AFRICA UNIVERSITY

(A UNITED METHODIST-RELATED INSTITUTION)

AN ANALYSIS OF CYBERSECURITY CHALLENGES IN PUBLIC CLOUDS AND APPROPRIATE INTRUSION DETECTION MECHANISMS

BY

TATENDA IRENE TAKAWIRA

RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF BACHELORS SCIENCE HONOURS IN COMPUTER INFORMATION SYSTEMS

2025

DECLARATION

I, Tatenda Takawira hereby declare that this dissertation for Bachelor of Sciences Honors in Computer Information Systems submitted to the College of Business, Peace, Leadership and Governance at Africa University has not been submitted previously for any degree at this or another university. It is original in design and in execution, and all reference material contained therein has been duly acknowledged.

Signature ……. **Date** ……

Tatenda Takawira

Supervisor …… **Date** ……

Mrs L Fundisi

1 Table of Contents

1. CHAPTER 1: INTRODUCTION

1.1 INTRODUCTION

The aim of this chapter is to introduce the research to the reader. This research is based on the researchers observation that most of the companies are making use of cloud services hence a high risk on them facing cyberattacks. The researcher will be. Research reference will be made to effectively analyse on the cybersecurity challenges in the public clouds and appropriate intrusion detection mechanisms that can be put into use with special reference to the PPC Group. The chapter will highlight the following key features – background of the study, statement of the problem, research objectives, research questions, scope of the study, assumptions, significance of the study, delimitation's and limitations of the study.

1.2 BACKGROUND TO THE STUDY

The trust of the user on the security and privacy of their data has always been the biggest point of concern. Cloud computing has numerous advantages as it provides better productivity for example resource pooling, elasticity of services, automated computing as well as cost effectiveness but security has and always will the main obstacle to the implementation of the cloud service models. There are several security and privacy challenges as data is stored on several remote servers. Keeping the important information of the user safe from security breaches, leakage of data and the user by unauthorized persons and hackers has always been an issue.

1.3 STATEMENT OF THE PROBLEM

Cyber security ensures real-time protection of information systems and networks from intruders. It has been receiving a significant amount of attention from the past till now because the number of computing, communications and critical infrastructure attacks have been significantly increasing. Cyber security denotes the application of technologies, processes and controls to defend computers systems, servers, mobile devices, networks, data and programs from malicious attacks. Cyber security aims to cut the risks of cyberattacks and protect systems from unauthorized exploitation of networks and technologies. Most companies use the cloud services to run their businesses hence they are at high risk of

cyberattacks. Everyone has access to the cloud whether they have subscribed for infrastructure, software or platform as services hence they need to be fully protected from any kinds of cyberattacks.

Despite the widespread adoption of public cloud computing, cybersecurity remains a major concern for organizations. Public clouds introduce new security challenges that require effective intrusion detection mechanisms to prevent data breaches and other cyberattacks. However, existing intrusion detection systems may not be suitable for public clouds due to their unique characteristics, such as multi-tenancy and dynamic resource allocation. Therefore, there is a need to investigate the cybersecurity challenges in public clouds and develop appropriate intrusion detection mechanisms that can provide effective protection against cyber threats.

1.4 RESEARCH OBJECTIVES

The overall objective of this research is to analyze the challenges of cybersecurity in public clouds and appropriate intrusion detection mechanisms.

This report looks at the following thematic issues:

- To investigate how data is protected from data breaches as well as unwanted access.
- To analyze the types of cyber security threats that are impacting the organization and how they are dealt with.
- To determine the components of intrusion detection techniques that can be used in cloud computing for better protection of information and data.

1.5 RESEARCH QUESTIONS

- How do you protect your organization from data breaches and unwanted access ?
- Which types of cyber threats have implicated your organization before? How have you dealt with them to protect company information?
- What are the components of intrusion detection techniques that can be used by your organization for better data protection?

1.6 ASSUMPTIONS/HYPOTHESES

The researcher has assumptions that are as follows, assumptions that the respondents to the questionnaires are able to read and write that is they will be able to fully understand what is required of them and the answers they need to give. The other assumption was that the respondents will give accurate and genuine information relevant to the research. The researcher assumes that they are well aware of how public clouds work and how much security is needed to protect organizational as well as user information from intruders, and that the respondents will also be able to include personal experience bases on of what they have encountered and might encounter in future.

1.7 SIGNIFICANCE OF THE STUDY

Cybersecurity is the use of technology, procedures, and practices to safeguard networks, computer systems, programs, and data from cyberattacks that could harm them or allow unauthorized access to them. This study is important because it enlightens on the importance of cyber security and intrusion detection systems. Cybersecurity is important as it protects all categories of data from theft and being damaged, there is company freedom as they will be able to operate without any interruptions from intruders. The other significance of cybersecurity is that it avoids financial strains from cyberattacks that includes losing revenue, damaged reputation and ransom demands.

Intrusion detection mechanisms are equally important as the help the organization in monitoring routers, firewalls, key servers and files from unwanted outsiders. They are also important for analyzing the different types of attacks, identify the patterns of malicious controls and they help the company to maintain regulatory compliance and meet security regulations.

The research findings benefit the organizations by way of blocking out external and internal intruders from accessing company data and information, helps control how the employees make use of the cloud services.

1.8 DELIMITATIONS OF THE STUDY

The research is confined to PPC group These are the plants selected and that are to be used in this research because the areas were viable and easy to carry out the research since the researcher was attached to PPC Zimbabwe and also has access to the LAN Administrators as

well as the attachment students from the other plants who can assist with the research information. The researcher chose opted for the PPC group because studying other organizations would have been expensive in terms of data for information on the internet and travelling to the organizations to gather information hence, it would be difficult for the researcher to solicit information needed for the research from other organizations.

In this study the researcher is soliciting the perceptions of LAN Administrators on the challenges faced in implementing strong cybersecurity and the possible intrusion detection mechanisms that can be put in place. The chosen respondents for the interviews were LAN Administrators, Technicians and IT interns. For the plants that are not in Zimbabwe the interviews are to be done via Microsoft Teams meetings as well as google forms for the questionnaires.

1.9 LIMITATIONS OF THE STUDY

- The research is limited to some information as the respondents may not be able to give out certain information for some reasons beyond their control, for example the fear of victimization and the fact that the information may be very strategic to the success of the company's IT department. However, to counter this limitation and be able to gather some information, the researcher let the respondents know that it was only for the purpose of a school research.
- The other limitation that the researcher may encounter is that of the respondents giving cosmetic results in the bid to protect cooperate image.
- The senior managers may be occupied and fail to get time to attend to the research questionnaires and this will pose as a limitation to the research.
- Among the data collection methods that are to be used by the researcher, respondents may not want to be responsible for the written information given out hence most of them may opt for the face-to-face interviews without being recorded.
- Lack of financial resources that is, travelling expenses to and from the other plants where research is to be carried out, internet and data expenses

2. CHAPTER 2: REVIEW OF RELATED LITERATURE

2.1 INTRODUCTION

This chapter will review the theoretical framework that is put forward as a review of existing theories that will be a roadmap for developing the arguments the researcher will use to come up with a unique study of their own. This chapter will also focus on the relevance of the theoretical framework to the analysis of cybersecurity challenges to public clouds and appropriate intrusion detection mechanisms.

Cybersecurity has been defined by various authors differently. Cybersecurity can be defined as the practice of protecting systems, networks as well as programs from cyberattacks which will be aimed at interrupting normal business processes, accessing, changing as well as destroying, sensitive user information, extorting money from users via use of ransomware a malicious software that encrypts the user's data then the attacker demands for a ransom from the account owner. Hence, after the ransom is paid the hacker will then decrypt and restore access to the account owner. Study has it that implementing effective cybersecurity measures is practically challenging because there are now more devices than people and hackers are becoming more innovative as technology is advancing.

