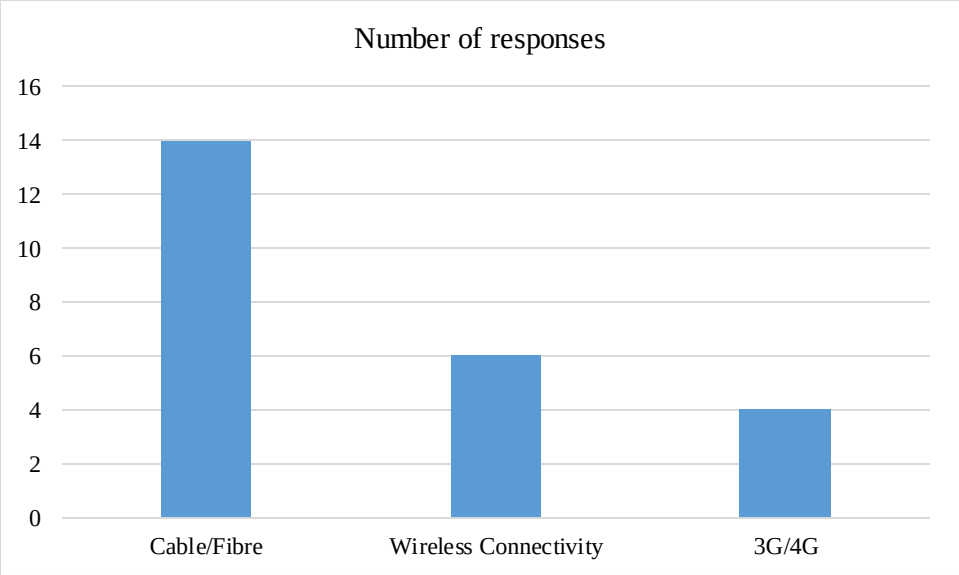


Figure 4. 2: *Type of Internet connection available in O/M/As*

The IT managers were also asked to indicate the types of internet access/connections available in their O/M/As. Ten (10) of the respondents acknowledged the presence of mobile broadband. Out of the ten (10), wireless internet connectivity were six (6) while the remaining four (4) was of 3G/4G connections accessible through mobile phones, USB wireless modems, tablets and IPADs.

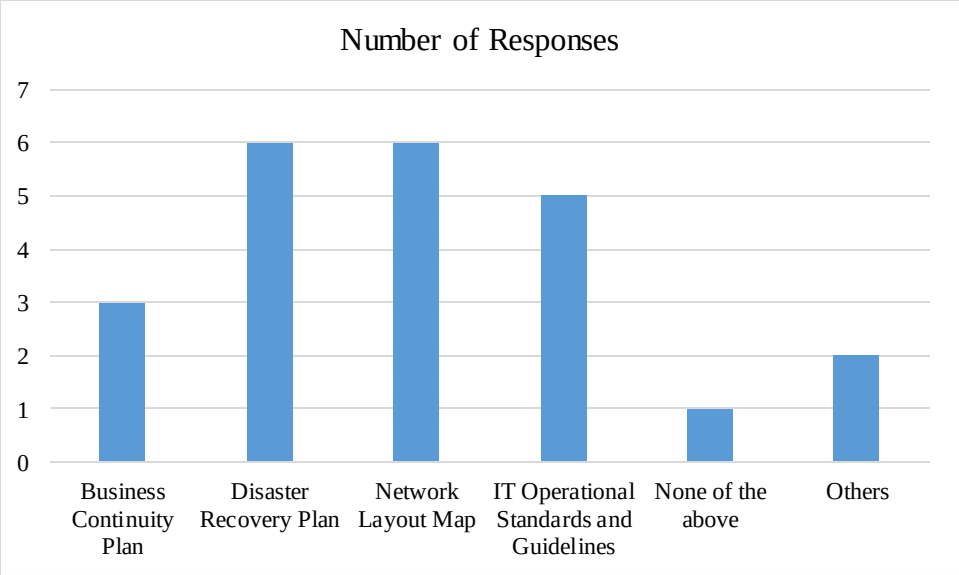


Figure 4. 3: *Documentation in place*

In the study conducted, only three (3) of the respondents indicated that they have business continuity plan in place. Six (6) indicated that they have disaster recovery plan in place. Five (5) indicated that they have IT operational standards and guidelines. About two (2) indicated that they have other documentation in place which includes IT security policy draft, infrastructure optimization plan, disaster risk reduction plan, IT equipment user policy and authentication policy.

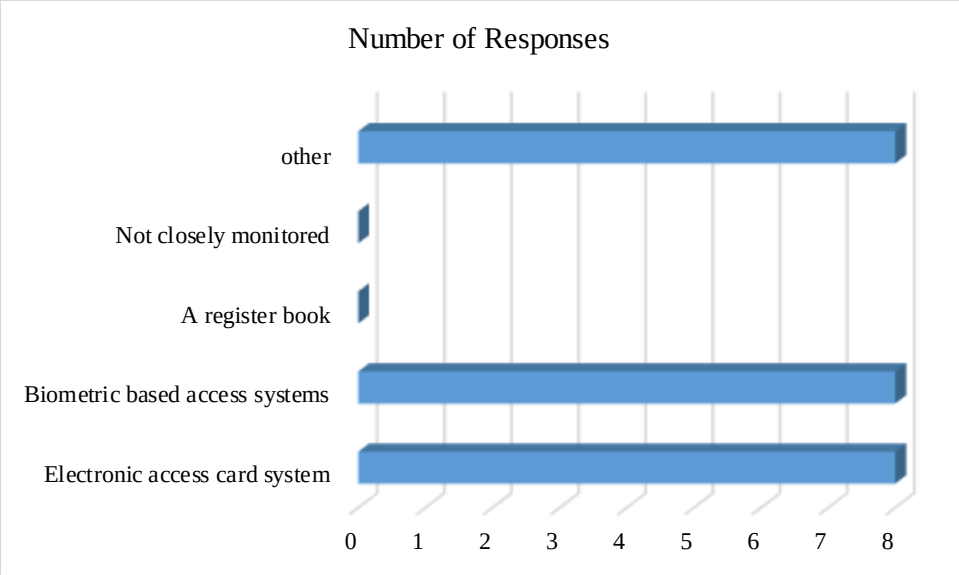


Figure 4. 4 *Physical access control to the server room*

Regarding physical access to the server room, respondents were requested to indicate the types of monitoring systems they have put in place at their O/M/As. It was interesting to learn that all server rooms for all the respondents were monitored in one way or the other. About eight (8) managers responded that they use Electronic Access Card systems while another eight (8) used Biometric Based Access System. Other physical access monitoring systems that were also presented included locked doors, CCTVs and electronic keypad which also represented eight (8) occurences.

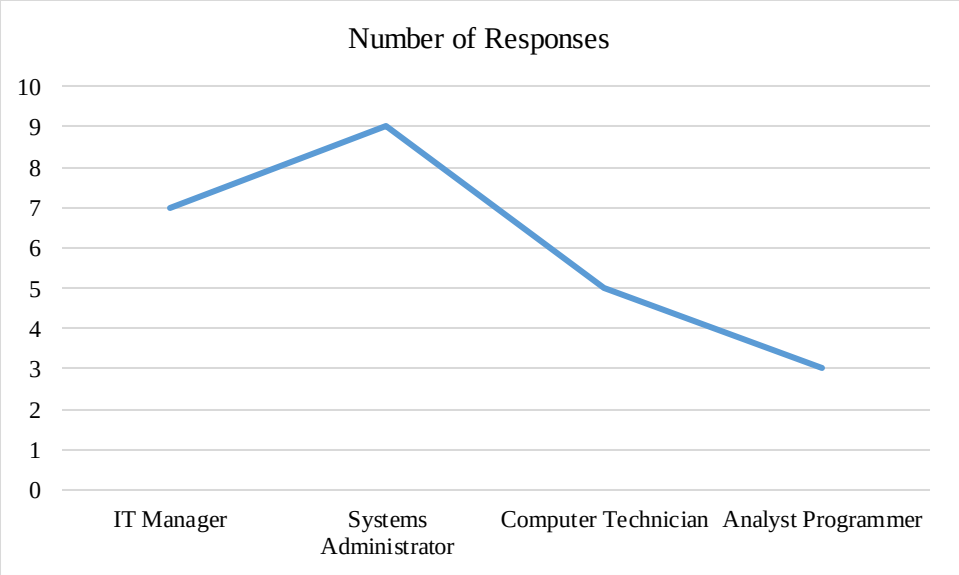


Figure 4. 5: *IT staff members with administrative rights to information systems and networks*

Regarding administrative rights to information systems and networks, it was clearly indicated that all IT positions were associated with some sorts of administrative right/ privileges at varying levels. The dominating group being Systems Administrators represented nine (9), followed by IT Managers with seven (7) and the least presented group was the Analyst programmers taking three (3) responses.

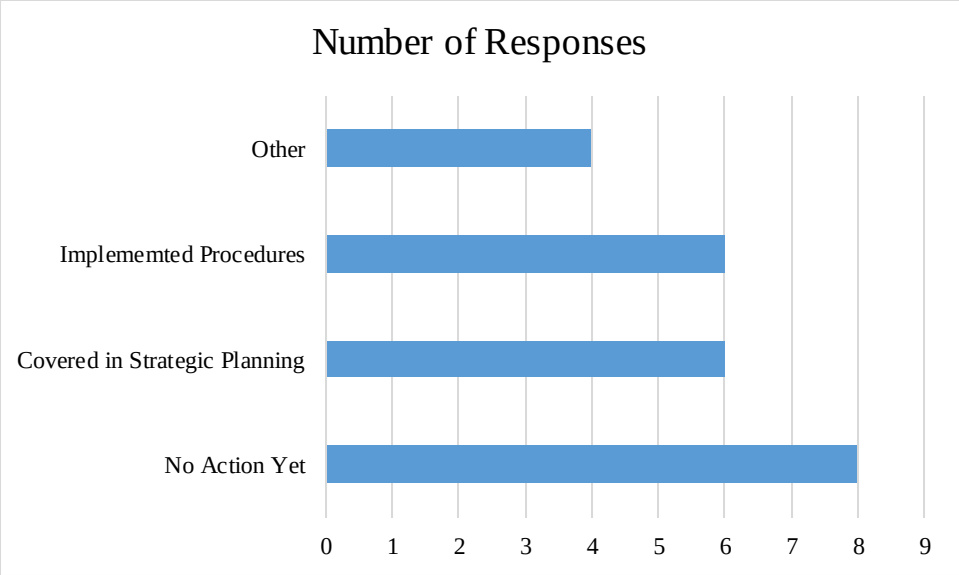


Figure 4. 6: *Actions taken to prevent cyber crime*

During the study, IT managers were asked to indicate if they were aware of cybercrime. It was very interesting to learn that all interviewed managers, representing twenty four (24) of respondents indicated that they were all aware.

The Managers were further asked to indicate the kind of procedures they had put in place at their O/M/As to enhance cyber security. As shown in Figure 4.6 above, eight (8) of the respondents indicated that they had not put in place any control measure to deal with cybercrime. About six (6) said they had covered it in their strategic planning, adding that they looked at the new IT solutions and included them in their annual and five-year strategic budgeting. Four (4) indicated other control measures like blacklist, whitelist, Kaspersky Internet Security (since it has network attack blocker and firewall) and dedicated equipment.

