Social technologies and cyber security challenges in Zimbabwean universities: a case of the University of Zimbabwe

FARAI FRANCISCO MADYIRA (R029029X)

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION

2015

GRADUATE SCHOOL OF MANAGEMENT
UNIVERSITY OF ZIMBABWE

SUPERVISOR: DR. G. HAPANYENGWI

DEDICATION

This dissertation I dedicate it to my sister Barbra Madyira, my wife Perseverance Mapunga and my two sons, Adriel Ropafadzo and Absolom Mufaro.

DECLARATION

I, Farai Francisco Madyira, do hereby declare that this dissertation is the result of my own investigation and research, except to the extent indicated in the Acknowledgements, References and by comments included in the body of the report, and that it has not been submitted in part or in full for any other degree to any other university.

_____	_____
Student Signature	Date
_____	_____
Supervisor Signature	Date

ACKNOWLEDGEMENTS

I would like to express my profound gratitude to all the people who contributed to ensure the successful completion of this dissertation. First and foremost, I would like to thank my supervisor Dr. G.T. Hapanyengwi, Director of Computer Centre and Lecturer at the University of Zimbabwe, for his expertise and guidance throughout the entire research process. I thank you Sir for your support. Secondly, my appreciation to my sister Barbra Madyira for without her financial support this project could not have been a success. I thank you Magumbo may God Bless You. I also thank Esau Dure, my sister The Late Lydia Kudakwashe Madyira and my brother Daniel Makundwaneyi Madyira for the advisory role that they played. I really appreciate your contributions for without them this dissertation would not have been a success. Last but not least I am extremely grateful to my wife Perseverance Mapunga and my two sons Adriel Ropafadzo and Absolom Mufaro for their support and understanding throughout my entire studying period. Thank you very much, I owe you one.

ABSTRACT

The introduction of social technologies in the education sector saw an upsurge in the intensity of their use on campus data networks. This study was driven by this phenomenon in a bid to determine if the uses of these social technologies contribute to a myriad of other challenges that institutions of higher learning have to grapple with as well as determining the level of usage and the diversity of the social technologies that are used in these institutions. After this determination, recommendations were given in line with the findings.

The study was conducted in the form of a case study. It was a quantitative survey that utilised questionnaires as the sole form of data collection. The data was collected from 3 groups which are non-technical staff, students and technical staff.

The study discovered that there is intensified use of diversified social technologies at the University of Zimbabwe. These social technologies have resulted in an increase of cyber security risk of the University of Zimbabwe. This risk increase was strengthened by a number of factors which include limited financial resources, lack of prioritisation, and threats awareness of the users and the perception of cyber security by the users. It was therefore recommended that for future studies with the same structure, triangulation should be applied. Furthermore, the university should come up with programmes to raise awareness on cyber security as well as changing the perceptions of users on cyber security roles. There is also the need to mobilise financial resources so as to bridge the gap between technological development and the status quo.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE: INTRODUCTION AND BACKGROUND

1.0 Introduction

The last few years have been characterised by the radical growth in the development and usage of social technologies. These have transformed human interactions. Social technologies have therefore become a force to reckon with as businesses stampede to harness the power thereof in profiteering but at the same time exposing themselves to threats that come with these technologies. The dynamic nature of technology entails dynamism of threats as well hence the exertion of pressure on the management of cyber security related issues. It is against this backdrop that this study explores the different forms and dimensions of social technologies and their impact on securing virtual resources and to some extent physical resources in Zimbabwean universities.

The next section will in brief elaborate on the background of the problem, the problem statement, research objectives, research questions, hypothesis/proposition, the significance of the study, scope/delimitation of the study, dissertation outline and finally the chapter summary.