2.2 THEORATICAL FRAMEWORK

The entire inquiry of the research depends on the theoretical framework as it is the blueprint of the study. It is a guide on what to build for the study and how to support your findings, and it also provides the structure of how you will philosophically, methodologically and analytically approach structure the research. According to Eisenhart, a theoretical framework is a structure that guides research by relying on a formal theory constructed by making use of an established, coherent explanation of certain phenomena and relationships (1991, p.205). Hence, the theoretical framework consists of selected studies that support the researchers way of thinking as well as how they understand and plan to carry out their research including the concepts and definitions available and relevant to the research topic. Krainovich-Miller (2010) identifies a theoretical framework as similar to a map that guides a traveller towards a certain destination. The absence of the theoretical framework in a research restricts the research of direction to come up with an appropriate literature and scholarly discussions that arise from research findings, Imenda (2014). According to the background of study stated above, the

trust of the user on the security and privacy of their data has always been the biggest point of concern. Cloud computing has numerous advantages as it provides better productivity for example resource pooling, elasticity of services, automated computing as well as cost effectiveness but security has and always will the main obstacle to the implementation of the cloud service models. There are several security and privacy challenges as data is stored on several remote servers. Keeping the important information of the user safe from security breaches, leakage of data and the user by unauthorized persons and hackers has always been an issue.

Cloud computing offers the providing storage and computation as a service and the services it offers are as follows : software as a service, platform as a service and infrastructure as a service as these are the main services offered by the cloud. According to (Miranda Mowbray, Siani Pearson. 2009) client based privacy management helps to reduce the risk of data breaches as well as loss of privacy. The other existing preventative measure is that of mirage image management, this is a system that caters for the issues related to security management of the virtual machine images that are connected to any application of the cloud.

The researcher will be guided by the National Institute of Standards and Technology (NIST, 2018) Cybersecurity Framework. With the goal of lowering cyber risk and enhancing the security of vital infrastructure, the NIST Cybersecurity framework was developed. It is based on norms set by organizations like the International Electrotechnical Commission, the International Organization for Standardization, and Control Objectives for Information and Related Technologies (COBIT) (IEC). It aims to give businesses a standard method of describing their ideal cybersecurity state as well as their present cybersecurity state or posture, pinpoint and rank improvement opportunities within the framework of an ongoing repeatable process, evaluate progress toward the required level of cybersecurity and to communicate cybersecurity risk to stakeholders internally or externally.
The framework is made up of the framework core, implementation tiers, and framework profile as its three primary parts. According to the National Institute of Standards and Technology (2018), this framework's component for cybersecurity risk consists of five subcomponents that is: identify, protect, detect, respond, and recover. Although smaller businesses and localities can use the cybersecurity framework, it is crucial to remember that it was primarily created for vital infrastructure. Alcaraz and Zeadally (2015) define critical infrastructure as a collection of assets and systems, both physical and virtual, that are so

crucial to a nation that any disruption in their operations could have a negative impact on the economy, national security, public health or safety, or any combination of these. Power grids, healthcare systems, and public transit systems are all examples of critical infrastructure.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is highly relevant to analysing the cybersecurity challenges in public clouds. The Framework consists of standards, guidelines, and best practices that organizations can use to manage cybersecurity risk. Public cloud environments are highly complex and dynamic, and the Framework provides a structured approach to identify, assess, and manage the risks .

The Framework's core functions - Identify, Protect, Detect, Respond, and Recover - are particularly relevant to public cloud security. For example, the identify function helps organizations understand the assets and data they are storing in the cloud and their associated cybersecurity risks. The protect function provides guidance on how to implement appropriate security controls to protect these assets and data from cyber threats therefore, determining the appropriate intrusion detection mechanisms to be adopted by organizations. The detect function helps organizations monitor and detect potential cyber threats in real-time, while the respond function provides guidance on how to respond to these threats effectively. Finally, the recover function helps organizations restore their systems and data in the event of a cyber incident.

NIST is also updating its Cybersecurity Framework to address emerging cybersecurity challenges, including those specific to public clouds and this will help the researcher to come up with a detailed research that covers and analyses all the critical areas that bring out a well detailed study. The new Foundational PNT Profile and Cybersecurity Framework 2.0 Concept Paper aim to provide updated guidance on how organizations can manage cybersecurity risk in these environments.

Overall, the NIST Cybersecurity Framework provides a valuable resource for organizations looking to manage cybersecurity risks in public clouds. The researcher will use the National Institute of Standards and Technology (NIST) Cybersecurity Framework because it provides a structured approach to identifying and managing risks, and its core functions are highly relevant to the unique challenges of public cloud security and the determination of appropriate intrusion detection mechanisms.

2.2.1 Definition of key terms

Cybersecurity Cybersecurity refers to the practice of protecting internet-connected systems like computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It involves various measures such as application security, information security, network security, disaster recovery, business continuity planning, cloud security, physical security, and end-user education to prevent unauthorized access, data breaches, and other cyber threats.

Public cloud refers to a type of cloud computing in which a third-party provider makes IT resources and services, such as virtual machines, applications, storage, and platform-as-a-service or software-as-a-service elements, available to remote users worldwide. These resources and services are accessed over a network connection, either over the public internet or a dedicated network.

Cloud computing is the delivery of computing services over the internet, including servers, storage, databases, networking, and software. It enables users to store files and applications on remote servers and gain access to them via the internet, freeing users from the need to be physically present in a specific location. Cloud computing can be deployed in three ways - on public, private, or hybrid.

Intrusion detection mechanisms are tools, techniques, or processes used to detect and respond to unauthorized access or malicious activity in a network or system. These mechanisms analyse network traffic or system logs to identify potential threats and alert system administrators of any suspicious activity.

3. CHAPTER 3: METHODOLOGY

3.1 INTRODUCTION

This chapter gives an insight on the research methodology used in thus research. It focuses on the process of data gathering and how the research is carried out. The chapter examines the techniques and methods used to collect data, give an overview of the research population and research instruments in order to address research questions outlined in preceding chapters.

3.2 RESEARCH DESIGN

This research study is based on qualitative study which is used to understand concepts and experiences. It will aid and enable the researcher to gather in-depth insights on the topic under study and allow it to be well understood. Qualitative research is meant for exploring and understanding the meaning of individuals or groups to a social or certain human problem. This process of research includes questions and procedures, data collected from the respondents, data analysis and the meaning of the data interpreted by the researcher (Creswell, 2007). The advantages of using qualitative research is that it allows respondents to be themselves and give accurate responses, it the same way it benefits the researchers as they will be able to investigate their methodologies with greater accuracy. Qualitative research is a content generator as it allows for ideas to be collected from social-economic demographics and the ideas are turned into data. Using the qualitative research approach will bring out a highly detailed description of the cybersecurity challenges faced from using public clouds and the best intrusion detection mechanisms that can be used to avoid cyberattacks. The researcher will be able to collect and analyse data using the research method. Face-to-face interview, online interviews as well as questionnaires. Respondents will be interviewed and audio recorded to capture data for data analysis.

3.3 POPULATION AND SAMPLING PROCEDURES

POPULATION OF THE STUDY

The population targeted by the researcher as mentioned earlier is LAN Administrators and the attachment students from all the PPC group plants. The respondents identities will not be disclosed.

3.4 SAMPLING PROCEDURES

Stratified random sampling will be used to divide the population in two that is, the LAN Administrators and the students. An individual sample will be extracted from each group and this will help the researcher conclude the characteristics, views and behaviors of the population. The researcher selected this sampling method because it provides precise estimates of the population under study.

3.5 DATA COLLECTION

Data collection is defined as the process that involves gathering and measuring information from variables of interest by the researcher with the aim to address a research problem, according to Henderson (2005). This research will collect data by making use of interviews and using available information as the data collection techniques. The data tools will be interview guides. The advantage of using this techniques is that with already available information there are lower costs as the data is already available and it permits the examination of trends from the past. The other advantage is that it will be possible to interview both the literate and illiterate and get a more clearer response from the respondents. However there may be constraints that is, data may not be easily accessible to come up with a full research and ethical issues concerning confidentiality may rise. This research will make use of the two to come up with an effective analysis of the cybersecurity challenges as well as the appropriate intrusion detection mechanisms.