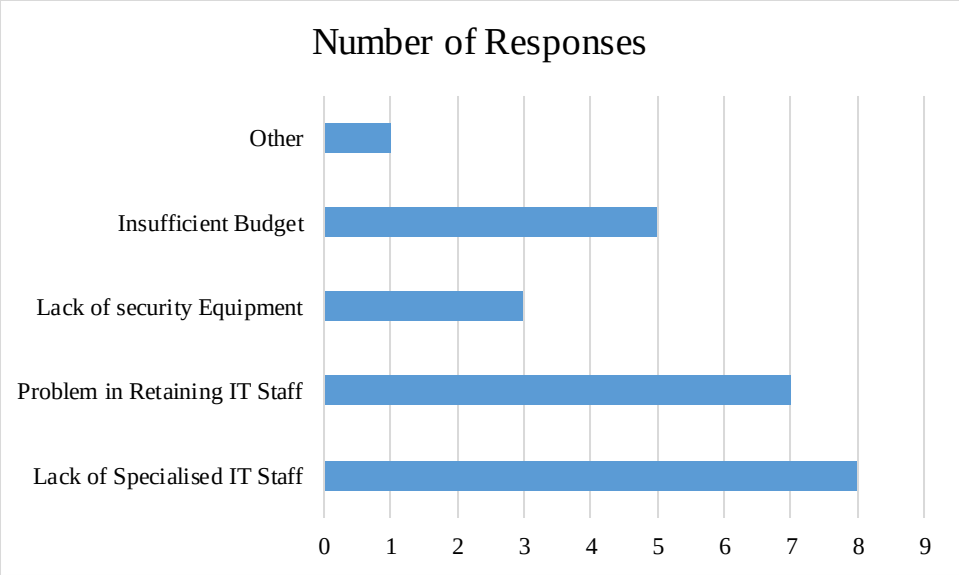


Figure 4. 7: *Security challenges facing O/M/As*

The IT managers were also asked to present their views on what they feel are the challenges facing their IT units or O/M/As in managing the security of their equipment. The majority of the respondents, representing (8) felt that the lack of specialized IT staff is the main challenge towards their security. Seven (7) of the respondents felt that the main challenges facing them was the problem of retaining IT staff. About (5) indicated that they do not receive sufficient budgets allocations to cater for their information security needs.

4.2. Section B: Systems Administrators

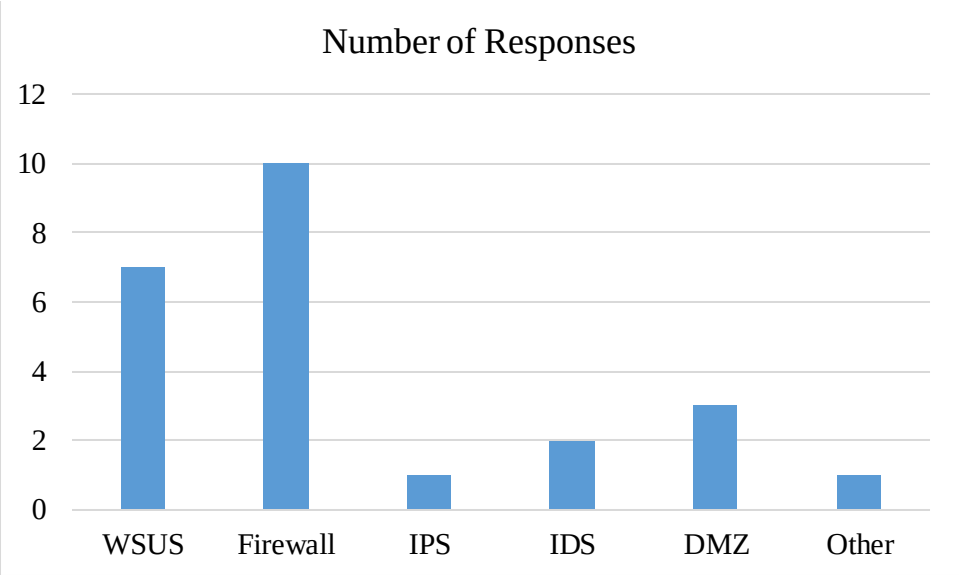


Figure 4. 8: *Security technologies in place in the Namibian Public Service*

Figure 8, presents the percentage distribution of the available security technologies in the NPS. It was quite interesting to learn that (7) of the respondents indicated that they had WSUS, a Microsoft update servers and (10) had firewalls. The IPS and IDS were only represented by (1) and (2) respectively. Other security technologies that were indicated included domain controller, antivirus server, and access system. This also represented (1) of the responses.

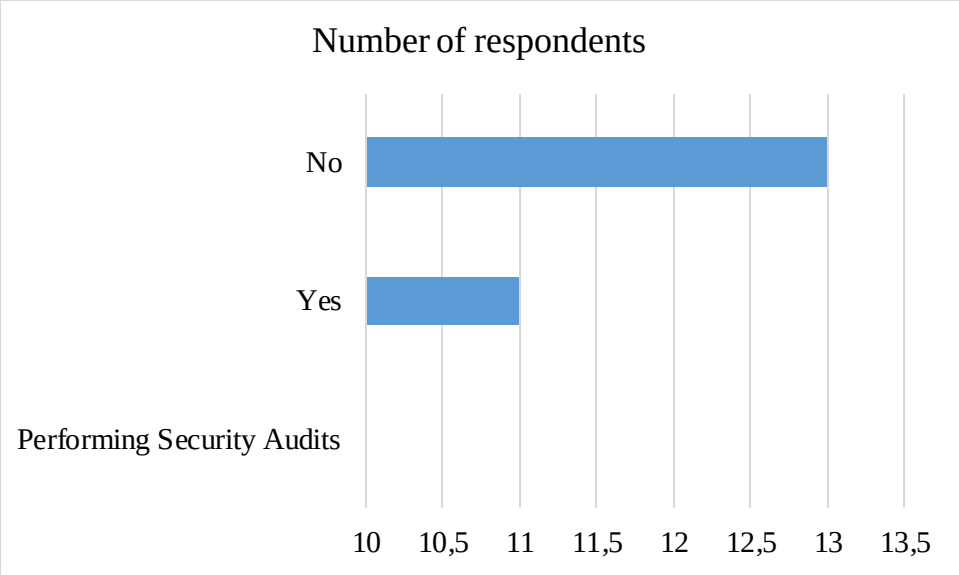


Figure 4. 9: *O/M/A performing security audit on information systems and networks*

Fig 4.9 shows the results of security audits responses collected during the study. Only eleven (11) of the respondents indicated that they perform security audits on their information systems and networks while the remaining (13) of O/M/As do not.

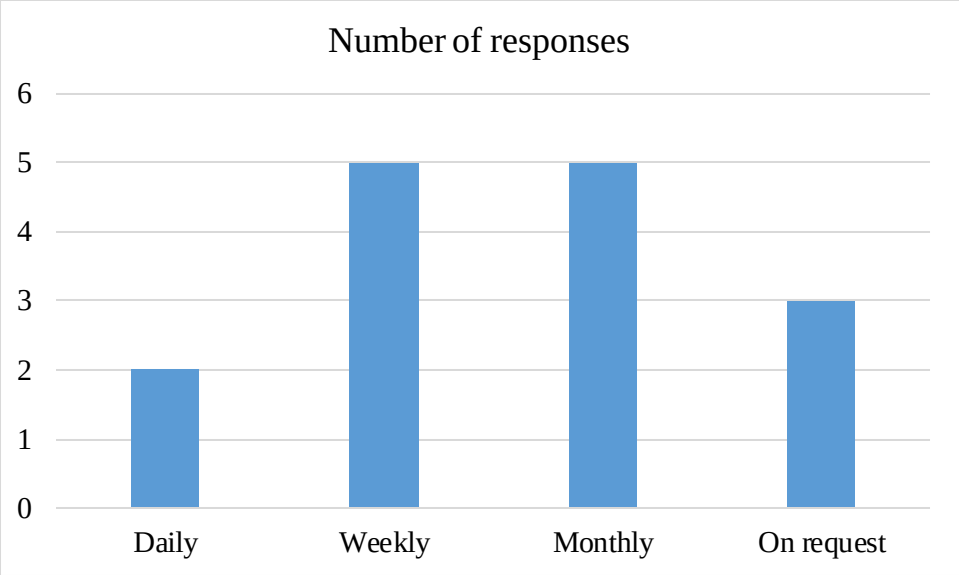


Figure 4. 10: *Security audit frequency*

The results further showed that out of those that performed security audits on their information systems and networks, the majority, representing (7) performed on a monthly basis. Only (6) performed daily while only (3) execute them on request.

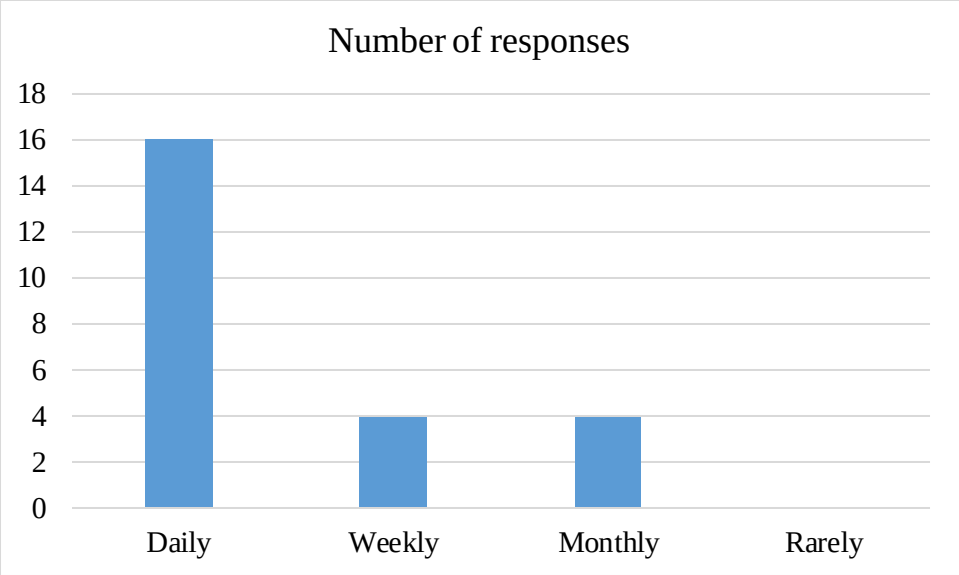


Figure 4. 11: *Antimalware definition update*

The study showed that only (16) of the participated O/M/As were updating their antimalware definition files daily while the remaining (8) was either doing it on weekly or monthly basis.

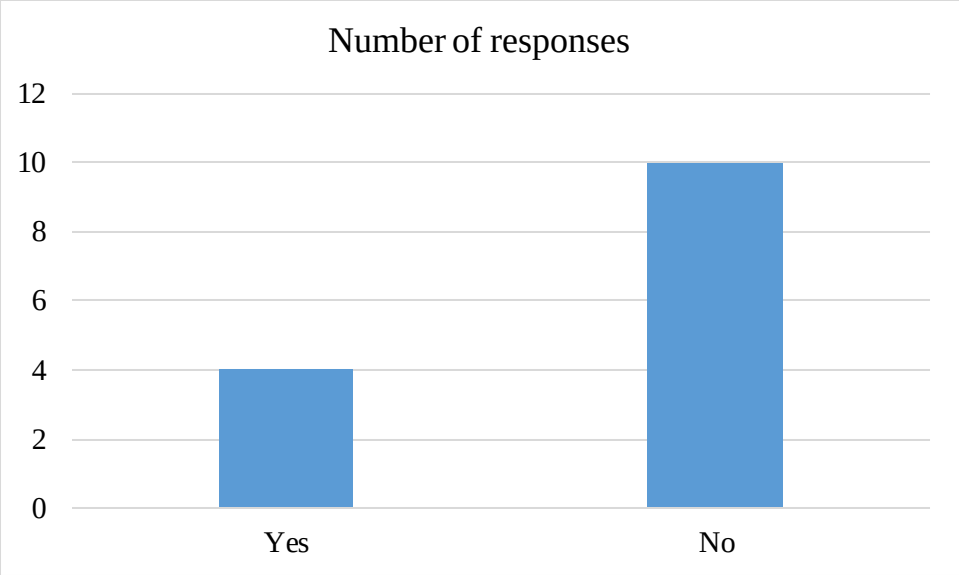


Figure 4. 12: *DNS scanning*

The respondents were asked to indicate whether they performed DNS scanning at their O/M/As in one way or the other. It was notable to learn from Figure 4.13 above that (10) of the interviewed O/M/As did not perform DNS scanning.