1.1 Background of the Problem

The commercialisation of the Internet resulted in its adoption as the benchmark of communication in the majority of environments and also being viewed as a basic necessity to the society (London and Stytz, 2005). This fuelled the development of social technologies dominated by web 2.0 such as wikis, social networks and weblogs for effective and efficient resource sharing, communication as well as tools for research (Jones, 2007). Indeed this development was welcome as it brought with it benefits both to the society and business. These benefits include convenience, enhancing operations, exploitation of new market possibilities and reduction of costs amongst many others (Bughin, Byers and Chui, 2011). It

can therefore be noted that these positive developments have substantially transformed business organisations in many aspects. It is no longer only about the accumulation of physical wealth for an organisation to make greater impact in a market but also having a significant Internet presence. This presence can easily be made by the use of the existing various social technologies.

In addition, the development of the cyber space has resulted in the unleashing of various threats which range from simple techniques such as spamming to more sophisticated acts of terrorism. On daily basis Internet users encounter new threats that are unleashed onto the cyber space. For Example, on the 24th of November 2014, Sony Pictures encountered cyber security breach from a hacker group referring to themselves as "Guardians of Peace" demanding that the company should cancel the scheduled release of the film "The Interview" (Robb, 2014). The actions of the hackers resulted in the exposure of sensitive corporate information into the public domain. This dimension further complicates an already complicated management structure of business organisation.

1.1.2 Social Media and Cyber Security Challenges in Zimbabwe

The Chief Executive Officer (CEO) of Astro Mobile is quoted in The Zimbabwe Mail online newspaper saying that more than 90% of Zimbabwean firms are cyber-crime vulnerable (Njanjamangezi, 2014). The most vulnerable organisations include banks. The cyber security vulnerabilities have been augmented by the use of Wireless Fidelity (Wi-Fi) technologies which further expose these organisations to cyber-criminal activities since most of these are not properly secured. In addition, the accessing of social technologies through corporate Internet is also a contributing factor as this simplifies the job of cyber criminals such as hackers to easily penetrate the corporate networks if not properly secured. Zanamwe, Rupere and Kufandiribwa (2013) provide evidence that there is intensive use of social technologies by students in the institutions of higher education in Zimbabwe. This intensified use of social technologies is mainly done by utilising the Internet resources in these institutions and hence contributing to increased cyber-crime vulnerabilities.

1.2 Problem Statement

Effective security, whether physical or virtual is an essential element in an organisation, and universities are no exception. Immense challenges begin to emerge as the population in the cyber space increases as well as the diversity of technologies at play and their rapid change. This phenomenon characterises the structure of most universities in Zimbabwe and hence the need to explore the relationship between the diverse social technologies and cyber security issues before an insurmountable damage has been caused. The increased use of social technologies has resulted in many cyber security flaws thereby complicating the management of Information and Communication Technology (ICT) resources in universities.

1.3 Aims and Objectives of the Study

1.3.1 Aims

The aim of this research is to explore the impact of increased social technologies usage on cyber security in Zimbabwean universities.

The study is anchored on three specific goals, which are:

1. To assess the level of usage of social technologies in Zimbabwean universities.
2. To identify how social technologies are contributing to the cyber security challenges.
3. To highlight the implications on cyber security policy as a result of increased usage of social technologies.

1.3.2 Objectives

The study is anchored on three specific objectives, which are:

1. To assess the level of usage of social technologies on the University of Zimbabwe data network.

2. To evaluate the level of cyber security awareness of users on the University of Zimbabwe data network.
3. To highlight the implications on cyber security policy as a result of increased usage of social technologies on University of Zimbabwe data network.

1.4 Research Questions

By conducting this study, the focus is to obtain answers to the following questions.

1. What is the level of usage of social technologies at the University of Zimbabwe?
2. How are social technologies contributing to cyber security challenges?
3. What are the policy implications that the University of Zimbabwe can observe for the increased safe usage of social technologies with respect to cyber security?

1.5 Hypothesis/Propositions

This research study will fundamentally be based on the following hypothesis:

H0: The increased usage of social technologies did not result in increased cyber security challenges at the University of Zimbabwe.

H1: The increased usage of social technologies resulted in increased cyber security challenges at the University of Zimbabwe.