3.6 DATA MANAGEMENT

Research data management describes how the researcher stores, preserves and shares data collected and how the data will be used in the research project. Data collected during the research will be stored in an external hard drive and on google forms for the interview questionnaire , these will be kept in a place where they will be safe and where there will not

be any risk of data breaches or the confidential data from leaking and being accessed by the wrong people. It will also help prevent errors and increase the research quality.

3.7 DATA ANALYSIS

Data analysis is deemed the most critical part of a research as it summarizes the data collected and it involves the interpretation of the gatherings through the use of analytical and logical reasoning to determine the patterns, relationships or trends. The researcher will analyse their collected data by following a few steps on the data analysis checklist that is cleaning the data to make sure that there are no errors, making sure that the next person who will read the findings will understand them.

3.8 ETHICAL CONSIDERATIONS

According to Kovacs, 1985; Blumberg et al, 2005 ethics is a branch of philosophy that deals with the conduct of people and guides the norms or standards of behaviour of people and relationships with each other. In a research ethical considerations are a set of principles that guide the research design and practices. The goal of this research is to study the challenges of cybersecurity and investigate the appropriate intrusion detection mechanisms and improving the impact of cyberattacks on the public cloud. The ethical considerations work to protect the rights of the research participants, enhance research validity and maintain scientific integrity. The researcher has to follow these throughout the research:

Participants need to know the purpose of the research and why it is being carried so as to avoid them answering and providing bias information. The researcher is required to draft a consent form for the respondent to sign before they are taken through the interview.

Confidentiality is the other main ethical consideration. Due to the theory under study the respondents identities will not be disclosed so as to protect them and the researcher together with the respondent will sign a non-disclosure form which will state that the information was collected for educational purposes only and it will not be disclose for any other reason.
The research finding will be free from any form of plagiarism that is, submitting others work as your own. The research will be honest, reliable and credible. There will not be any form of self-plagiarism and the researcher will provide a unique research study which will be used by the organization to over-come any cybersecurity challenges.

4. CHAPTER 4 : DATA ANALYSIS

4.0 INTRODUCTION

The previous chapter gave an insight on the research methodology to be used by the researcher. The data presentation, analysis and implementation chapter focuses on presenting the findings of the study in order to come up with a detailed conclusion. The results being used in the research were obtained from questionnaires sent to PPC LAN Administrators and Interns, where the researcher sought to get a deep understanding of the cybersecurity challenges of public clouds and the appropriate intrusion detection mechanisms.

4.1 DATA PRESENTATION AND ANALYSIS

4.2 RESEARCH FINDINGS

Statistical information from the research is going to be presented using charts and the information gathered from the questionnaire sent to the respondents is going to be written beneath the charts representation. A total of 8 people filled in the questionnaire.

4.2.1 RESPONSE RATE

	Number of targeted	**Number of actual**	
PPC LAN ADMINISTRATORS	4	4	100%
PPC INTERNS	4	4	100%
TOTAL	8	8	

The table above shows that a total of 8 respondents received the research questionnaire and of the 8 all of them managed to send back their responses giving back a 100% response rate.

The response obtained was very high and impressive as it enabled the researcher to acquire the necessary data which was needed for the study. Hence, the findings. Of the study are based on the 8 respondents who participated and returned the questionnaires for analysis. The research design is most affected by the methods of data collection and the interaction of the respondents and the data collection tools adopted in the research determines the response rate. The response rate shows that this topic under analysis was very relevant to the respondents and the findings of the study will help improve the cybersecurity challenges being faced by public clouds as well and identifying the appropriate intrusion detection mechanisms. Participants were drawn from PPC Zimbabwe factories so as to enrich collection process with different views and opinions from different people and the participants were mainly the LAN Administrators and the Interns.

4.2.1.1 What is your level of education?

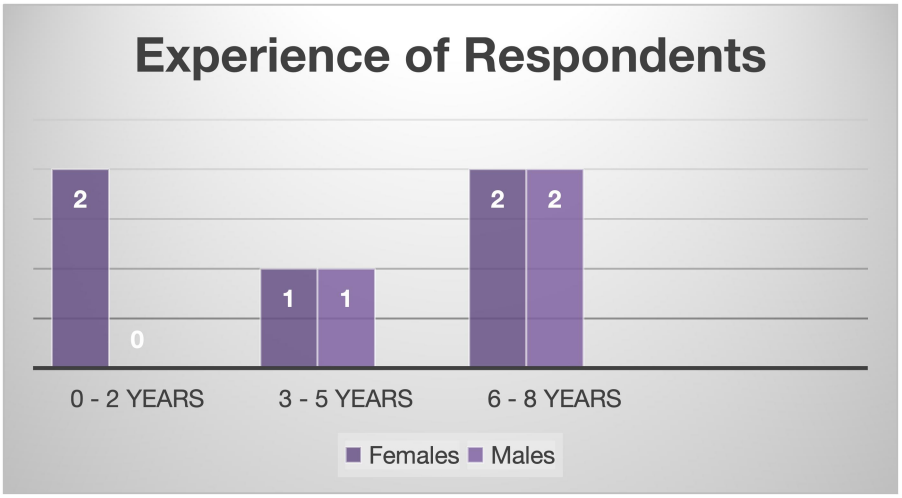
The study was interested in examining the level of education of respondents in order to determine the quality of responses by the respondents.

		Frequency	**Percent %**	**Valid percent %**	**Cumulative percent %**
VALID	A' level	2	25%	25%	25 %
	Undergraduate	2	25%	25%	50%
	Masters	4	50%	50%	100%
	Total	8	100%	100%	

The table above shows that the majority of respondents were educated, with the highest having a master's degree in the related field. This educational analysis is very important in this study as it determines the comparative knowledge network administrators and well as the interns have in the use of public clouds and the know how in controlling as well as identifying a cyber-attack when it arises. Hence, in this study most of the respondents were educated, thus guaranteeing quality responses for quality results.

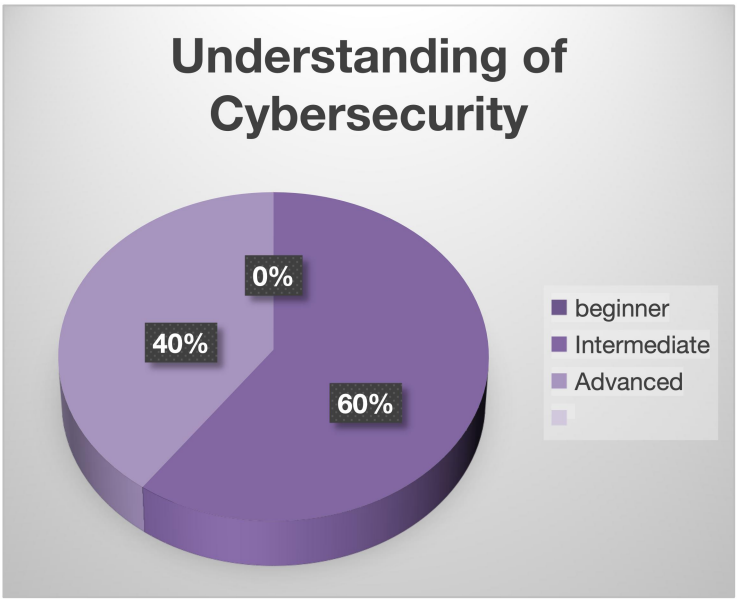
4.2.1.2 What is your work experience?

The research sought to find the amount of experience that each respondent carries so as to develop relatively accurate data on the cybersecurity challenges faced by public clouds and appropriate intrusion detection mechanisms.



For the research to be more accurate, the network administrator need to have more years of experience in that field which gives more certainty for them to be able to deal with problems and situations that may lead to or that come with facing cyberattacks. The analysis on experience is important as it provides more quality responses for this study as the participants will be responding from experience and not just using the theoretical approach.