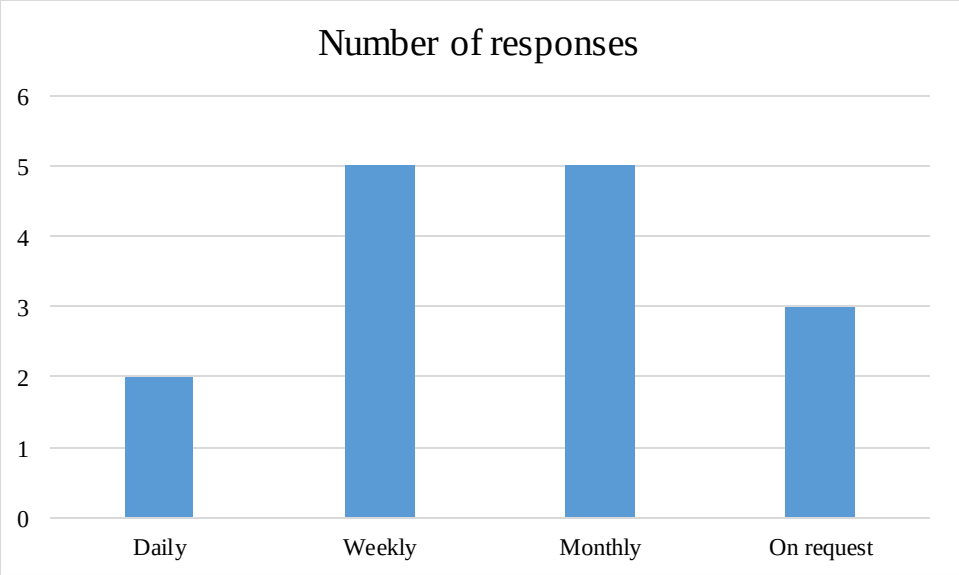


Figure 4. 13: *DNS scanning frequency*

Out of the fourteen respondents (14) that performed DNS scanning, ten (10) did it on either weekly or on monthly basis, while others only executed them on request.

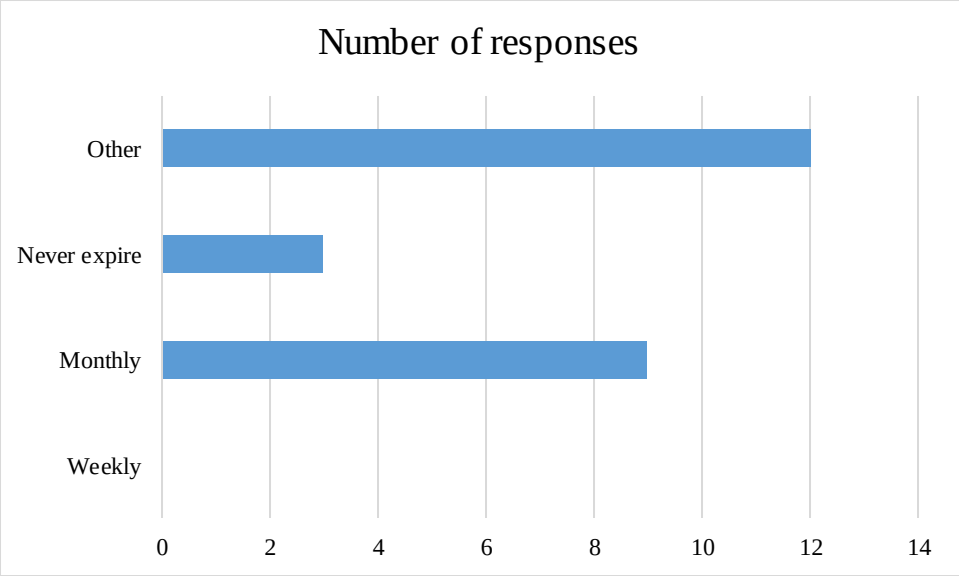


Figure 4. 14: *Password validity*

Information was also gathered on the duration taken for user passwords to expire at various O/M/As under study. About nine (9) of O/M/As indicated that their passwords took a month to expire and three (3) indicated that their passwords never expired. Twelve (12) of the participants gave other time frames including three (3) and two (2) months. Some indicated that their passwords were only changed when a user requested. Other respondents also indicated that at their regional offices or for the PCs that were not joined to the domain, the passwords did not expire.

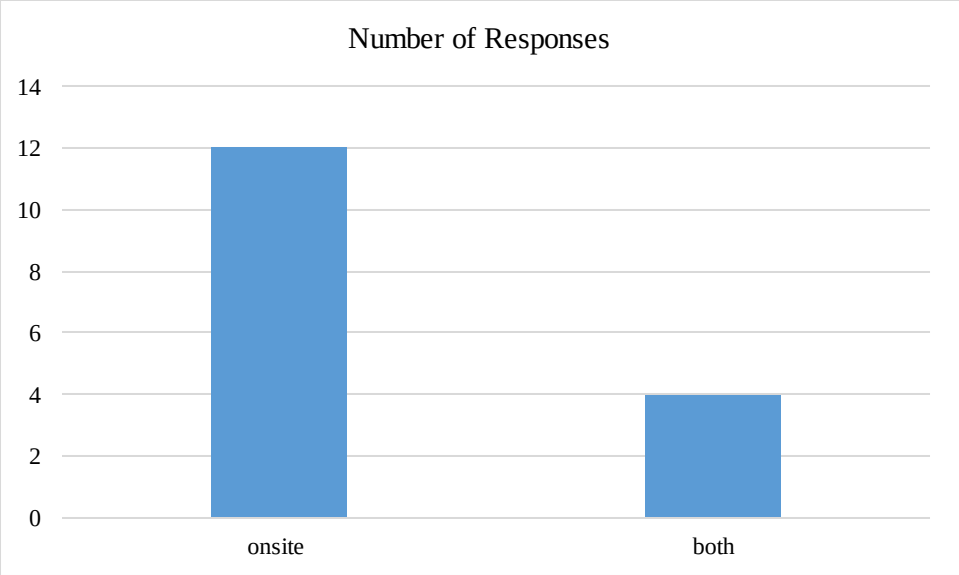


***Figure 4. 15**:Backups*

It was motivating to learn that all O/M/As were performing backups. However, out of the group that performed backups, only (4) of them kept their backups both onsite and offsite, while (12) only kept onsite.

4.3 Section C: Analyst Programmers

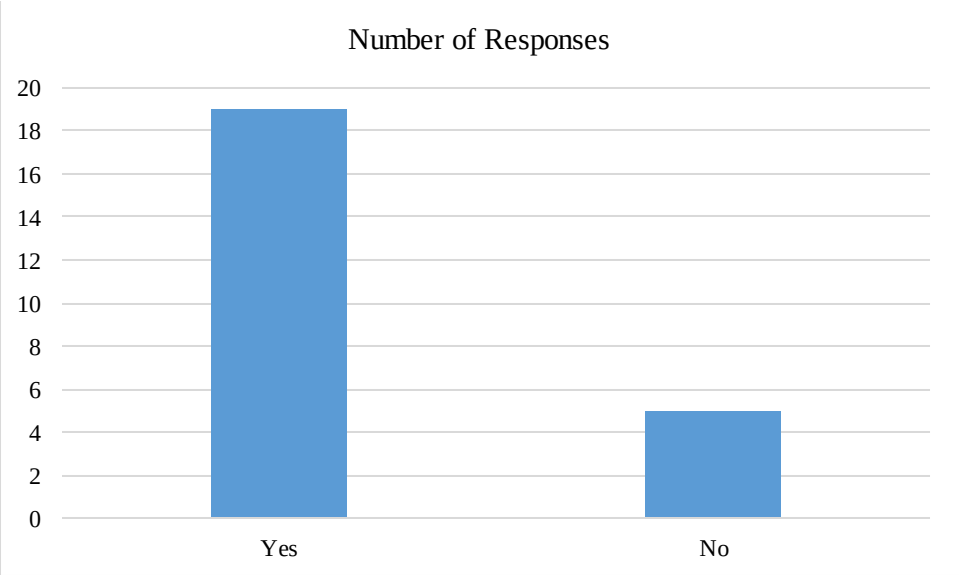


Figure 4. 16: *Application development security related course attended*

The Analyst Programmers were asked to indicate if they had ever attended a course related to application development security. Approximately (15) of the participants indicated that they never attended such courses, whilst (9) indicated that they did attend similar courses.

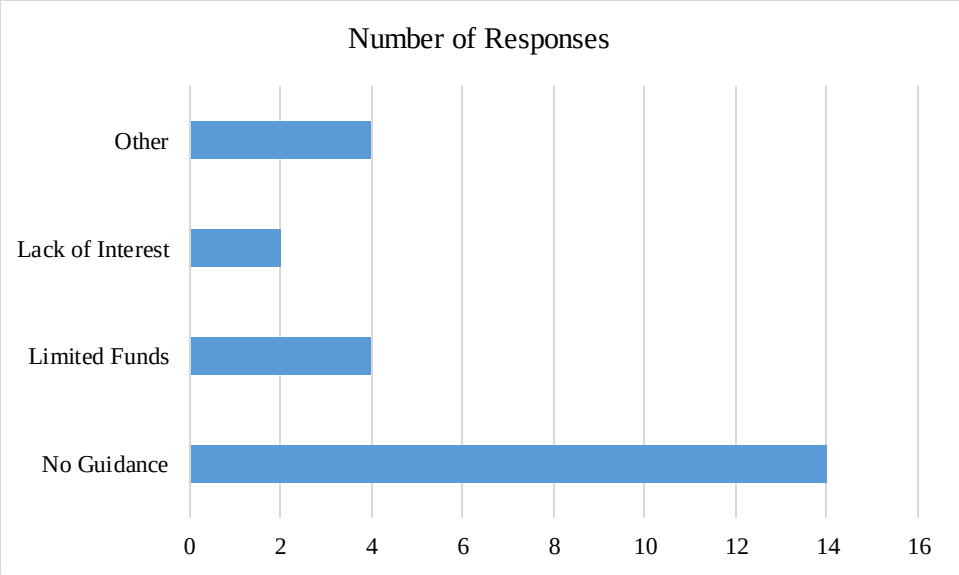


***Figure 4. 17**: Reasons for not attending courses related to application development security*

From the group that never attended a courses on application development security, about fourteen (14) stated that there were no guidance from the senior staff members. Two (2) said they lacked interest while another four (4) indicated that they were not granted from the training committees.

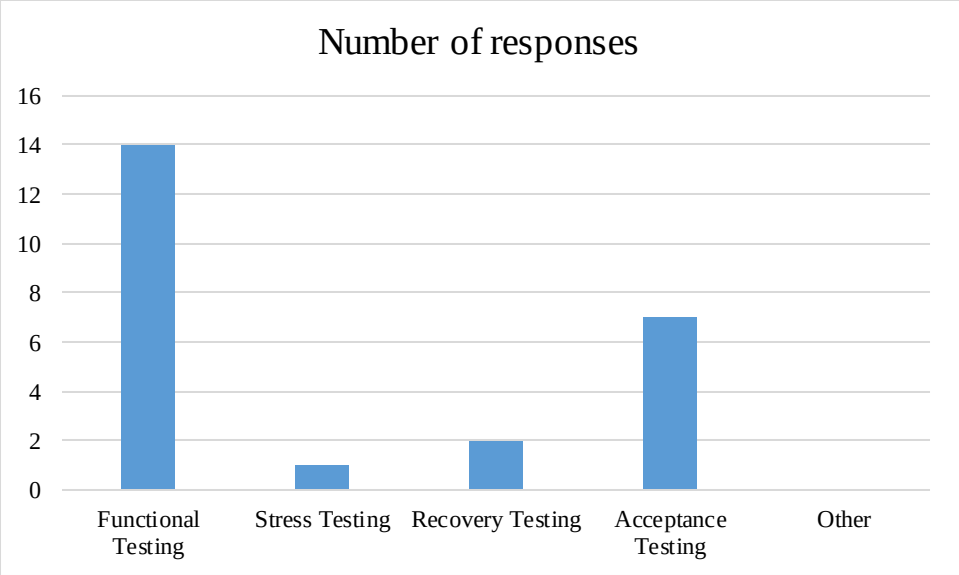


Figure 4. 18: *Application tests performed by Analyst Programmers*

Information was also collected regarding the type of testing that Analyst Programmers performed on the applications they developed. About fourteen (14) of the interviewed Analyst Programmers said they always performed functional testing whenever they were testing their applications and seven (7) indicated that they performed acceptance testing. Recovery testing and stress testing was only represented by (2) and (1) responses respectively.