1.6 Significance of the Study

In this era that we are living in our interactions whether social or professional are extremely dependent on the use of social technologies. This being the case, this leaves a lot to be desired about our cyber space security as a people to safeguard our interests and resources at this intensified use of technology. Cyber security is a sensitive issue to any organisation. An organization becomes even more vulnerable as the number of users, technologies and knowledge increases. It is therefore the intent of this study to explore and explain the relationship between cyber security challenges and the increased use of social technologies at the University of Zimbabwe. This paves the way for the development of solutions to mitigate the increased cyber security risk that characterises most organisations in Zimbabwe. The study will also contribute to the body of knowledge on cyber security issues.

1.7 Scope/Delimitations of the Study

Delimitations are those elements which limit the study's scope and also define boundaries of the same (Simon, 2011). This study therefore, seeks to explore the relationship between social technologies usage in Zimbabwean universities and cyber security challenges. It is against this background that the study was confined to the University of Zimbabwe community as it is large enough to be representative of other institutions of higher learning in Zimbabwe. The University of Zimbabwe comprises of 8250 students and staff complement of 3 485 which gives a population of 11 735 for the 2014.

1.8 Dissertation Outline

This chapter focused on the introduction and background of the study covered by this dissertation. Chapter 2 will present the literature review that is relevant to this study while Chapter 3 will focus on the methodology to be applied during the investigation. Results and

discussion of the study are presented in Chapter 4. Chapter 5 will close the dissertation with a presentation of the conclusions and recommendation drawn from the study.

1.9 Closing Remarks

In summary, this chapter gave the introduction and background of the study which laid the foundation of the problem statement. The problem statement was then provided to illustrate the inspiration of conducting the research work. In this chapter, the outline of the dissertation, scope of the research, significance of the study, hypothesis of the study, research questions as well as the objectives of the study were exposed. In the following chapter, the focus will be on reviewing literature that will clarify the concept of social technologies and cyber security challenges in Zimbabwean universities as well as the exploration of other related researches that were conducted in the past.

CHAPTER TWO: LITERATURE REVIEW

2.0 Background Remarks

This chapter will present literature review that indicates the state of knowledge relevant to this study. Topics that are covered include social technologies, cyber security, social technologies and education in Africa, social technologies and education in Zimbabwe, cyber security in Africa, cyber security in Nigerian Institutions, cyber security in Zimbabwe, social technologies and cyber security challenges and lastly the conceptual framework.

2.1 Introduction

The introduction and embracement of the Internet in developing countries has seen the ushering in of a new paradigm (Hungwe, 2002). Zimbabwe as a developing nation experiences the former mainly through the utilisation of social technologies at this stage. This transformation has also been critical even in the developmental process of educational institutions such as the University of Zimbabwe (Zanamwe *et al*., 2013). The transformation came about as a result of social technologies growing in popularity in business organisations as they are used to enhance their operations as well as exploit new market spaces (Bughin *et al.,* 2011 and Skaržauskien, Pitrnait-Žilnie, Leichteirs and Paunksnie, 2014). It is against these developments that institutions of learning in developing and emerging economies such as Zimbabwe draw their inspiration to virtualise their educational resources as a way of complementing the traditional teaching approach.

However, these social technologies have evidently shown that besides providing progressively more efficient ways for communication as well as learning, they also present consequential problems in the very same education sector (Berg, Berquam and Christoph, 2007). This being the case, literature has it on record that these potential damages are still to be fully comprehended by the researchers (Treem and Leonadi, 2012).

It is therefore the focus of this chapter to provide the theoretical framework of the research by exploring the literature that underpins the critical concepts of social technologies usage in Zimbabwean universities with respect to cyber security challenges.

2.2 Definition of Key Terms

This research is underpinned by two key concepts. These concepts are social technologies and cyber security. The following two sub sections provide the working definitions for this research with respect to these concepts.