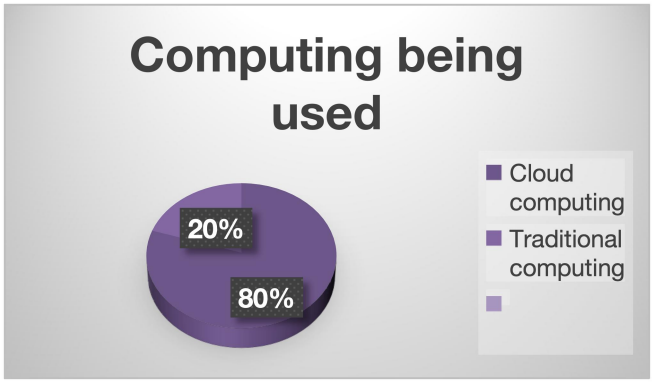
4.3.1 Question 1: How well do you understand cybersecurity?



The researcher sought to find how well the participants understand cybersecurity so as to come up with an accurate as well as positive research. The objective of this question was to analyze the participants understanding of cybersecurity. Hence, 40% of the respondents highlighted that they have an advanced understanding of the area under investigation and 60% of them highlighted that they have an intermediate understanding of cybersecurity. Refer to the chart for the number of responses on this particular question.

4.3.2 Question 2: Which type of computing is your organization using?

The other objective of the researcher was to identify the type of computing that is being currently used by the respondents so as to find out if they will be able to assist her in her research which was to analyze the cybersecurity challenges that are being faced by public clouds and the appropriate intrusion detection mechanisms to put in place so as to curb these challenges.

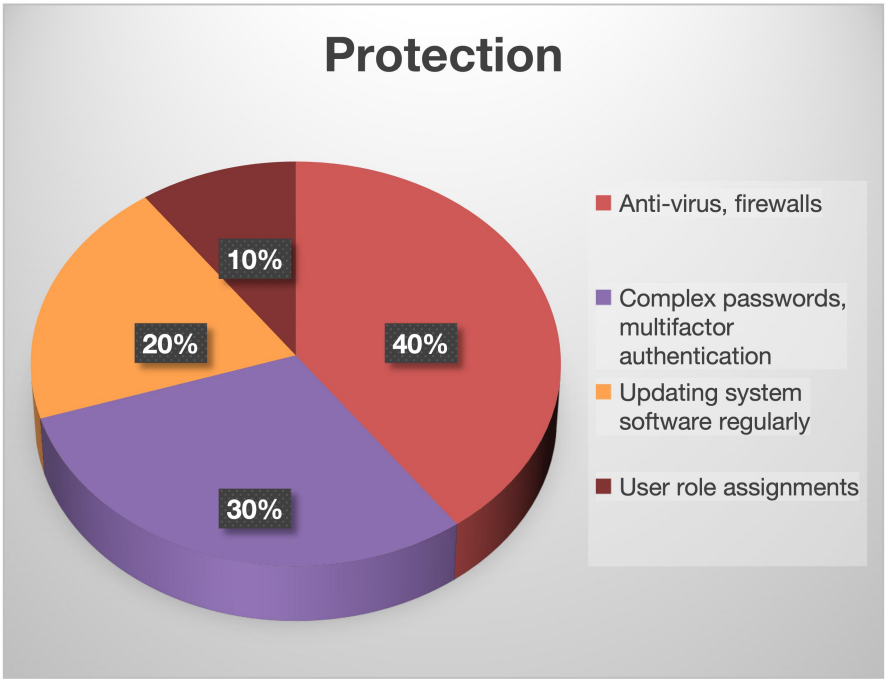


From the interview the researcher found out that most of the respondents are using cloud computing (80%) and the remaining are using traditional computing, refer to the above chart. Traditional computing is the use of physical data centers for storing digital assets and running complete networking system for daily operations (geeksforgeeks Nov 2021). This type of computing only gives users access to the data only on system in which data is stored. Cloud computing is the collective combination of configurable systems resources and advanced services that can be delivered quickly using the internet (geeksforgeeks Nov 2021). Cloud computing makes organizations perform more efficiently, become more secure and it provides flexibility.

4.4 Investigate how organizations protect data from breaches and unwanted access

This section sought to explore into the techniques that are currently being used by the organization to protect data from data breaches and unwanted access. This section also comprises of the question asked by the researcher to the participants in order to seek clarification on the investigating how organizations protect data from data breach's objective. The major techniques were stated by the participants and the responses are presented in the form of a pie chart.

4.4.1 Question 4: How do you protect your organization from data breaches and unwanted access?



In implementing a more advanced way of data protection from breaches and unwanted access, the researcher investigated on how the PPC organization has been protecting its own data from data breaches and unwanted access using various methods mentioned. The participants stated that the protection methods that they have been making use of which have been very effective and relevant for them. 40% of the respondents stated that they have been making use of anti-viruses, 30% are making use of complex passwords (with a minimum of 13 characters), for increased security the other 20% update the system software regularly that is weekly, user role assignments are used by the remaining 20%.

According to the research findings, the objective of investigating how data is protected from data breaches and unwanted access the was met because the researcher managed to gather information from the respondents as they stated that they make use of anti-viruses, complex passwords (with a minimum of 13 characters), updating the system software's every week, making use of user role assignments, multifactor authentication and firewalls.

The use of anti-viruses poses a positive effect on the organizations software's as they protect you against malicious threats by scanning the computer for viruses and other malicious software's which hide in files. Respondents also highlighted that they use complex passwords as way of data protection from hackers. Complex passwords are important because they prevent the hackers from guessing the obvious ones and gaining access to organization and personal user information.

The other way of protection data that was highlighted was the use of multifactor authentication. This is a multi-step process of logging into an account which requires the user to enter more information than just entering the password (amazon web services 2023). This can be done by entering a code from your email or sent to your phone via SMS. Multifactor authentication stops attackers from gaining access as they will not have the emails and the phone numbers of the users. They are also beneficial because they reduce security risk, enables digital initiatives and improves security response. According to Microsoft, user role assignment refers to a collection of one or more end-ser roles that enable users to manage their mailbox settings and distribution groups in Exchange Online. The use of user role assignments is important because they simplify the administration and management of privileges by allowing the administrator to group user authorities and their privileges into

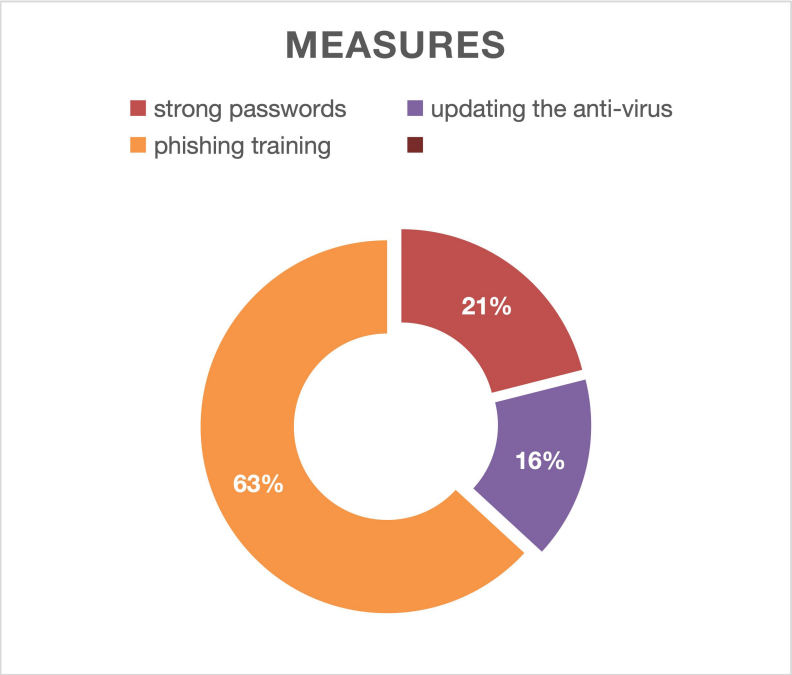
single roles as well as granting the users that need the authorities to perform their jobs. This helps to prevent unwanted users from gaining access to user information.