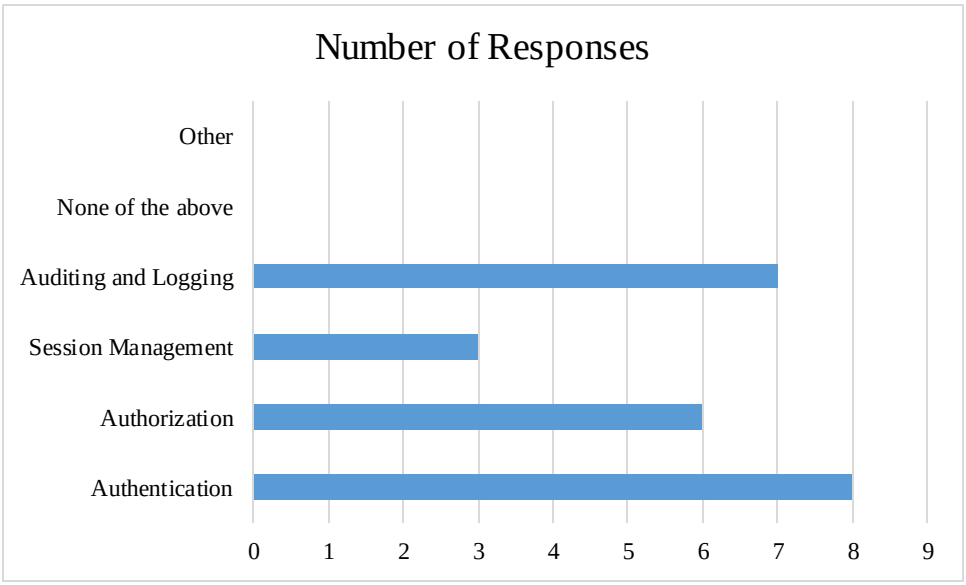


Figure 4. 19: *Security features/measures incorporated during application development*

Information regarding the type of security measures incorporated by Analyst Programmers when developing applications was also collected. About eight (8) of the respondents included authentication, and six (6) catered for authorization. Three (3) incorporated session management features and (7) included auditing and logging.

In the next chapter, results and findings are discussed in relation to the objectives of the study.

5. DISCUSSION

The discussion chapter examines the results of data collected during the study, in relation to research questions. The questions posed in the first chapter of this thesis were discussed and answered separately. The sub-questions were answered first and thereafter the major question was tackled.

The essential purpose of the study was to understand cyber risks facing the NPS as a result of the lack of security best practices. The ways in which various O/M/As were managing the security of their information assets was assessed. The objective of the study was to advice IT managers and senior officials in the NPS with the necessary information regarding the importance of security policies, standards and guidelines to provide overall protection for information systems networks across all O/M/As.

With the growing dependency of societies on ICT and Internet, the existing literature has shown that it is important for organisations to protect their information assets against cyber threats to avoid IT-security incidents. Panda et al. (2006) stated that all segments of society had become more dependent upon networking and IT, and this same technology became an increasingly tempting target for malicious activity. Graham et al. (2011) also observed that every day, new vulnerabilities and malicious code threatened systems on networks. Maskun et al. (2013) identified three (3) classes of attacks that were possible from Internet, namely service disruption, theft of assets, as well as capture and control. They further advised that to eliminate or dismiss cyber risks, protection of cyberspace infrastructure is needed in order to stop hackers from committing crimes.

In support of the above authors, it would be equally important that the NPS adopt cyber security best practices such as ISO 27000 series, to prevent or reduce cyber risks and protect the Government IT infrastructure across all O/M/As. Furthermore this adoption of cyber security best practices would be required to maintain the confidentiality, integrity and availability of information also referred to as CIA triad.

Barman (2002) advised that the only way to understand your infrastructure was to perform a full risk assessment on the entire enterprise and then ensured that information security policies appropriately addressed diverse threats. Similarly, a risk assessment was conducted in the NPS to collect sufficient information that could be used as inputs to the development of the CSRM-TC model.

Other important aspects regarded to be crucial in the management of security risks included: configuration management and control, business continuity and disaster recovery, incident response planning, security training, physical / logical security, personnel security, security assessments, access control mechanisms and encryption technologies.

5.1 What cyber security risks are facing the Namibian Public Service?

For the purpose of this study, the researcher learned that in order to successfully understand the security risks facing the NPS, it was important to first identify the information assets that needed to be protected against security threats. Thereafter, the

possible threats and vulnerabilities facing those assets would be identified and analyzed to determine the potential risks.

In this study, a cyber-security risk (hereinafter referred to as risk) is defined as the potential loss, damage or destruction of an information asset as a result of a cyber-threat exploiting vulnerability. A threat is defined as an object, person or other entity that represents a constant danger to an asset (Whitman & Mattord, 2008). Donald Pipkin in his book defined system vulnerability as a condition, a weakness of or an absence of security procedure, or technical, physical or other controls that could be exploited by a threat (as cited in Kizza, 2013).

5.1.1 Information Assets Identification

According to Rok and Borka (2008) the first step in security risk analysis process was to identify the organization's information assets. They defined these assets as information and resources that had value to the organization. CSRM-TC identified six types of information assets in the Namibian Public Service to be considered for cyber security. These were hardware, software, data, people, services, procedures and networks.

5.1.1.1 Hardware

The hardware that were identified during the study included all physical computing devices and network related equipment. These included computers, laptops, cellular phones, tablets, printers, servers, routers, switches and firewalls. The identified hardware needed to be protected against physical theft and unauthorized access. When some of these assets are lost or stolen, the value of information inside them might be much higher than their monetary values. This was particularly risky when an equipment was lost with data that had not been effectively backed up or was too sensitive to disclose. Business operations may also be interfered as a result of such.

5.1.1.2 Software

The software considered for the study included system software, all applications (off-the shelf and custom written) and utilities software. These were considered because it was believed that a gap in the protection efforts for any of these software resulted in software vulnerabilities.

5.1.1.3 Data

Data was believed to be the main target of attack to information systems. The study considered the protection of data at rest, in processing as well as data in transit via communication channels. Data needed to be protected against unauthorized access and integrity violation.

5.1.1.4 People

The people considered, included all public servants, application developers, IT staffs and customers. People needed to be protected and educated so that they would be aware of the safe and unsafe system practices. These would also assist in reducing the chances of risks that occurred as a result of unintentional behaviors.

Other issues considered included:

a) Services

Services included those that rendered within O/M/As, between them, outside to external stakeholders as well as to members of the public. The availability of public services needed to be guaranteed at all times.

b) Procedures

The procedures for carrying out various tasks in the NPS while adhering to the security principles were also considered to be one of the critical matters to be addressed in the NPS for effectiveness.

c) Network Communications

All interconnections or communication channels within and around the NPS network where data could travel through were also identified as crucial.

5.1.2 Threats Identification

Mouna et al. (2014) stated that managers needed to know threats that influenced their assets and identified their impact to determine what they needed to do to prevent attacks by selecting appropriate countermeasures. Threats to the NPS were observed and identified from the information collected during the study. These threats were further classified as either intentional or unintentional.

5.1.2.1 Intentional Threats

a) Infection with Malware (malicious software)

Malware considered in this study included viruses, worms, trojan horses and many other software designed to "infect" computers or install themselves onto them without user's permission. Kim et al. (2011) stated that computers around the world are vulnerable to infections by thousands of newly created malware if update was delayed even to a single hour. The results of this study showed that eight (8) of the participated O/M/As were not updating their antimalware definition files regularly. They were either performing them on weekly or monthly basis.

According to the interview conducted with IT staff members, some IT equipment were not joined to the O/M/A domains hence, it was difficult to have full control of antimalware deployments. They indicated that laptops and standalone PCs that were mostly used at regional offices out of Windhoek were not normally part of the domain. Therefore, they were mostly left out from automated antimalware update deployment.

Jaccard and Nepal (2014) indicated that once malware was carried out to the victim's system, cyber criminals could utilize many different aspects of existing vulnerabilities in the victim's system further to use them in their criminal activities. The results shown in this study therefore showed a gap in the protection efforts of malware threats in the NPS.

b) Insider Abuse

The possibility of insider abuse was identified in reference to the allocation administrative rights to IT staff. The dominating group was Systems Administrators represented by nine (9) respondents**,** followed by IT Managers with seven (7) and Analyst Programmers had three (3) responses**.** Lee (2012) stated that organizations needed to take a close look at the privileged access within their own walls, to make sure that all access rights were appropriate and necessary to those employees using them, and – more importantly – that the information they accessed was being used appropriately at all times.

The interview results showed that the allocation of administrative rights came as a result of the fact that there were no clear boundaries in the duties and responsibilities of the different IT job categories. In most cases the IT Administrators and Analyst Programmers executed the same duties hence the need for administrative rights allocation. COBIT 5 defines information security roles and structures and also examines accountability over information security, providing examples of specific roles and structures and what their mandate is, and also looks at potential paths for

information security reporting and the different advantages and disadvantages of each possibility (ISACA, 2014).

According to the CSI Computer Crime and Security Survey in 2008, the second most frequent incident was insider abuse (Richardson 2008). Besides malicious purpose, people unintentionally made mistakes. In response to insider abuse CSRM-TC identified that the issue of access privileged allocation was not properly managed due to an unclear division of roles and responsibilities.

c) Equipment Theft

Although Figure 4.4 indicated that all O/M/As were active about physical security, equipment theft was one of the threats that were common to any organization and requires continuous monitoring. It appeared that portable devices like laptops and tablets were most commonly vulnerable to these type of threats.

The interview results also showed that some users were only assigned laptops for official purposes. They further indicated that these users were storing the official information locally on the devices and sometimes backups were not performed. That therefore posed a great risk when such equipment got lost or stolen. Although Fig. 4.4 indicates that there were a number of control measures towards physical security, but interviews indicated that monitoring and audit were not done regulary on the systems in place.

5.1.2.2 Unintentional Threats

a) Human Error

Human error may occur when a user provides wrong inputs to the system or when they set wrong configurations. This becomes a concern when users have accounts with administrative rights that enable them to make changes to the devices or application settings. Humphley (2008) emphasized that human error or mistakes in handling data through careless working or lack of training can threaten the integrity of information assets. This possibility of human error threats was also noted in the NPS based on the results of administrative rights allocation and lack of training as shown in Figure 4.5 and Figure 4.17 respectively.

b) Equipment Malfunction

This includes any malfunction to the physical devices as a result of hardware threats. Jaccard and Nepal (2014) indicated that the lack of tools support in hardware detection, and hardware-based attacks have been reported to be on the rise. They referred specifically to the hardware Trojan stating that it could physically destroy, disable, or alter the device's configuration, for example, causing the processor to ignore the interrupt from a specific peripheral.

The lack of hardware threat detection tools were equally lacking in the NPS. This was proved during the interviews when participants indicated that they did not have tools to detect hardware-based attacks.

c) Software Malfunction

Jaccard and Nepal (2014) stated that the majority of cyber-attacks today still occur as a result of exploiting software vulnerabilities (caused by software bug and design flaws) or fault in computer programs (such as internal OS, external I/O interface drivers), and applications. This gap was also identified from the study in reference to the results presented on antimalware updates as well as the lack of security related training for Analyst Programmers when the whooping nineteen (19) respondents indicated that they never attended security trainings.

5.1.3 Vulnerabilities

Rok and Borka (2008) defined vulnerability as a weakness in security procedures, technical controls, physical controls or other controls of an asset that a threat may exploit. They emphasized that although most security incidents were caused by vulnerabilities presented by flaws in software, others were caused by human factors. Kim (2011) advised that the best way to minimize vulnerabilities in software and prevent attacks was to follow best practices in the design, coding, testing, operation and maintenance of software.

The following vulnerabilities were observed in the NPS during the study.

5.1.3.1 Lack of User Education and Training

The aspects of the lack of user education and training was confirmed when IT Managers were asked to present their views on what they pursue as the challenges facing their IT units or O/M/As in managing the security of their equipment. The majority of the respondents, representing eight (8) respondents felt that lack of specialized IT staff was the main challenge towards their security.

Similar observation was also made when Analyst Programmers were asked to indicate if they ever attended courses related to application development security but majority of the participants representing nineteen (19) indicated that they never attended such courses. Further, fourteen (14) of those who never attended these courses indicated that there was lack of guidance from the supervisors while four (4) indicated that the funds were limited.

Sanderson (2011) emphasized that everyone who manages, administers or operates IT infrastructure needed to become security conscious. He emphasized that organizations that assess risks and train staff were more likely to implement security policies, procedures and technologies that protected vital assets. The result shown from the study however shows a gap on the training aspects in the NPS.