2.2.1 Social Technologies

The recent past has seen the birth of popular social technologies such as Twitter (2004), Facebook (2004) and MySpace (2003). Social technologies are those various digital mechanisms that mankind in their individual or diverse groupings use in interacting, communicating, in an effort to convey information, data and knowledge or as a way of making decisions. Therefore, these are the digital tools that can be used to interact or collaborate. Chi (2011) refers to social technologies as Internet and mobile based technologies that are used by people to interact and communicate. He attributes that the main use of these social technologies is sharing content with one another with the most popular being social networking sites. Social technologies can be said to exist in two major states, that is, as socialising technology or as collaborating technology (Skaržauskienė, Tamošiūnaitė and Žalėnienė, 2013). These assortments exist because we use different technologies for different purposes.

Furthermore, this concept of social technologies is deeply rooted in the social sciences with particular focus on human interaction and communication. Derksen, Vikkelsø and Beaulieu (2012) assert that all technologies can be referred to as social technologies as they contribute to the shaping of societies. This argument rests on the fact that social technology combines

two aspects which are society and technology. In this regard, social technology refers to the usage of systematic intelligence in the modelling and management of social entities (Auger, 2010).

2.2.2 Cyber Security

The evolution of the Internet and the perpetual increase in connectivity has seen a surge in the cyber space threats hence the need for cyber security (Belk and Noyes, 2012). This has created immense challenges for individuals, business organisations and governments. These challenges arose as a result of the increased reliance on computer systems by society and business organisations in general (KPMG, 2011). As a result the term cyber security is fairly new though based on the old concepts of systems protection. It has been noted that variations do exist in the definition of this term (Delloitte, 2014, Microsoft, 2011 and PWC, 2011). The variance in the definitions is a result of different perspectives which include citizen, business and government perspectives. The general consensus is that the term is a description of the capacity of an entity to secure its cyber resources from a cyber-attack. According to Cole, Chetty, LaRosa, Rietta, Schmitt and Goodman (2008) cyber security exists in two states which are passive and active. The main objective of passive cyber security is to restrict unauthorised access to a system, which can be either intentional or unintentional, by coming up with preventative mechanisms to safeguard data resources from being compromised, stolen or attacked. In some instances this is referred to as cyber-defence. On the other hand, active cyber security deals with the ability to track attackers with the aim of stopping the present attack or preventing another attack.

In addition, cyber security is a science which is also deeply anchored in computer sciences but also related to fields like medicine, epidemiology and economics (Jason, 2010). It is a dynamic discourse because the threats to be prevented continue to evolve at an alarming rate. This dynamism tends to create a lot of challenges in as far as the determination of a stable and secure cyber environment is concerned. As a science, it gives direction to the conduct of research in order to bridge the gap created by the evolving threats.

2.3 Social Technology Trends

The recent past has witnessed a consecutive introduction of several social technologies. These technologies have immensely transformed human interactions and communication with a visitor spending 66% more time on social technology sites in 2010 as compared to 2009 (Vanheuangdy, 2010). Face-to-face associations have evolved and are now heavily dependent on social technologies. This has seen a great reduction in the cost of communication across the globe hence benefiting both individuals and corporate groupings in a number of ways. These benefits are enshrined in the ability of social technologies to cheaply and easily relay information and its magnitude in availability which has empowered the society to self-teach on both good and bad subject matters of life.

The benefits and power associated with social technologies has led to all forms of organisations stampeding to harness the power of these technologies. It has been due to the realisation of the existence of a number of dimensions that business organisations, whether profit making or non-profit making, can benefit from the use of these technologies. One of the interesting developments was the adoption of social technologies in the political arena (Langmia, 2013) although their impact can be felt in the entire spectrum of the human activities. In the same article, it is articulated that the success of politicians such as Barack Obama clearly demonstrates that social technologies are instrumental in our modern communication system. They are a crucial tool in education of any kind. Clearly, this development has ushered in a new paradigm in global politics.