The use of anti-viruses poses a positive effect on the organizations software's as they protect you against malicious threats by scanning the computer for viruses and other malicious software's which hide in files. Respondents also highlighted that they use complex passwords as way of data protection from hackers. Complex passwords are important because they prevent the hackers from guessing the obvious ones and gaining access to organization and personal user information. The other way of protection data that was highlighted was the use of multifactor authentication. This is a multi-step process of logging into an account which requires the user to enter more information than just entering the password (amazon web services 2023). This can be done by entering a code from your email or sent to your phone via SMS.

Multifactor authentication stops attackers from gaining access as they will not have the emails and the phone numbers of the users. They are also beneficial because they reduce security risk, enables digital initiatives and improves security response. According to Microsoft, user role assignment refers to a collection of one or more end-ser roles that enable users to manage their mailbox settings and distribution groups in Exchange Online. The use of user role assignments is important because they simplify the administration and management of privileges by allowing the administrator to group user authorities and their privileges into single roles as well as granting the users that need the authorities to perform their jobs. This helps to prevent unwanted users from gaining access to user information.

4.4.2 QUESTION 5: What measures have been put in place to raise awareness for cyberattacks like spoofing and phishing?

Data gathered from the response from the question also highlight how data is protected from breaches and unwanted access by outside users. The measures are shown in the pie chart below.



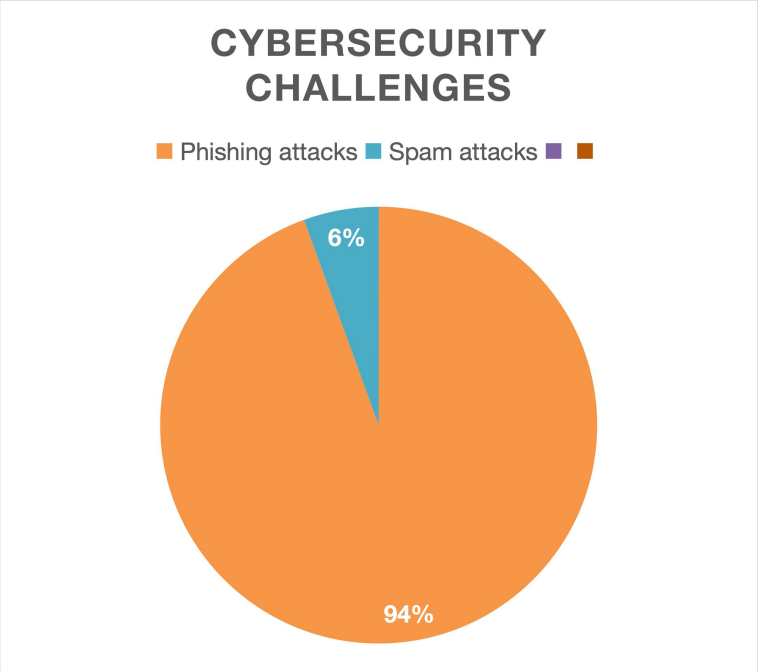
As part of the study investigation, the researcher asked for the measures that the organization have put in place to raise awareness for cyber security attacks like spoofing and phishing. A large number of the respondents stated that they conduct regular phishing training for the employees for them to be aware and more alert of the emails that may come as phishing or the sites that they may be redirected to that may cause phishing attacks for them. The rest of the respondents stated that they raise cyberattack awareness amongst the users is by updating the antivirus regularly and making use of strong passwords for the current and all new users so that they do not fall into the attacker's trap.

4.5 Types of cybersecurity threats that are implicating the organization and how they are dealt with.

This section sought to explore into the types of cybersecurity threats that are implicating the organization and how they are dealt with as a research objective. This section also comprises of the question asked by the researcher to the participants in order to seek clarification on the research objective. The major types were stated by the participants and the responses are presented in the pie chart below.

4.5.1 QUESTION 6: What are the challenges being faced by your organization in terms of cybersecurity?

The data presented below shows the data gathered by the researcher that responds and illustrates how the research objective of analyzing the types of cybersecurity threats that are implicating the organization and how they are dealt with were met.



94% of the respondents sited that they have been facing a phishing attack in terms of cybersecurity. Phishing refers to a form of social engineering where attackers deceive people into revealing sensitive information or installing malware such as ransomware (Jansson 2011). The rest of the respondents that is 6%, stated that they are facing spam attacks. Spam attacks refer to the electronic mail that ae sent to the mailbox and these contain malicious attempts to gain access to a user's computer.

According to the research findings, the objective analyzing the types of cybersecurity threats that are implicating the organization and how they are dealt with as a research objective the was met because the researcher managed to gather information from the respondents as they stated that they have faced a number of phishing attacks as well and spam attacks. These finding will also help the researcher come up with possible solutions to help curb these attacks.

The side effects of phishing are that it will install malicious software on to the user's machine and when the machine has been infected this gives the scammers access to user files and they can also track the user's behavior and patterns. When the files have been accessed the cyber criminals can then get access to the critical data and tamper with it. Spam attacks also have negative side effects to the user machine by way of communicating through sending bulk emails and messages on websites. Spam attacks spread malwares and they trick you into letting out personal information like credit card details as well as passwords, they also scare the user into thinking that they will have to pay a certain amount of money in order for them to escape the situation that they maybe in.

The researcher went further to ask if the respondents have faced any other challenges and how they have delt with them. Social engineering is one of the challenges being faced. This is the technique that is aimed at taking target into revealing any specific information and acting on illegal actions. An example of social engineering is the use of "forgot password" function that is found on various websites, this may lead the user to a password-recovery systems that may not be properly secure which will give an attacker full access to a user's account and the original user of the account loses access to their account. The respondents stated that they encourage their users to check the source, for example if it is an email, they should check the header to make sure that it matches with the other emails form that same sender.

Adware is the other challenge being faced. This is a type of software in which an advertising banner displays or downloads while a different program is running. Indications that a user's device has been infected with malicious adware include that there will be advertisements that appear in unusual places, new unwanted applications that appear on the user's home screen, the user's web searches get redirected to advertising websites and the device begins to run slowly. According to the respondents they deal with adware by way of manually removing them from user's machines after they would have identified the adware.

4.5.2 QUESTION 7: What are the possible interventions that can be implemented by your organization to protect their data, networks and systems from malicious attacks?

This section gives further information on the objective of the type of cybersecurity threats that are being faced by the organizations. This section will give the possible interventions that the organization can put into place to protect their sensitive information from intruders.

Some of the participants make suggested that the possible interventions that can be implemented by the organization in order to protect their data is by use of firewalls that is the 31%. Firewalls are an important tool for the organizations as the can act on previously set policies to better protect your network and can carry out quick assessments to detect invasive or suspicious activity, such as malware, and shut it down. The other percentage stated that the other possible interventions are to make use of cloud tools to mitigate against phishing training, continuous phishing training and ensuring that the anti-virus is running because users are the weakest links for the hackers when it comes to breaching any organizations cybersecurity.