Qualified IT security was also not considered as first priority as indicated in Fig 4.1. The procurement of sufficient security equipment was instead preferred as a first priority. However, the (ITU, 2015) report stated that capacity building is intrinsic to technical and organizational measures. The report affirmed that understanding the

technology, risk, and implications could help develop better policies, strategies and organization.

5.1.3.2 Account with Weak or No passwords

Julisch (2013) stated that weak, default or shared passwords continued to be a frequent security problem. Kim (2011) also assured that hackers often exploit weak authentication to break into computer systems.

During the study, information was also gathered regarding the duration taken for user passwords to expire on different applications at various O/M/As. A similar observation made with antimalware updates was also echoed here when three (3) of the respondents indicated that user passwords for PCs that were not joined to the domain never expired. These include portable devices as well as desktop computers used at regional offices.

Twelve (12) of the participants gave other time frames from two (2) to over three (3) months while some indicated that their passwords are only changed when users requested so. Graham et al. (2011) advised that it is important that systems administrators enforce sufficient password construction complexity rules to frustrate both dictionary and brute-force attacks.

5.1.3.3 Unpatched or Outdated Software

Unpatched or outdated software was one of the vulnerabilities identified during the study. In addition to the results showing that seven (7) of O/M/As were not regularly updating their anti-malware applications, only six (6) indicated that they were making use of Window Server Update Services (WSUS) in their O/M/As. According to the Systems Administrators interviewed, WSUS enables administrators to authorize or publish and distribute windows updates automatically within a network. WSUS caters for critical updates, definition updates, drivers, feature packs, security updates, service packs and update rollups. The study showed that only six (6) of O/M/As are deploying windows updates automatically. All in all, windows operating system is widely used in all O/M/As of the NPS.

Shostack (2003) observed that many systems were left unpatched for months, even years, and the consequences of not updating systems promptly with necessary patches could cause severe damage. Rok and Borka (2008) clarified that to fix vulnerabilities in software products, vendors release patches. They advised that organizations must act fast and apply patches to the system as soon as they are released by the vendor in order to avoid damages due to malicious acts. However, the instant application of security patches was not reflected during this study.

5.1.3.4 Missing or Inadequately Documented Policies, Standards & Procedures

In the study conducted, it was noted that three (3) of the participated O/M/As had business continuity plans in place. About six (6) had disaster recovery plans in place, and 5 indicated that they had IT operational standards and guidelines and one (1) indicated that they had none of the stated documentation in place. Also, about two (2) indicated that they had other documentation in place which included IT security policy draft, infrastructure optimization plan, disaster risk reduction plan, IT equipment user policy and authentication policy.

These results presented a lack of standardization and uniformity in the available procedures, guidelines and documentation. These documentations could be of high importance to recover from critical situations should a disaster strike.

5.1.3.5 Backups

One of the vulnerabilities indicated during the study was on backups. Figure 4.16 shows that fourteen (14) of interviewed O/M/As were keeping their backups onsite. However, Westfall et al. (2012) advised that backups should be taken completely offsite to ensure protection against intentional or unintentional deletion of files, server security breaches, server hardware failures, and physical threats to the machine.

The interviews conducted also revealed that data on mobile or portable devices were not regularly backed up. This therefore also presented another information security challenge in the NPS.

5.1.3.6 Adoption of New Technologies

Broadband has gained more popularity nowadays due to mobility convenience reasons. The adoption of mobile broadband technologies including 3G/4G has increased the entry points to the NPS information systems and networks. This was also confirmed during the study when IT managers were asked to indicate the types of internet access/connections that were available in their O/M/As. About ten (10) acknowledged the presence of mobile broadband. Out of the ten (10), wireless Internet connectivity made up six (6) while the remaining 4 was made up of 3G/4G connections accessible through mobile phones, USB wireless modems, tablets, IPads and Wireless Fidelity (Wi-Fi).

The adoption of cloud computing has also enabled staff members to subscribe to cloud applications. This was confirmed when some participants indicated that they were using these services (mostly "Dropbox") to store data and save storage spaces on their devices. This therefore presented another security gap.

5.1.4 Risks

5.1.4.1 Unavailability of Service

As the NPS continues to prosper towards making Namibia a "knowledge based society and technology driven nation" as stated in the Vision 2030 of Namibia, most of the government services are being computerized, automated, and interconnected to improve security delivery.

One of the initiatives towards embracing this is e-Governance. Through this initiative, electronic systems were expected to be accessed by all via Internet through the government web portal. Zhao (2010) observed that the growing popularity of e-Government services on Internet, e-Government sites might become potential targets for cyber attackers and terrorists. Halcnin (2004) stated that cyber intrusions into e-Government network systems could impair e-Government services any time if the e-Government sites were not properly secured. Therefore, given the threats and vulnerabilities identified during the study, the NPS could be at risk of possible unavailability of services should nothing be done to the current situation.

5.1.4.2 Exposure of Sensitive Data

Sensitive data is exposed when confidential data of the NPS is revealed to unauthorized recipients when intruders gain access through weakness in computer systems. Through interviews, the study revealed cases whereby laptops and other equipment of the NPS could get lost or stolen. Other cases also showed how access to

the server room was not audited. Other results showed how different users could all have administrative rights to network resources. Others showed the lack of trainings. Others showed the lack of password management and patches.

5.1.4.3 Identity Theft

When intruders uses identifiers belonging to the NPS to impersonate themselves. The issue of passwords, administrative rights and patches indicated in this study shows a possibility of identity theft if not managed appropriately.

5.1.4.4 Distributed Denial of Service (DDoS) Attack

Jaccard and Nepal (2014) indicated that DNS had been the target of several Denial-of-Service (DoS) attacks. Kim (2011) explained that Denial of Service attacks floods a target computer system with bogus requests, making it unable to provide normal services to intended users.

During the study, respondents were asked to indicate whether they performed DNS scanning at their O/M/As in one way or the other. It was remarkable to learn from Figure 4.13 that ten (10) of the interviewed O/M/As did not perform DNS scanning.

5.1.4.5 Software Defects

To avoid cyber incidents results such as damage to infrastructure, down time, service interruption, exposure of sensitive data, theft of intellectual property and fraud software systems also need to be protected and updated. The lack of security updates on applications and the security training gap identified might lead to instability resulting in software defects.

5.1.5 Risks Impacts

From Chapter 3 above we learned that risk occurs as a result of an intersection between an asset, a threat and a vulnerability. This happens when a threat exploit vulnerability in an asset leading to an unpleasant result as demonstrated in Figure 5.1.

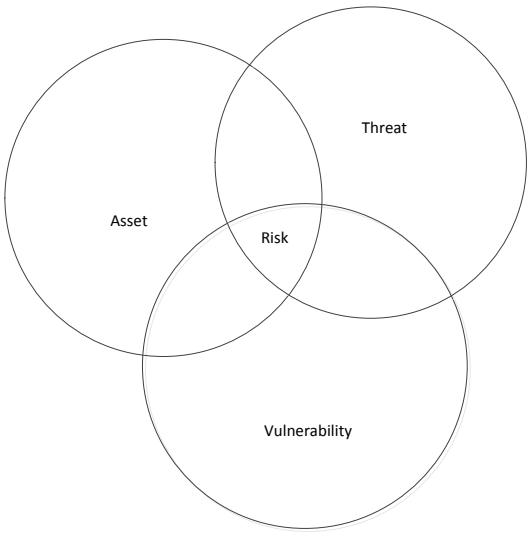


Figure 5.1 *Asset-Threat-Vulnerability-Risk*

Sanderson (2011) stated that in order to assess potential risks, managers must examine each section of the organization's process, looking for security vulnerabilities. He emphasized that managers needed to understand exactly which files, databases and columns are sufficiently sensitive to warrant the additional cost of protection. Contrary to the results shown in Figure 4.1 all IT managers therefore needed to take ownership of the various information systems in their O/M/As and be accountable for all the security responsibilities.

Based on the risks identified, the following impacts were identified.

5.1.5.1 Damaged Reputation of the Namibian Public Service

Damaged reputation was identified as a potential risk as a result of identified physical and technical threats that are capable of causing information compromise or misappropriation. Sanderson (2011) indicated that failing to manage physical and digital information can result in potentially catastrophic financial and reputational damage. Similarly, if the security threats and vulnerabilities identified in this study are not managed, reputational damage may occur in the NPS. Looking at the results presented under from the interviews it was evident that a security risk may spread throughout the government systems unnoticed if no proper monitoring and controls are not put in place.

5.1.5.2 Financial Loss

The financial loss impact may occur as a result of crisis managements of risks, replacement of damaged systems as well as other recovery costs. Also considering the fact that there is no sufficient capacity of security individuals and foundational measures are not in place it is evident that the government may be required to spend money on recovery costs.

5.1.5.3 Loss of Personal Privacy

This would happen when individual's personal data is illegally accessed or obtained from the NPS information systems. Data from this study has shown that, more than one staff members are using a common username and password on certain applications. This in itself provides evidence of danger to personal privacy.

5.1.5.4 Loss of Confidentiality

This may happen in any situation when data is disclosed to any unauthorized individual. Data from the study has supported the possibility loss of confidentiality with the allocation of administrative rights and when staff members share passwords.

5.1.5.5 Danger to Personal Safety

Individuals whose private data is disclosed may suffer more personal harm. The information assets, threats, vulnerabilities and risks identified during the study were summarized in Table 5.2 as follows: The information from the study indicated that there is no close monitoring of systems in terms of who accessed what and so it may not be known when certain information about an individual has been leaked or not. These might land sensitive information of individuals in wrong hands.

Table 5.2: *Security risks identification process*

Information Assets	**Threats**	**Vulnerabilities**	**Risk**	**Impacts**
a) People b) Hardware c) Software d) Data e) People f) Services g) Procedures h) Network communications	a) Malware b) Insider abuse c) Equipment theft d) Human error e) Hardware malfunction f) Software malfunction	a) Lack of user education and training b) Accounts with weak or no passwords c) Unpatched or outdated software d) Missing or inadequately	a) Unavailability of Service b) Exposure of sensitive data c) Identity theft d) Violation of privacy e) Distributed Denial of Service	a) Damaged reputation of the Namibian Public Service b) Financial Loss c) Loss of confidentiality d) Legal actions

		documented policies, standards and procedure e) Backups f) Adoption of new technologies	(DDoS) attack f) Software defects	e) Danger to personal safety

Table 5. 1 *Security risks identification process*

5.2 What strategies can be employed to mitigate risks facing the Namibian Public Service?

The diagram below summarizes the cyber security risks cycle.

The figure shows that a threat exploits vulnerability in an asset, resulting in a risk that causes damages to an asset. These threats therefore need to be controlled to reduce the risk impacts.

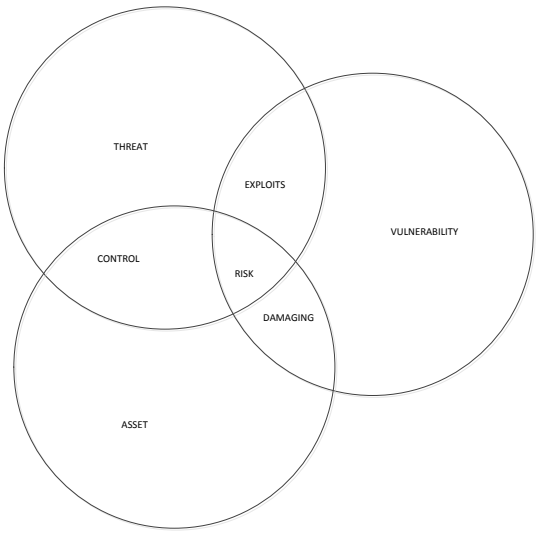


Figure 5.2 Cyber Security Cycle Summarized

Based on the risks identified a qualitative analysis was performed. This was based on probability of occurrence and possible impacts should the risk occur.

The study encouraged that appropriate security measures should be in place to ensure that information assets remain secured and that whatever might happen should not lead to a complete disaster that might halt the NPS operations.