However, it has been realised that full permeation has not been attained yet because some quarters regard social technologies as surrounded by ambiguity (Government of India, 2011). Business organisations are the majority of those disregarding the use of social technologies as they cite cyber security concerns. It has also been noted that the absence of the basic guidelines and a proper usage framework especially in government agencies of India tends to put off business organisations in the uptake of these technologies.

Furthermore, Hansen and Nissenbaum (2009) discovered that some regimes, for example, China have gone to the extent of banning the use of social technologies citing their destabilising nature as witnessed by most uprisings of the recent past. China in the recent past has been seeking to block the use of social technologies by its citizens citing that they are a threat to the stability of society and politics at large.

2.3.1 Social Technologies and Education in Africa

Africa as a continent has the majority of its members as developing countries with the exception of a couple which are emerging economies. According to Boora and Chazovachii (2010) the majority of the African population still has no access to the rudimentary Information and Communication Technology (ICT) and in the event that one has access it tends to be restricted to the urban areas since these harbour those that can afford to acquire and maintain these technologies. The government of Zimbabwe, in its ICT policy framework, acknowledges the existence of the digital divide which is mainly a result of lack of primary as well as the supporting infrastructure and hence targets were set to transform the nation into a knowledge based economy by year 2020 (Isaacs, 2007). This has resulted in a number of projects that are aimed at the promotion of the use of ICTs in the education sector such as African Virtual University Teacher Education Project, College IT Enhancement Programme and Kubatana Trust of Zimbabwe.

The radical rising as well as the adoption of social technologies in the education sector has resulted in the introduction of a new paradigm in the educational sector (Hungwe, 2002). This new paradigm possesses a new set of benefits in the process of teaching and learning as well as new challenges in the management of this new structure. The institutions of learning have two sub-sets that can be derived from them. There exist two groups which are employees and students. These two groups have different roles that they play in the institution but when it comes to the use of social technologies they are unified mainly in socialisation. Challenges will stem from two key sources which are bringing your own devices (Cisco, 2014) and the diversity of technologies that are used. There is therefore the need to balance access using

personal devices that are beyond organisational firewall and protection of the information resources of the organisation.

2.3.2 Social Technologies and Education in Zimbabwe

In Zimbabwe, the Internet has been utilised predominantly for communication activities hence the popularisation of social technologies. Social technologies form one of the key pillars of ICTs. According to Tsokota, Chipfumbi, Mativenga and Mawango (2013), Sub-Saharan countries such as Zimbabwe are prioritising the development of ICTs as a way of attaining the Millenium Development goals one of which is the right to education. The agenda is to provide both hardware and software requirements for communication as a way of bridging the digital divide. Therefore, there has been notable improvement in infrastructural development and the usage of Internet-based communication technologies such as Facebook, WhatsApp and Twitter across the whole spectrum of the Zimbabwean economy.

According to Zimbabwe e-readiness survey report of 2005, the rate of permeation of technology usage is highly dependent on the literacy level (Mhlanga, 2006). At the helm in the education sector are universities which possess the highest levels of ICT literacy rates. There is an unending demand for the upgrading of the infrastructure in the universities in order to satisfy the demand at the same time not compromising the cyber-security element of the institution. The report also alludes to the poor economic performance of the country as a contributing factor to the down play of ICT development in Zimbabwe in general. This has however resulted in most of the technological infrastructure in use being slightly obsolete and expensive. The state of the infrastructure coupled with the fact that 43% of the population is 15 years or younger, the tendency of the users is experimentation which tends to pose cyber-security risks.

Zanamwe *et al*. (2013) provides the evidence that social technologies are used in Zimbabwean universities for both learning and socialisation. Their main focus was on the adoption of social networking sites in which institutions of higher learning have mixed

feelings in embracing them as they have cyber-security fears. They noted that the most commonly used social networking sites are Facebook and MySpace. It is also crucial at this point to also assess the impact of the popular chat system WhatsApp as it has become more popular due to its low cost attribute as well as the popularisation of smart phones which support both Wi-Fi and cellular phone networks.