The use of updated firewalls is also a possible way of protecting data, networks and systems from malicious attacks. A firewall is a network security device used to monitor and filter incoming as well as outgoing network traffic based on the previously established security

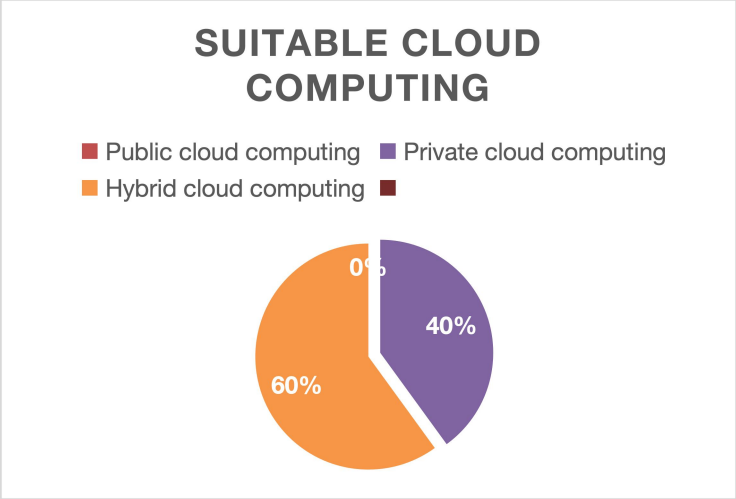
policies of the organization. Firewalls are an important tool for the organizations as the can act on previously set policies to better protect your network and can carry out quick assessments to detect invasive or suspicious activity, such as malware, and shut it down.

Ensuring that the antivirus is always running and that it is up-to-date is an important an great way of making sure that information is protected because anti viruses scan the whole machine and cleans it of any malicious attacks as well as nay viruses that will have attacked the machine under threat.

Using email filtering and management tools, regular phishing training and using cloud intervention tools to mitigate against phishing are some of the possible interventions that can be implemented by the organization to protect their data from malicious attacks that the respondents stated during the interview.

4.5.3 QUESTION 8: Which solution is the most suitable for your organization in terms of cloud computing?

Analyzing the best suitable solution in terms of cloud computing was the other objective of the research. The researcher gave the participants 3 options to choose from that is, public cloud, private cloud and hybrid cloud. From the options 60% of the respondents chose hybrid cloud computing and 40% chose private cloud computing.

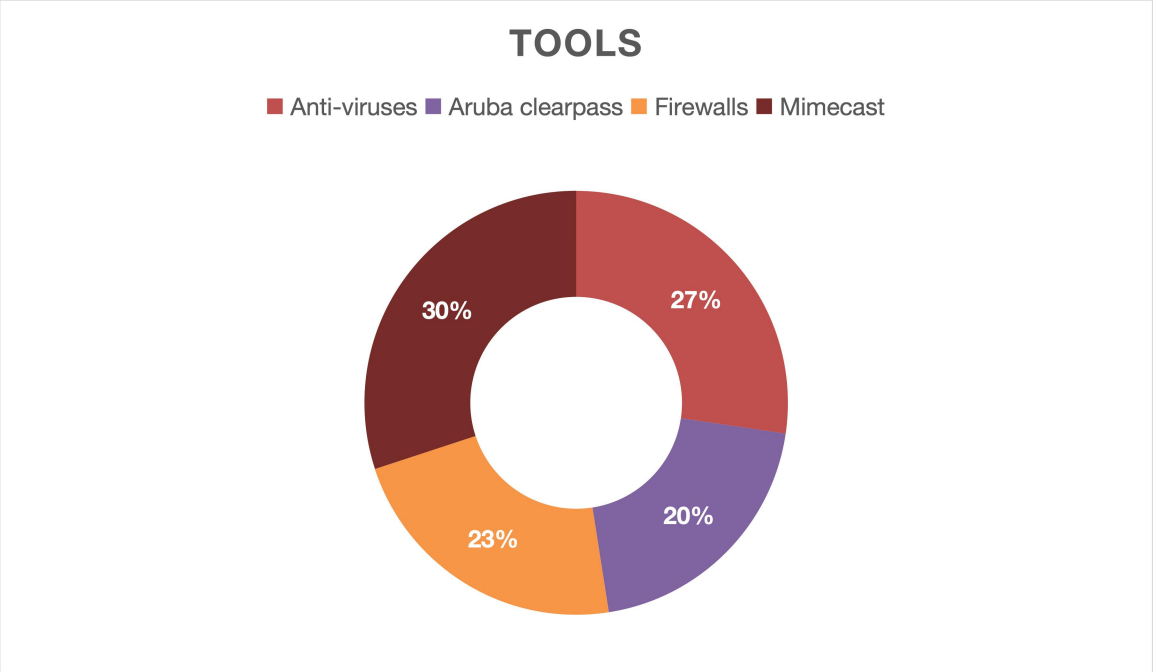


The fig above shows the responses given by the participants, they also went further to explain why they chose those specific types of cloud computing. The 60% of the participants chose Hybrid cloud computing because they can help grow the business and move into the cloud while you connect the internal systems. For instance, you can use on-premises infrastructure for sensitive or critical work while a cloud provider hosts less critical network resources. They also stated that hybrid cloud computing enables the company to utilize the cost-effective public cloud services whilst also benefiting from the security of private cloud environments, ensuring customized solutions for sensitive data. The 40% stated that they prefer private cloud computing because it avoids non organizational participants from getting in contact with the organizational data and also because it is manageable.

4.6 The components of intrusion detection techniques that can be used by your organization for better data protection

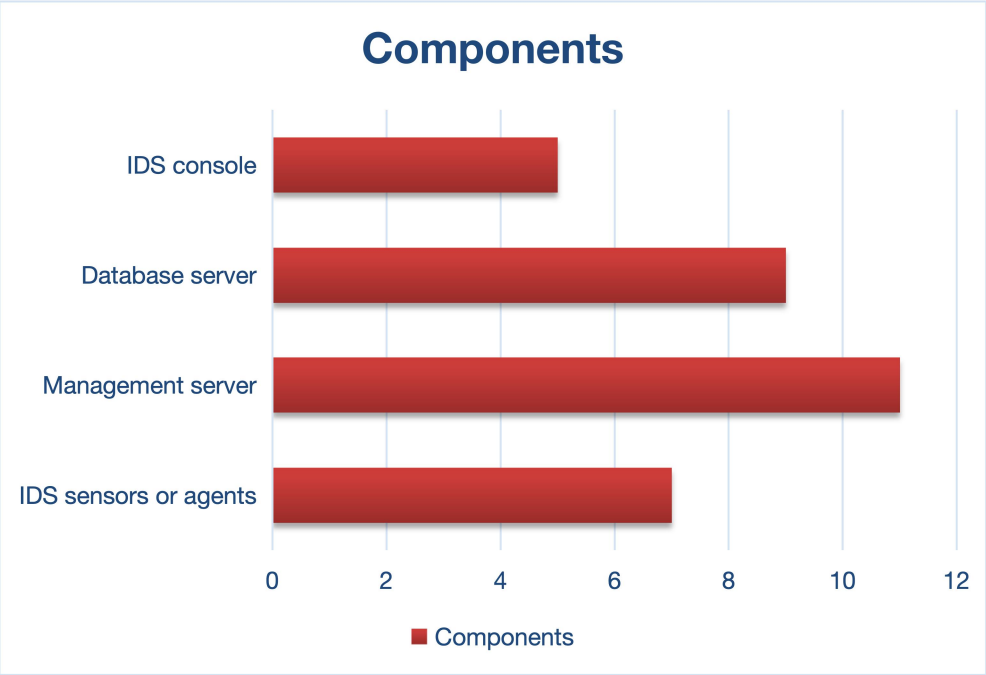
This section sought to show how the objective of determining the components of intrusion detection mechanisms that can be used by the organizations for better protection was met. This section also comprises of the question asked by the researcher to the participants in order to seek clarification on the research objective. The components were stated by the participants and the responses are presented in the pie chart below.

4.6.1 QUESTION 9: What tools have been out in place by your organization for intrusion detection?



27% of the respondents stated that they have put firewalls into place for intrusion detection. Some stated that they make use of Aruba Clear-pass, this is an access management system which provides a window into network and covers all access security requirements from a single platform. It has granular role-based policies for authentication, authorization and continuous monitoring as well as enforcement (HPE 2023). 30% of the participants have put Mimecast into place for more protection because it provides the organization with security, continuity and it helps achieve cloud services in a mail management system that is designed to protect emails as well as ensuring and simplifying the tasks and managing emails so as to curb assess of any unknown senders.

4.6.2 QUESTION 10: What are the components of intrusion detection techniques that can be used by your organization for better data protection?