To determine the appropriate strategies that needed to be employed by the NPS there was a need to carry out an assessment of risks identified during the study. This was also supported by Rok and Borka (2008) when they stated that once security risks have been identified, they must be assessed as to their potential loss and to the probability of occurrence. They defined this assessment as the determination of potential effect of an individual risk by assessing the likelihood and impact should it occur. Similarly, in this study, the assessment was conducted on the risks identified to determine their probabilities of occurrence and impacts should they occur. This was performed to assist the NPS in taking informed decision regarding the necessary investment in security controls.

The assessment was also important to enable prioritization of risks so that majority of time and efforts is spent on the crucial dangers.

To prioritize these, an Impact/Probability Chart was used to rate the potential risks and decide on those that requires high level of attention.

With this chart, security risk is viewed from two primary dimensions:

1. **Probability** – the probability of a risk is the extent to which it is likely to happen.
2. **Impact** – An impact on the other hand, is the adverse effect that may result if the risk strike.

In this chart, the probability of risk occurrence was represented on one y-axis. Whilst, the impact, was represented on the x-axis.

The three key risks identified were analyzed in the Impact/Probability chart as shown it Table 5.2.

Probability of Occurrence	**High**			**Unavailability of service**
	Medium		**Exposure of sensitive data**	
	Low	**DoS**		
		Low	**Medium**	**High**
	Impact of Risk			

Table 5. 2 *The risk impact/probability chart*

The chart presents the following information:

- **A Low impact/low probability** – low level temporary risks that may sometimes be ignored.
- **A Medium impact/medium probability** – these are risks with which the NPS can cope but an effort to reduce the likelihood of occurrence is important.

High impact/high probability –very critical risks that requires serious attention and so, they should be prioritized.

To successfully address cyber security risks in the NPS, the attention and resources should go to the medium and high priority areas through adopting various suitable strategies.

The Risk Mitigation Strategy

Mitigation is the choice of reducing the impact of the resulting damage to an acceptable level. The mitigation strategies are required to minimize the magnitude or impacts of the residual risks. It is important that the NPS identifies appropriate mitigation strategies for the various risks identified during the study. The NPS is required to perform a cost-benefit analysis and decide on the best possible strategies based on the risks at hand. The mitigation strategy options are as explained below.

Risk Acceptance: is a strategy that is taken when the cost of other management options such as avoidance or limitation is greater than the cost of the risk itself.

Risk Avoidance: is the action that avoids any exposure to the risk. Avoidance is the choice to avoid a risk by removing the source and/or consequences. Examples are deleting some functions in the system or even removing the whole system. The NPS needed to look at obsolete systems that could no longer be updated, old operating systems and applications that are no longer supported by their developers and perform security risk analysis.

Risk Limitation: is the act of trying to minimize the impact of the risk. Limitation is the choice to mitigate the impact of vulnerability exploitation by implementing proper information security systems or tools such as antivirus or firewall or implementing proper security policies such as access control or passwords.

Risk Transference: Involves handing over the risk to a third party if it cannot be handled internally. Transference is the choice to shift risk to other assets, processes or organizations by outsourcing information security services, buying rethinking how services are offered, revising deployment models or implementing service contract with providers (Whitman & Mattord, 2008). Therefore risks that were identified but could not be managed within the public service should be transferred to trusted service providers.

5.3 How can cyber security risks be addressed to protect data and control threats in the Namibian Public Service?

From the study conducted, it could be learned that to address the current cyber security risks facing the NPS, it is important that all information assets that were identified during the study were secured. It is also important to ensure that security control measures against the identified threats and vulnerabilities were in place. The appropriate countermeasures for the risk identified should also be implemented according to cyber security best practices.

Maskun et al. (2013) stipulated that the activities and other measures to protect computers, computer networks, related hardware and software can include security audits, patch management, authentication procedures, access management, detection and reaction to security events, mitigation of impacts, and recovery of affected components. They added that other measures can include such things as hardware and software firewalls, physical security such as hardened facilities, and personnel training and responsibilities.

Therefore, it should be understood that to address cyber security risks in the NPS, the subject of cyber security needed not to be considered only as an IT problem but as an organisational concern that needed to be addressed from the top management. In this way, physical, procedural, technical and regulatory security controls would be considered concurrently.

Based on the results of the study, the researcher believes that, to protect data and control threats in the NPS, the following should be considered:

a) All information assets in all O/M/As were identified and classified in terms of security access levels.
b) Both technical and non-technical foundational cyber security control measures needed to be addressed. Julisch (2013) observed that many organizations fail to implement foundational security controls and consequently, were easy targets for opportunistic and novice attackers.
c) Ensuring security controls for addressing the identified threats and vulnerabilities were in place. These included preventative controls, detective controls and corrective controls.
d) The development of the cyber security cyber security policy framework for the NPS based on best practices and standardize them across all O/M/As was necessary. This should be in terms of policies, guidelines and procedures.
e) Ensuring that all relevant policies, from general to device and application specific were developed, implemented and executed.
f) Ensuring that all O/M/As adopt, implement and comply with the developed framework.
g) Relevant security training on general cyber security, application level, device level and action based security are made compulsory to all staff.
h) Clear roles and responsibilities for the different job categories are set and adhered to ensure clear allocation of access level privileges.

i) Performance of regular monitoring and evaluation on security controls to ensure effectiveness. Calder and Watkins (2012) advised that it is essential that security processes and procedures are completely up to date, to reflect current risks.

6. PROPOSED FRAMEWORK

This chapter presents the Cyber Security Risk Management and Threat Control (CSRM-TC) model. The model was introduced to manage cyber security risks identified during the study. This model could be adopted in the Namibian Public Service for the harmonization of cyber security risk management strategies in all O/M/As.

In the NPS, information systems continue to be interconnected and made accessible through the internet in the absence of cyber security best practices. Considering this gap the study was carried out to identify how these non-technical information security issues had impacted the effective utilization of technical security measures looking at both internal and external influences.

The model was therefore developed to enhance the effectiveness of existing security measures, by controlling both internal and external targeted or widespread threats.

The different components of the architecture were explained separately in details as shown below:

The CSRM-TC model consists of three (3) key components namely: Cyber Security Policy Framework, Cyber Security Risk Management and Cyber Security Threat Control. These components are integrated to control threats and minimize impacts of the resulting risks within the NPS.

6.1 Cyber Security Threat Control

This component is responsible for controlling both external and internal security threats through prevention, detection, correction and reporting. Information regarding various threats detected are compiled and presented under the reporting section to be fed into the Cyber Security Policy Framework. This was done to enhance the relevance and effectiveness of the policy framework through regular updates. Figure 6.1 shows the relationship between various phases within the Cyber Security Threat Control. The different components were explained in details as shown below:

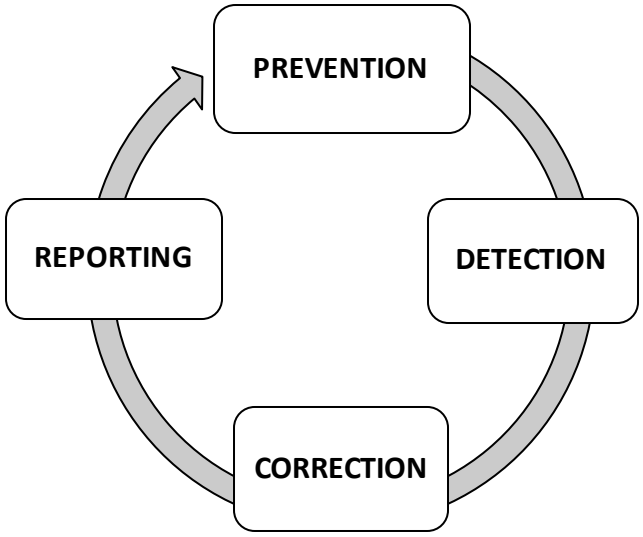


Figure 6.1 Cyber Security Threat Control

a) Prevention: this component is responsible for blocking known security threats originating from both internal and external sources. These could be at the level of network perimeter (e.g. Firewalls, Intrusion Prevention Systems (IPS)) or physical security (e.g. lockable doors and security guards) as well as at the level of device or application (e.g. Passwords)

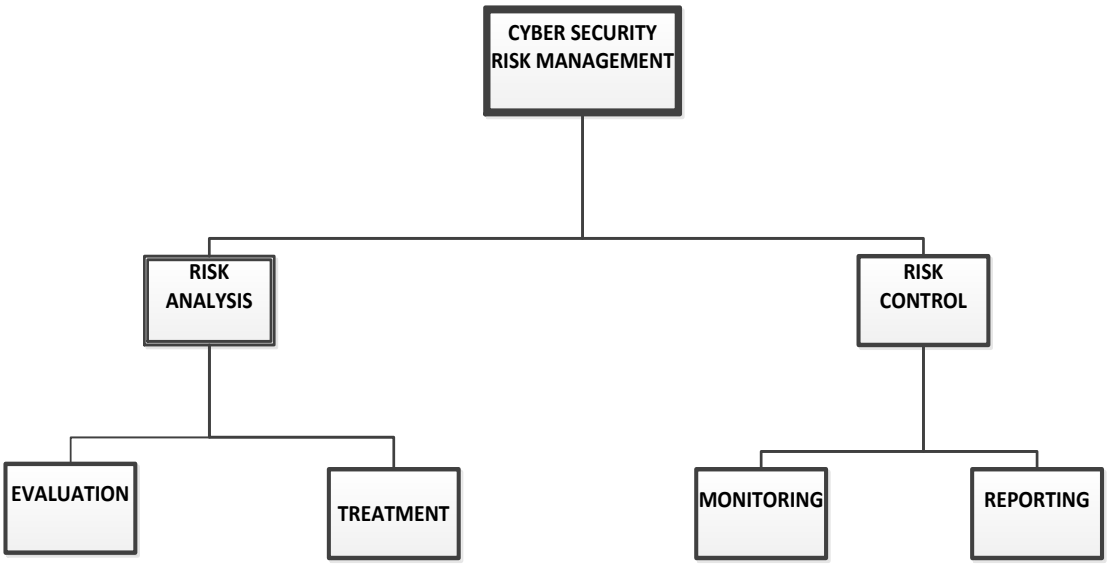
b) Detection: this component is responsible for recognizing threats that may have protruded to the protected zones. These could be alarm systems for physical access or Intrusion Detection Systems (IDS) at the network perimeter level.

c) Correction: This is the corrective action taken against the threat detected.

d) Reporting: The action taken on the various threats are documented and fed into the Cyber Security Policy Framework for review and consideration.

6.2 Cyber Security Risk Management

To enhance the availability of public information and services at all times, residual risks are taken through the management component, where they are analyzed and controlled. Processes under risk management are shown in Figure 6.2. The different components are explained in details in terms of their functionalities.



6.2 Cyber Security Risk Management

The Risk Management component consists of two major phases namely Analysis and Control. When residual risks are encountered they enter the Analysis phase, where they will be evaluated and treated.

During evaluation the probability and impact of individual risks, as well as their interdependencies are investigated. Evaluation assists with the decisions made under treatment whereby risks are treated through mitigation, elimination, prevention or reduction.

On the other hand, the Control section is responsible for monitoring risks after having been treated, and reporting on the findings. The monitoring component is responsible for inspecting whether the established controls are functioning properly or not. The reporting component presents information or actions gathered during monitoring. This information is therefore fed into the Cyber Security Policy Framework for review and policy update.

6.3 Cyber Security Policy Framework:

This components comprises of all relevant security policies, standards, guidelines and procedures developed according to cyber security best practices. Kizza (2013) stated that vulnerabilities not only exist in hardware and software that constitutes a computer system but also in policies and procedures, especially security policies and procedures that are used in a computer network system and in users and employees of the computer network system. Sanderson (2011) emphasized that when assessing risk, it is imperative to have policies and procedures that provide a good understanding of where data lives at any point in time. He defined policies as formal, high level strategic

document of intent. He further defined standards as mandatory requirements on specific hardware or software that are more detailed than policies. In addition, he defined procedures as step by step operational instructions that is tied to a specific technology or devices.

This component provides O/M/As with ways of executing cyber security policies in a standardized manner and it is updated with information from Risk Management Component, Threat Control Component, as well as the international security best practices.