2.4 Global Cyber Security Trends

Cyber security has become a critical issue that boggles the mind of individuals, private organisations and even governments. Microsoft (2011) reports that hardly a week passes by without a headline pertaining to an attack affiliated to the cyber space. This has seen governments being driven into reactionary mode in order to contain the situations and plan for the future. These actions have resulted in the crafting of frameworks for ICT and in most cases frameworks specifically for cyber security.

According to Malby, Mace, Holterhof, Brown, Kascherus and Ignatiuschtschenko (2013) there exists very strong indications that cyber security, especially cyber crime, is a growing global challenge. This has been driven by the booming growth in connectivity which in turn has to some extent been influenced by the availability of affordable smart devices such as tablets and phones as well as the introduction of online social technologies. Therefore, criminals have been motivated to commit cyber crime as this has created a beneficial opening for them. This is evidenced by the high frequency of cyber crime news globally with developing environments such as Africa also not being spared.

The ITU Telecom World 2013 exhibition which was held in Bangkok, acknowledges the increasing cyber security threats and the need for all stakeholders to work together in bringing sanity in the cyber world (ORF Cyber Monitor, 2013). These threats are the works of individuals or groups who are seeking psychological and or financial incentives. They are basically taking advantage of the fact that 90 percent of the world's people under the age of 40 use social technologies with 73 percent doing their shopping online (*ibid*).

On the other hand, governments are working flat out to try and contain this scourge. The evidence can be drawn from KPMG (2011) where some government initiatives are specified. These government efforts include investments in the improvement of cyber crime defence strategy by the United Kingdom, facilitation on cyber security issues by the United States of America, the establishment of Information Technology Institute by India, the setting up of cyber police unit by Iran and last but not least, the efforts of China to fight cyber crime in partnership with the international community.

2.4.1 Cyber Security in Africa

Africa is currently experiencing adoption of ICTs at an exponential rate with the worrying issues of lack of cyber security awareness. Many authors concur that cyber security is a new challenge that has been added to a host of other challenges that are already bedevilling the African continent with most countries having been caught unprepared in terms of awareness, laws, technical expertise and technical resources (Akuta, Ong'oa and Jones, 2011; Herselman and Warren, 2004; and Odumesi, 2006). Against this background, it is of paramount importance to have collective efforts in Africa aimed at promoting cyber security in the continent. According to Janson (2011) the African continent harbours two nations that are in the top ten of countries with hyper cybercrime activities in the world as of the end of year 2010. These countries are Ghana and Nigeria. Ajao (2008) adds another country to this list which is South Africa. Another survey conducted by KPMG uncovered that 74% of the cyber fraud related cases reported in Africa are accounted to four countries, that is, South Africa, Kenya, Nigeria and Zimbabwe (Government of Zimbabwe, 2015). This is a worrying development as the scourge of cyber crime derails the attainment of the Millennium Development Goals that have been set for the continent (Waziri, 2009).

2.4.2 Cyber Security in Nigerian Tertiary Institutions

Okeshola and Adeta (2013) conducted a study in the Zaria-Kaduna state of Nigeria in order to determine the "nature, causes and consequences of cyber crime in tertiary institutions".

They asserted that Nigerians experience a plethora of cyber crimes which include hacking, cyber harassment and identity theft. These crimes are said to be a threat to the country's security and the financial well-being of the citizens (Akogwu, 2012).

In addition, Olaide and Adewole (2004) discovered that the majority of the perpetrators of these crimes are youths. This is also in line with the findings of the study conducted by Zero Tolerance (2006) as cited by Okeshola and Adeta (2013) which found that the majority of cyber criminals are in the age range of 18 to 30 years. They uncovered that these youths are keen and always come up with new ways of conducting these criminal activities. These youths are found in the institutions of higher learning in Nigeria. Okeshola and Adeta (2013) acknowledge the existence of cyber crimes in Nigerian universities and attributes lack of cyber security awareness on part of the users as the major culprit. This culprit they say has resulted in a negative impact on the economy of Nigeria that is, the crumbling of business confidence as well as credibility of most transactions. This confirms the assertions by Kumar (2003) and Olayemi (2014) that cyber crime is independent of geographic location hence the need to observe cyber security as a global issue that requires significant attention.