Intrusion detection mechanisms help detect attacks by capturing and analyzing network packets by way of listening on a network segment or switch (NIST). Participants gave a number of intrusion detection mechanisms that can be adopted by their organizations to improve and increase data protection and these include intrusion detection console, sensors or agents, management servers and database servers.

The researcher gathered that IDS console, database servers, management servers and IDS sensors are the components of intrusion detection mechanisms that can be used to ensure more security.

4.7 SUMMARY

The chapter presented the research findings and interpretation and analysis of data for the topic understudy. The presentation of data was done in form of pie chart descriptions and bar graphs to analyse the challenges faced by public clouds and appropriate intrusion detection mechanisms. The researcher also made an objective analysis of the data which was gathered in relation to the views of scholars articulated in the second chapter. The National Institute of Standards and Technology (NIST) Cybersecurity Framework is highly relevant to analyzing the cybersecurity challenges in public clouds. The Framework consists of standards, guidelines, and best practices that organizations can use to manage cybersecurity risk. Public cloud environments are highly complex and dynamic, and the Framework provides a structured approach to identify, assess, and manage the risks.

5. CHAPTER 5: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 INTRODUCTION

This chapter summarizes the entire research project as the final section of the research study. The main theme driving the research was to analyse the cybersecurity challenges faced by public clouds and appropriate intrusion detection mechanisms. In this view this episode serves as a roundup of the whole research paper work which was prepared by the researcher which was in the study in line with the area of research that is PPC Zimbabwe factories. Conclusions were drawn from the data collected in the research area and analyzing the data gathered from the research questions using the views from the National Institute of Standards and Technology (NIST) Cybersecurity Framework stated in chapter 2. In addition, the researcher will provide recommendations in this chapter to ensure appropriate intrusion detection mechanisms that curb the increase of cyberattacks.

5.2 SUMMARY

The main motive of the research was to analyse the cybersecurity challenges faced by public clouds and to address the appropriate intrusion detection mechanisms. This research was based on the researchers observation from the comments made by most of the companies that are making use of cloud services hence a high risk on them facing cyberattacks. Research reference was made to effectively analyse on the cybersecurity challenges in the public clouds and appropriate intrusion detection mechanisms that can be put into use with special reference to the PPC Group.

According to the researchers findings, it is stated that despite the widespread adoption of public cloud computing, cybersecurity is a major concern for organizations. Public clouds introduce new security challenges that require effective intrusion detection mechanisms to prevent data breaches and other cyberattacks. However, existing intrusion detection systems may not be suitable for public clouds due to their unique characteristics, such as multi-tenancy and dynamic resource allocation. Therefore, the need to analyse cybersecurity challenges in public clouds and develop appropriate intrusion detection mechanisms that can

provide effective protection against cyber threats. The idea for conducting this research was driven by the desire to achieve research objectives namely:

- To investigate how data is protected from data breaches as well as unwanted access.
- To analyze the types of cyber security threats that are impacting the organization how they are dealt with.
- To determine the components of intrusion detection techniques that can be used in cloud computing for better protection of information and data.

Chapter 2 of the study critically analyzed relevant literature which is linked to the topic under study. In this chapter, already existing literature by other scholars who focused on the analysis if cybersecurity challenges faced by public clouds and appropriate intrusion detection mechanisms. The researcher was guided by the NIST Cybersecurity Framework because it provides a valuable resource for organizations looking to manage cybersecurity risks in public clouds. The National Institute of Standards and Technology (NIST) Cybersecurity Framework provided a structured approach to help identify and manage risks, and its core functions were highly relevant to the unique challenges of public cloud security and the determination of appropriate intrusion detection mechanisms. Thus at the same time addressing research questions propounded in Chapter I.

The research methodology underpinned in chapter three was the qualitative approach to research, the sampling technique used was random sampling. The research instruments such as interviews were used as the main data gathering instruments. Chapter four was concerned with the detailed findings from responses that were gathered using various data collection instruments. Findings were analyzed and presented in relationship with the views of scholars that were reviewed in chapter two. The data was also analyzed through the guidance of the broad objectives introduced in chapter one.

5.3 CONCLUSION

The chapter consisted of the research summary, conclusions, limitations and recommendations and suggestions for future research. The researcher concludes on the cybersecurity challenges faced by public clouds and appropriate intrusion detection. The study finding show that the majority of respondents were educated, with the highest having a

master's degree in the related field and 40% of the respondents highlighted that they have an advanced understanding of the area under investigation and 60% of them highlighted that they have an intermediate understanding of cybersecurity. The researcher found out that most of the respondents are using cloud computing (80%) and the remaining are using traditional computing. The participants stated that the protection methods that they have been making use of which have been very effective and relevant for them. 40% of the respondents stated that they have been making use of anti-viruses, 30% are making use of complex passwords (with a minimum of 13 characters), for increased security the other 20% update the system software regularly that is weekly, user role assignments are used by the remaining 20%. From the research findings it also shows that 94% of the respondents cited that they have been facing a phishing attack in terms of cybersecurity.

From the research it was evident that the organization had been facing cybersecurity challenges even though they had introduced some detection mechanisms as well as some protection for their company critical data and there are facing a lot of challenges that that needs to be addressed in order to increase their effectiveness of the protection techniques that they have put in place. The chapter also presented recommendations that can be used as remedies to the challenges facing the public clouds.

The study finding show that the respondents suggested that the organization should make use of Hybrid cloud computing because they can help grow the business and move into the cloud while you connect the internal systems. For instance, you can use on-premises infrastructure for sensitive or critical work while a cloud provider hosts less critical network resources
We also gather information that 27% of the respondents stated that they have put firewalls into place for intrusion detection. Some stated that they make use of Aruba Clear-pass, this is an access management system which provides a window into network and covers all access security requirements from a single platform. It has granular role-based policies for authentication, authorization and continuous monitoring as well as enforcement (HPE 2023). 30% of the participants have put Mimecast into place for more protection because it provides the organization with security, continuity and it helps achieve cloud services in a mail management system that is designed to protect emails as well as ensuring and simplifying the tasks and managing emails so as to curb assess of any unknown senders.

Participants gave a number of intrusion detection mechanisms that can be adopted by their organizations to improve and increase data protection and these include intrusion detection console, sensors or agents, management servers and database servers.

The researcher gathered that IDS console, database servers, management servers and IDS sensors are the components of intrusion detection mechanisms that can be used to ensure more security. Intrusion detection system console is one that provides the system administrator with a graphical user interface which will be used to manage the intrusion detection system, view alerts and configure the sensors. The other component is the IDS sensor, this is responsible for inspecting content in each packet for any malicious activity so that it detects and prevents unauthorized and unwanted interference. A management server is responsible for the overall management of the IDS. The last component is the database server which stores information about the detected attacks and alerts generated by intrusion detection systems. The components of intrusion detection mechanisms work to provide a comprehensive and robust system that will be used in the detection and prevention of malicious activities on the network system.

5.4 LIMITATIONS

The research was limited to some information as the respondents were not be able to give out certain information for some reasons beyond their control, for example the fear of victimization and the fact that the information may be very strategic to the success of the company's IT department. However, to counter this limitation and for the benefit of gathering some information, the researcher let the respondents know that it was only for the purpose of a school research. The other limitation that the researcher encountered was that the respondents gave cosmetic results in the bid to protect cooperate image. The senior managers were occupied and failed to get time to attend to the research questionnaires and this posed as a limitation to the research. Lack of financial resources that is, travelling expenses to and from the other plants where research was carried out, internet and data expenses was the other limitation that the researcher faced hence, the researcher carried an electronic interview.

5.5 RECOMMENDATIONS

In the research findings of this research, the researcher came up recommendations that would be remedies for the cybersecurity challenges faced by public clouds and the appropriate intrusion detection mechanisms. The recommendations were proffered to the organizations and individuals that use cloud computing.