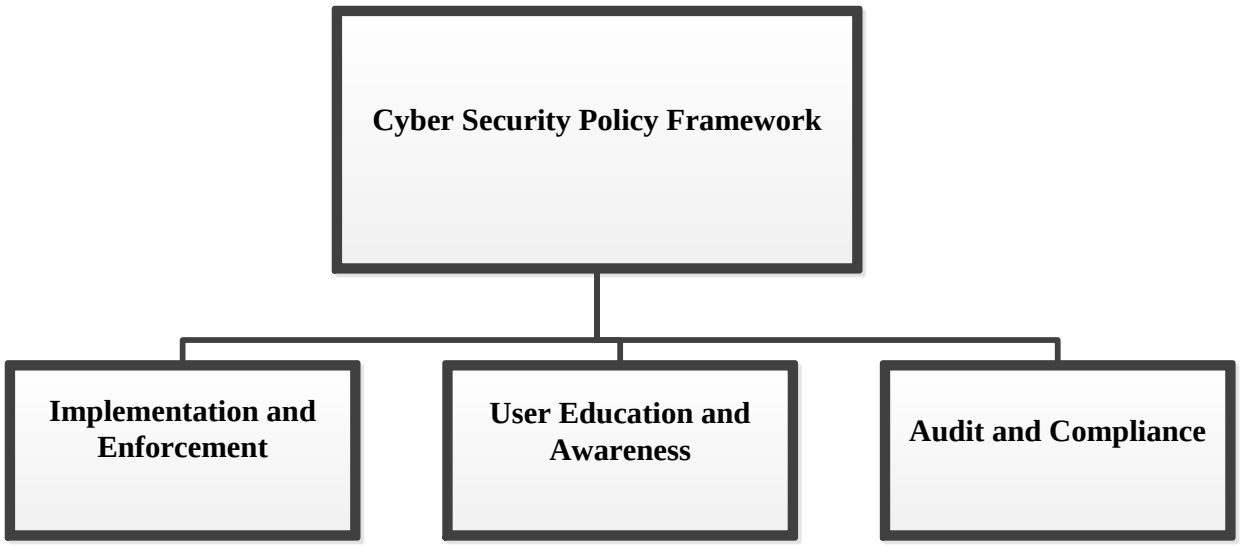


Figure 6.3 Cyber Security Policy Framework

a) Security Best Practices

The framework is based upon internationally recognized best practices including the following:

- ISO/IEC 27001 is the international standard for best practice information security management systems (ISMS) (Calder and Watkins, 2012).
- ISO/IEC 27032 is the international standard focusing explicitly on cyber security (Calder and Watkins, 2012).
- ISO/IEC 27035 is the international standard for incident management which forms the crucial first stage of cyber resilience (Calder and Watkins, 2012).
- ISO/IEC 27031 is the international standard for ICT readiness for business continuity (Calder and Watkins, 2012).
- ISO/IEC 22301 is the international standard for business continuity management systems and forms the final part of cyber resilience (Calder and Watkins, 2012).

b) Audit and Compliance

Under this component, information systems and/or O/M/As are reviewed on their adherence to regulatory guidelines stipulated in the policy documents.

c) Implementation and Enforcement

This component is responsible for ensuring that all necessary security measures are applied and executed according to the rules provided.

d) User Education and Awareness

This component caters for a compulsory staff training program whereby contents of the security policy are regularly explained to all users to maintain awareness. Sanderson (2011) advised that when an organization has defined its processes for

ensuring that sensitive data is properly protected and handled, it is important to ensure that the people responsible for carrying out its security were informed and trained.

It is also equally important that the acceptable and non-acceptable user actions are clearly explained to staff members within the NPS, as stipulated under the Cyber Security Policy Framework. Relevant technical training to all end-users on various applications as well as for IT staff is carried out under this section. This component promotes effective and optimal utilization of information systems by minimizing the chances of unintentional errors through training.

6.4 Cyber Security Risk Management and Threat Control Model

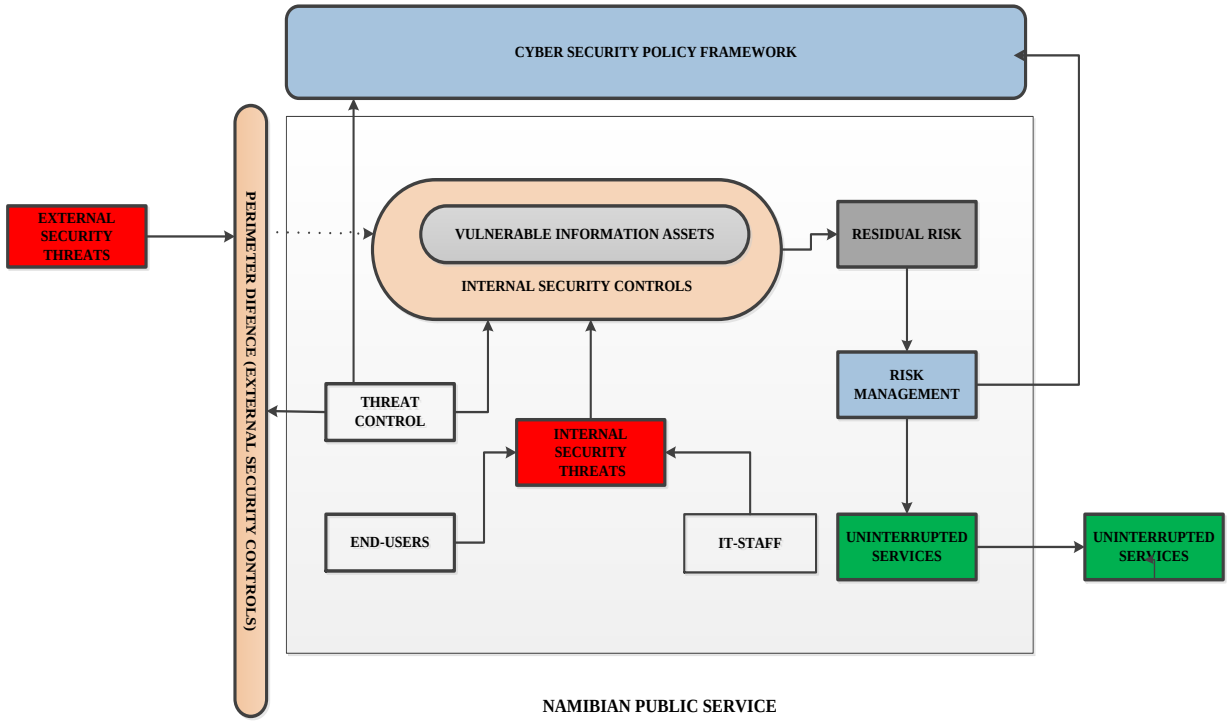


Figure 6.4 CSRM-TC Model

a) Vulnerable Information Assets:

Figure 6.4 represents information assets of all O/M/As. These include connected computing devices, personnel, applications, services, telecommunications systems, as well as data in transit, at rest or in processing within the NPS. The information assets are deemed vulnerable as a result of constant insider abuse and the unceasing evolvement of security threats from the cyber space.

b) Perimeter Defense (External Security Controls):

Refers to the security controls at the edge of the network that blocks external threats from entering the network. All possible threats originating out of the NPS are managed under this component. These include threats from internet, physical theft, threats associated with mobile and cloud solutions as well as those associated with outsourced ICT solutions.

c) Internal Security Control

This section addresses security risks that might occur as a result of insider/internal threats originating from either end-users or IT staff. All potential technical and non-technical security threats originating within the NPS are managed under this section. These include human errors, fraud, identity theft, violated confidentiality and integrity. Sarkar (2010) stated that the greatest security threat comes from the person with authorized access. Jouini (2014) also stated that implementing perimeter defenses can protect an organization from the outside but it cannot address the dangers from within. He added that insiders can pose significant risk to information security if motivated.

d) Residual Risk

When unknown threats manage to bypass the 'threat control' and strike through the available security controls to expose the vulnerabilities within the information assets, a certain risk may occur. This stubborn danger that is not prevented by the available security controls is referred to as residual risk and is treated under the management component.

e) Uninterrupted Service:

This represents a continual service provision within and outside the NPS. This means that, even if a disaster strike, the delivery of service to customers does not cease but continues uninterrupted due to the availability of security controls.

6.5 Maximising the CSRM-TC Model

This model could be maximized when the NPS embrace it as a compulsory model and adopt other relevant best practices for each component. For instance, COBT 5 as a framework for the governance and management of enterprise IT connects and aligns with other major standards and frameworks. Similarly, the CSRM-TC was designed to operate in the same way.

CSRM-TC comes with the risk management component that aims at providing awareness and training to users and IT staff members. The training and awareness on security need further guidelines to be developed and standardized based on the need at hand.

The next chapter presents the conclusions of the study as well as proposed recommendations for future studies.

7: CONCLUSIONS AND RECOMMENDATIONS

This chapter presents the conclusions and recommendations made in the study. These were based on the results of the study, literature and empirical data analysis. In this chapter the suggestions for future research were also presented.

7.1 Conclusions

The study investigated behavior of various O/M/As on managing the security of their information assets in the absence of cyber security best practices. These include security policies, standards and guidelines in the NPS. Cyber security is required to ensure that all the organizational information assets are protected against unauthorized access and all possible threats originating from the cyber space and within the NPS.

The study revealed that although there may be an abundance of security technologies in the NPS, the absence of security policies, standards and guidelines has led to a huge disparity regarding the way in which information assets are managed in various O/M/As. This therefore poses security risks to the NPS information assets especially, as systems continue to be interconnected.

The researcher further noted that in order to provide effective cyber security, it is important that all information assets that need to be protected are identified and classified.

It was very interesting to learn that all participated IT Managers were aware of cybercrime but also sad to learn that only (23.5%) have actively covered it in their strategic plans. They clarified that improved security solutions is their focus hence include them in their annual and five-year strategic budgeting and handle it as a daily responsibility.

The study concluded that the best way to achieve a substantial and enduring improvement in cyber security is not only by embracing technical solutions but also by ensuring that human management and regulatory directives are addressed. This is true because in general security systems may be upgraded and physical security can be tightened but, if employees at different levels are not informed about the correct procedures of handling such systems, those security initiatives will remain a challenge.

7.2 Recommendation

The goal is to mitigate the cyber security risks facing information assets of the NPS by addressing threats and vulnerabilities and decide on appropriate strategies to mitigate the resulting dangers.

To enable the NPS to shift from the current level to the desired stage, the following recommendations were made:

a) Staff members should be educated on the secure and unsecure online practices.
b) They should be educated on the importance of maintaining foundational security measures.

c) The NPS should also engage some ethical hackers to test the security of existing systems in advance.

d) The NPS need to review the existing IT policy and e-Government policy to maintain relevancy of the content with changing technology.

e) Development of topic specific policies including e-mail policies, password policies, and internet policies is necessary.

f) The NPS need to develop standards and guidelines through which policies can be executed, and encourage all O/M/As to comply.

g) Make cyber security training a compulsory requirement for all employees and educate them how security can benefit their daily works.

h) The NPS should ensure that the written policy is translated into actions.

i) Prioritize assets according to risk impacts to ensure effective security investment.

7.3 Recommendation for Future Research

- Penetration testing on critical web based information systems of the NPS
- The role of cyber security in e-Government: The Namibian Perspective
- The collaboration between Government, private and educational institution on addressing cyber security at national level.

The next section presents a list of reference materials cited in this study.

8. REFERENCES

Atul M. T., Suraj S. K., & Surbhi R. C., (2013). Cyber security: challenges for society-literature review. *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727, 2(12), 67-75.*

Ayofe, A. N., & Irwin, B. (2010). Cyber Security: Challenges and the Way Forward. *: Computer Science and Telecommunications 6(29) 56*

Barman, S. (2002) Writing information security policies. New York: New: Riders

Bennett, A. (2015, May 22) Workshop-held-to-tackle-cybercrime. *Economist*. Retrieved from http://www.economist.com.na

Calder A. & Watkins S. (2012), IT Governance: An international Guide to Security and ISO 27001/ISO 27002, CIP Group Croydon

Calder, A. & Watkins, S. (2012) IT Governance: An international guide to data security and ISO27001/ISO27002 (5th Ed.). Croydon. CPY Group Ltd

Ganesh, D.B., & James, H. Graham, J. H. (2009). Improving the Cyber Security of SCADA Communication Networks. Communications of the ACM, 52 (7) doi: 10.1145/1538788.1538820

Geers, K. (2009). The Cyber Threat to National Critical Infrastructures: Beyond Theory. *Information Systems Security*, *18*(1), 1-7.

Government Accountability Office. (2013). National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. (GAO Publication No. 13-187). Washington, D.C.: U.S. Government Printing Office.

Government of the Republic of Namibia. (1996). *Manual of Guidelines for Common Minimum Standards of Protective Security Measures for Government Ministries/Public Offices and Agencies of the Republic of Namibia*. Windhoek, Namibia: Office of the President.

Government of the Republic of Namibia. (2004). *Information Technology Policy for the Public Service of the Republic of Namibia. Windhoek*, Namibia. *Office of the Prime Minister*.

Government of the Republic of Namibia. (2013). *National e-Government Strategic Action Plan: e-Government Readiness Report*. Windhoek, Namibia: Author.

Herath, H. S.B & C. Herath, T.C (2014). IT security auditing: A performance evaluation decision model. *Decision Support Systems 57, 54–63*

HIPPSA First Mission Report (2013) HIPSSA Support for Harmonization of ICT Policies in Sub---Sahara Africa (HIPSSA) Transposition of SADC Model Laws On Cybersecurity for the Republic of Namibia First Mission Report 2013. Windhoek. MICT

Humphley, E. (2008). Information Security management standards: Compliance, governance and risk management. *Information Security Technical Report 13, 247 -255*

Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security 31, 83 e95*

ISACA (2014, December 8). COBIT 5 for Information Security. *COBIT documents*. Retrieved from https://www.isaca.org

ITU (2014, September 20) Cybersecurity. ITU News. Retrieved from https://www.itu.int

ITU-ABIresearch (2015). Global Cybersecurity Index & Cyberwellness Profiles Report: Telecommunication Development Bureau; Brahima Sanou.

Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences 80, 973–993*

Jirasek, V., (2012). Practical application of information security models. *Information Security Technical Report 1 7, 1e8*

Jouini, M., & Rabaia, L.B.A., & Aissa, A. B. (2014) Classification of security threats in information systems. *5th International Conference on Ambient Systems, Networks and Technologies*

Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. *Computer Networks 57, 2206-2211*

Kaze, H. (2014, August 13). ITU gives thumbs up to Nam's ICT progress. *The Villager newspaper*. Retrieved from http://www.thevillager.com.na

Kim, W., & Jeong O., & So, J. (2011).The dark side of the Internet: Attacks, costs and responses. *Information Systems 36, 675-705.*

Kizza J.M. (2013). Computer Communications and Networks: *Guide to Computer Network Security*, 465 -489, Springer.

Knapp, K.J., Morris. F., Marshall. T.E., & Byrd, T.A. *(2 0 0 9).* Information Security Policy: An Organizational-level Process Model. *Computers & Security 2 8, 4 9 3 – 5 0 8*

Kritzinger E., & Solms S.H. (2010) Cyber security for home users: A New Way of Protection Through Awareness Enforcement Computers & Security. 2 9, 8 4 0 - 8 4 7

Kritzinger, E. & Smith, E. (2008) Information security management: An information security retrieval and awareness model for industry. *Computers & Security 27, 2 2 4 – 2 3 1*

Maskun, & Manuputty, A., & Noor S.M. & Sumardi J. (2013). Cyber Security: Rule Of Use Internet Safely? *13th International Educational Technology Conference. Procedia - Social and Behavioral Sciences 103, 255 – 261*

Maskun, Manuputty, A., S.M.Noor, S.M. &, Sumardi, J., (2013). Cyber Security: Rule of Use Internet Safely? *Procedia - Social and Behavioral Sciences 103, 255 – 261*

Mattord W. & Hulme G.V. (2008), Getting at risk. In: Whitman ME, Mattord HJ, editors.

McLean, S. (2013). Beware the Botnets: Cyber Security Is a Board Level Issue *Intellectual Property & Technology Law Journal* 25, 12

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection 3, 103 – 117*

Moore, T. (2010). The Economics Of Cybersecurity: Principles And Policy Options. *International Journal of Critical Infrastructure Protection 3, 1 0 3 – 1 1 7*

Mouna, J., & Latifa, B. A. & Anis, B.A., (2014). Classification of security threats in information systems: *5th International Conference on Ambient Systems, Networks and Technologies: Procedia Computer Science 32, 489 – 496.*

Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis*, *31*(3), 497-512.

Panda, B., Giordano, J., & Kalil, D. (2006). Next-Generation: Cyber Forensics. *Communications of the ACM*, 49(2), 44-47.

Pant, H., McGee, A. R., Chandrashekhar, U., & Richman, S. H. (2006). Optimal Availability and Security for IMS-Based Voip Networks. *Bell Labs Technical Journal*, *11*(3), 211-223.

Peltier, T. R. (2002). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. New York, NY. Auerbach Publications.

Pilling, R. (2013) Global Threats, Cybersecurity Nightmares and How To Protect Against Them. *Computer Fraud & Security September 2013*

Richardson R. (2008), CSI Computer Crime and Security Survey. Computer Security Institute 1, 1–30.

Rok, B., & Borka, J. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management 28, 413–422.*

Sanderson, R. (2011) A secure data protection strategy. *Network Security 10 – 12*

Shackelford, J. S., (2012). Should your firm invest in cyber risk insurance? Journal Business Horizons

Slay J. & Koronois A. (2006), Information Technology: Security& Risk Management, John Wiley & Sons, Sydney.

Solms, R., and Niekerk, J., (2013). From information security to cyber security. *Computers & Security* (38), 97–102

Tudose M. (2012). Identifying the Risks Towards Critical Information and Communications Technology Infrastructure. *Buletin Ştiinţific 1 (33) 77*

Vladimir Jirasek, V., (2012). Practical Application of Information Security Models. *Information Security Technical Report 17, 1e8*

Webb, J. Ahmad, A. Sean B. Maynard, S. B., & Shanks, G. (2014) A situation awareness model for information security risk management. *Computers & Security 44, 1e15*

Westfall, J. E. & Kim, C. M. & Ma, A. Y. (2012). Locking the virtual filing cabinet: A researcher's guide to Internet data security. *International Journal of Information Management 32, 419– 430.*

Willison, R., & Siponen, M. (2009). Overcoming the Insider. *Communications of the ACM,* 52(9), 133-137.

Works B., (2013). Management of information security: Thomson Course Technology; 2004. pp. 307e8.

Xoagub. F. (2014, January 23). Namibia Develops Cybersecurity Law. Windhoek Observer. Accessed from http://observer24.com.na

Zernike, K. (2009, April 1). Paying in full as the ticket into colleges. *The New York Times*. Retrieved from http://www.nytimes.com

Zhao, J.J., & Zhao, S.Y., Opportunities and Threats: A Security Assessment of State E-Government Websites. *Government Information Quarterly 27 (2010) 49–56*

9. GLOSSARY

Asset or Information assets: An asset is a tangible or non-tangible items that may include people, property and information. It is what we are trying to protect against possible harm.

Availability: The property of being accessible and usable upon demand.

Information security: refers to measures taken to protect or preserve information on a network as well as the network itself

Confidentiality: A property that information is not disclosed to users, processes, or devices unless they have been authorized to access the information

Countermeasures: Preventative (proactive or reactive) actions, devices, procedures, techniques, or other measures that reduce the impact of a vulnerability or the likelihood of successful exploitation of a vulnerability.

Disaster recovery: The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions.

Intrusion: An unauthorized act of bypassing the security mechanisms of a network or information system.

Impacts: The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information (loss of confidentiality), unauthorized modification or destruction of information (loss of integrity), or disruption of access to or use of information or an information system (loss of availability).

Incident: Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in the quality of that service.

Integrity: The assurance that computerized data is an accurate and complete representation of the data as created or modified by its originator and that computerized information resources remain configured as intended by the person responsible for them.

Strategy: A method or plan chosen to bring about a desired future, such as achievement of a goal or solution to a problem.

Human threats: Possible disruptions in operations or breach of security controls resulting from intentional or unintentional human actions.

UNIVERSITY OF NAMIBIA
Computing Department
Private Bag 13301, Windhoek, Namibia

QUESTIONNAIRE

CYBER SECURITY RISK MANAGEMENT AND THREATS CONTROL (CSRM-TC): ENHANCING THE PROTECTION OF INFORMATION IN THE NAMIBIAN PUBLIC SERVICE.

Instructions: Answer all questions in the section that applies to you.
Tick where appropriate and write your responses in the spaces provided.

NB: *Information provided in this questionnaire will be treated with anonymity and confidentiality.*

SECTION A: IT MANAGER

1. Who would you consider has the overall accountability for Information Systems security management in your O/M/A?(*select **one** option*)
   ☐ IT Manager ☐ Systems Administrators ☐ All IT staff ☐ All staff members
2. Rank the following options in order of priority with regards to effective security
   (*where **1** is **1st Priority**, **2** is **2nd Priority** and **3** is **3rd Priority***):
   ☐ Advanced security equipment ☐ Qualified IT Security staff ☐ User education and training
3. What type of Internet connection is available in your O/M/A? (*including regional offices*)
   ☐ Cable/Fibre ☐ Wireless (Wi-Fi) ☐ Mobile (3G/4G)
4. What documentation is in place to ensure business continuity and disaster recovery for your O/M/A? (*select **all** that apply*)
   ☐ Business continuity plan ☐ Disaster recovery plan
   ☐ Network layout map ☐ IT operational standards and guidelines ☐ None of the above
   ☐ Other .....

5. What monitoring system does your unit have in place to control physical access to the server room at your O/M/A? Electronic access card system ☐ Biometric based access system ☐ A register book ☐ Not closely monitored ☐ Other.....
6. Who has administrative rights to Information Systems and networks resources in our O/M/A?
   ☐ Systems Administrators ☐ Computer Technicians ☐ IT Manager
   ☐ Analyst Programmers ☐ Other.....
7. Are you aware of Cybercrime? ☐ Yes ☐ No
8. If **Yes**, what does your unit have in place to address the challenges faced with Cybercrime?
   ☐ There are no actions yet ☐ Cyber risks management is covered in our strategic planning
   ☐ Our unit has implemented procedures to deal with Cybercrime ☐ Other.....
9. What are the challenges faced by your units with regards to information security?
   ☐ Lack of specialised IT staff ☐ Problem in retaining IT staff
   ☐ Lack of security equipment ☐ Insufficient budget ☐ Other.....

SECTION B: SYSTEMS ADMINISTRATOR

1. Which of these security technologies are deployed in your O/M/A network? (*select **all** that apply*)
   ☐ WSUS ☐ Firewall ☐ IPS ☐ IDS ☐ DMZ ☐ Other .....
2. Does your O/M/A perform security audits on Information Systems and networks? ☐ Yes ☐ No

3. If **Yes**, how often? Daily ☐ Weekly ☐ Monthly ☐ On request ☐ Rarely ☐
   Other .....
   .....
4. On average, how often do you update antimalware definitions for the various equipment in your O/M/A? Daily ☐ Weekly ☐ Monthly ☐ Rarely ☐
5. Are the unused ports on dedicated servers disabled? Yes ☐ No ☐
6. If **No**, specify reason .....
7. Does your O/M/A perform DNS scanning? ☐ Yes ☐ No ☐
8. If **Yes**, how often?
   ☐ Daily ☐ Weekly ☐ Monthly ☐ On request ☐ Rarely ☐
9. How long does it take user passwords to expire in your O/M/A?
   ☐ A week ☐ A month ☐ Our passwords never expire ☐ Other ☐
   .....
10. Are you performing backups at your O/M/A? Yes ☐ No ☐
11. If **Yes**, where do you keep the backup copies Onsite ☐ Offsite ☐ Both ☐

SECTION C: ANALYST PROGRAMMER

1. Have you ever attended a course related to application development security? Yes ☐ No ☐
2. If **No**, what were/are the reasons for not attending?
   ☐ No guidance ☐ Limited funds ☐ Lack of interest Other .....
   .....
3. When developing or building applications which of the following tests do you carry out before implementation? Functional testing ☐ Stress testing ☐ Fuzz testing ☐ Recovery testing ☐ Acceptance testing ☐
   Other .....

4. Which of these features would you incorporate in an application to ensure that sensitive data is protected? ☐ Authentication ☐ Authorization ☐ Session Management ☐ Auditing and logging ☐ None of the above Other.....