The use of anti-viruses, backup tapes, strong passwords, firewalls and updating systems weekly was one of the recommendations to ensure that data is protected

Awareness training videos to ensure that users are aware of how phishing attacks may come to them because users are the weakest links to the organization when it comes to cybersecurity

Ensuring the antivirus is always running and up to date, using email filtering and management tools, as well as regular phishing training for users.

Making use of hybrid solutions because they can help grow the business and move into the cloud while you connect the internal systems. For instance, you can use on-premises infrastructure for sensitive or critical work while a cloud provider hosts less critical network resources.

Making use of intrusion detection mechanisms like anomaly-based, signature based, host-based and application based intrusion detection mechanisms to help prevent data breaches and attacks. Signature-based intrusion detection technique. This approach, also known as knowledge-based, involves looking for specific signatures and when they occur, almost invariably they imply bad news. Signature based intrusion detection mechanisms read malware or packets sent by attackers in the attempt to create or leverage a security breach. These solutions generate fewer false positives than anomaly solutions because the search criteria is so specific, but they also only cover signatures that are already in the search database (which means truly novel attacks have good odds of success).

Host-based intrusion detection techniques revolve around individual hosts — usually

servers — by monitoring the hard drive and both inbound and outbound packets, and constantly comparing the results against a pr-created image of the host and the host's expected packet flow. The idea is to look for malicious changes both in the logical contents of the host as well as the host's activity. It often relies on a local client or agent of the IDS system to be installed on the host.

Application-based intrusion detection techniques widen the scope to an application in an abstract sense — meaning, everything in the infrastructure that's involved in the way that application functions, but only that application. These solutions are used for applications that perform particularly crucial functions for the organization, because the potential consequences of a breach are high.

The intrusion detection techniques and they stated that the IDS solutions will evolve in such a way as to integrate with more infrastructural solutions, as well as incorporate new strategies at a basic level. For instance, through neural network/artificial intelligence capabilities, IDS anomaly-based solutions should be able to more accurately predict and recognize "normal" activity — which also means they'll be able to spot malicious activity faster, and generate a much lower percentage of false positives – without the tremendous amount of continuous tuning effort that takes place.

5.6 FURTHER RESEARCH

Dealing with cyber-crime issues is very pertinent in the management of businesses in Zimbabwe. Further research should be done on evaluating or integrating cybersecurity in public clouds and mitigating appropriate intrusion detection mechanisms. In as far as understanding the general state of cybersecurity infrastructure for Zimbabwean organizations, there is need for that assessment of how prepared, the knowledge, perception and needs for the management that are hindering the implementation of adequate cybersecurity and curb the dexterity of cyber-criminals. According to United Nations report on global security, the African continent has long been considered as an opportune for cyber-criminals to commit criminal acts. Statistics derived from various sources indicate that Africa is very prone to cyber-related threats due to high numbers of domains coupled with very weak network and information security.

APPENDIX

INTERVIEW QUESTIONS

1) Kindly choose your experience level

- O 0-2 years
- O 3-5 years
- O 6-8 years

2) How well do you understand cybersecurity?

3) Which type of computing is your organization currently using?

4) How do you protect your organization from data breaches and unwanted access ?

5) What measures have you put in place to raise awareness for cyberattacks like spoofing a phishing?

6) What are the challenges being faced by your organization in terms of cybersecurity?

7) Which types of cyberattacks have affected your organization before?

_____

_____

_____

8) What are the possible interventions that can be implemented by your organization to protect their data, networks and systems from malicious attacks?

_____

_____

_____

9) Which solution do you see as the most suitable for your organization in terms of cloud computing?

_____

_____

_____

10) What tools have been put in place by your organization for intrusion detection?

_____

_____

_____

11) What are the components of intrusion detection techniques that can be used by your organization for better data protection?

_____

_____

_____

Name of interviewer : TATENDA I TAKAWIRA

Designation: CIS STUDENT

Signature: _____

Date: 12 – 13 FEBRUARY 2023

REFERENCES

1. Eisenhart, M. (1991). Conceptual frameworks for research circa 1991: Ideas from a cultural anthropologist; implications for mathematics education researchers. Paper presented at the Proceedings of the Thirteenth Annual Meeting North ADMINISTRATIVE ISSUES JOURNAL : CONNECTING EDUCTATION, PRACTICE, AND RESEARCH 25 Grant & Osanloo DOI: 10.5929/2014.4.2.9 VOLUME 4, ISSUE 2 b American Paper of the International Group for the Psychology of Mathematics Education, Blacksburg, Virginia, USA.

2. Miranda Mowbray, Siani Pearson. 2009. A client based privacy manager for cloud computing. COMSWARE '09

3. B.Meena, Krishnaveer Abhishek Challa. 2012." Cloud Computing Security Issues with Possible Solutions" IJCST

4. Sai et al. (2015). *Classification of Point of Sale nformation Security Threats: Caseof Smes In Zimbabwe.* Research Inventy: International Journal of Engineering And Science.

5. Alkandary and Alhallaq. (2016). *Computer Security.* International Journal of Advanced Research in Computerand Communication Engineering.

6. https://www.nist.gov/cyberframework

7. Cybersecurity Framework | NIST

8. Understanding the NIST cybersecurity framework

9. Cybersecurity Framework Implementation Guidance

10. Krainovich-Miller B. (2010): Gathering and appraising the literature. In LoBiondo-Wood G, Haber J. (Eds)Nursing research: methods and critical appraisal for evidence based practice. Seventh Edition, MosbyElsevier, Missouri, 56-84.

11. Imenda S. (2014): Is there a Conceptual difference between Conceptual and Theoretical Frameworks? Journal of Social Science, 38(2):185-195.

12. Bande S. (2018): Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities. International Journal of Cyber Criminology,Vol. 12, Issue 1, January-June 2018

13. Seuring, S. and Gold, S. (2012), "Conducting content-analysis based literature reviews in supply chain management", Supply Chain Management, Vol. 17 No. 5, pp. 544-555. Retrieved from: https://doi.org/10.1108/13598541211258609

14. Creswell, John W.2009 . Research design: Qualitative, quantitative, and mixed methods approaches/John W. Creswell.—3rd ed. p. cm. Retrieved from ; Creswell, John W.2009 . Research design: Qualitative, quantitative, and mixed methods approaches/John W. Creswell.—3rded. p. cm. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjckN3C94P7AhUFh1wKHXviA7MQFnoECCoQAQ&url=https%3A%2F%2Fwww.ucg.ac.me%2Fskladiste%2Fblog_609332%2Fobjava_105202%2Ffajlovi%2FCreswell.pdf&usg=AOvVaw0Tgstt9jdhN02OqiC3NS3c

15. https://www.trellix.com/en-us/security-awareness/cybersecurity/what-is-cybersecurity.html

16. https://d1wqtxts1xzle7.cloudfront.net/48737531/Data_collection_tecniques_Chaleunvong_Laos_2009-with-cover-page-

17. https://library.up.ac.za/c.php?g=485435&p=4425510#:~:text=Data%20analysis%20is%20the%20most,determine%20patterns%2C%20relationships%20or%20trends.

18. Blumberg, B, Cooper D.R, & Schindler P.S. (2005). Business Research Methods, Mc Graw Hill: Berkshire.

19. https://www.scribbr.com/methodology/research-ethics/

20. https://www.geeksforgeeks.org/difference-between-cloud-computing-and-traditional-computing/

21. https://aws.amazon.com/what-is/mfa/

22. https://learn.microsoft.com/en-us/exchange/permissions-exo/role-assignment-policies

23. Jansson, K.; von Solms, R. (2011-11-09). "Phishing for phishing awareness". *Behaviour & Information Technology*. **32** (6): 584–593. doi:10.1080/0144929X.2011.632650. ISSN 0144-929X. S2CID 5472217.

24. https://www.arubanetworks.com/products/security/network-access-control/secure-access/

25. National Institute of Standards and Technology (NIST) U.S DoC- 100 Bureau Drive Gaithersburg, MD 20899 https://csrc.nist.gov/glossary/term/intrusion_detection_system