Furthermore, Okeshola and Adeta (2013) found out that the escalating cyber criminal activities are as a result of several motivational factors. These motivational factors include disgruntlement, economic benefit, and lack of legislation, inexpensive cost of crime, slim chance of being apprehended and many others. These discoveries were obtained through triangulation where 400 questionnaires were issued out and 12 key participants were interviewed. Their justification of applying the triangulation approach was that it increases the validity of their study as the use of multiple data collection mechanisms results in complementing each other.

2.4.3 Cyber Security in Zimbabwe

Zimbabwe, like all other countries, has not been spared by the scourge of cyber space threats. All organisations in Zimbabwe are potential targets, be they, nongovernmental organisations

(NGOs), and state owned enterprises (SOEs), small, medium and large organisations as long as they are a member of the cyber environment. Cyber security is a new and dynamic phenomenon even to Zimbabwe and posses serious challenges to the nation of Zimbabwe. According to Njanjamangezi (2014) Munyaradzi Gwatidzo the CEO of Astro mobile asserts that more than 90% of organisations in Zimbabwe are exposed to cyber security risks. This has been as a result of many factors chief among them being the poor economic performance in which organisations fail to acquire equipment and training that can cushion themselves against these risks. This is contradictory to the finding of Zimucha, Zanamwe, Chimwayi, Chakwizira, Mapungwana and Madhuku (2012) who certified the electronic banking system in Zimbabwe as offering solid security for the electronic banking service. Their main focus was on the strategies that are being used to safeguard the electronic banking transactions which do not necessarily translate into a secure system as Zimbabwe is still trailing behind in technological developments.

Furthermore, Zimbabwe just like most global nations lacks statutory instruments that can be used to protect organisations from cyber security risks (McConnell International, 2000). This entails that business organisations and governments are entirely reliant on the technical implementations in order to cushion themselves from the prevalent cyber security risks. With this predicament, it is crucial for Zimbabwe to develop strong legal instruments as these compliment the technical efforts that business organisations are implementing as this goes a long way in making the cyber environment a safe haven to do business in. This has also been advocated by Minister of Transport and Communication, Christopher Mushohwe in 2009 when he was quoted by newzimbabwe.com saying Zimbabwe requires new laws on cyber security and cyber crime as cyber criminals are constantly updating themselves hence the laws are trailing behind and never catching up with the developments (Nkatazo, 2009). He highlighted that this has to be done in order to remedy the outdated cyber laws as is the case for many African countries.

According to Ncube (2014), the government of Zimbabwe is formulating “laws to regulate the activities on social media in order to protect its citizens and the state from cyber crimes”. When enacted, the laws will play the role of regulating social technologies content as well as protecting the privacy of the general public from hackers. *Ibid*, the government acknowledges

the dynamism of technology and hence have devoted to be on their toes in the regulation process. Zimbabwe currently does not have any laws that govern social technologies hence it is vulnerable to cyber crimes and cyber terrorism. This has been reflected by the failure of the government to deal amicably with the Facebook case of Baba Jukwa. These and other global trends on cyber security have prompted Chitauro (2015) to advocate that laws to curb cyber crime are vital to the nation of Zimbabwe and the year 2015 should have cyber security on the top of the agenda.

2.5 Social Technologies and Cyber Security Challenges

Social technologies are synonymous with twin edged daggers, in which their misuse is detrimental whilst their correct and consistent use creates significant value for both individuals and organisations. Therefore, it is important for an organisation and its stakeholders to comprehend the unfavourable outcome of using social technologies as tools of trade as this helps in protecting the organisational digital resources (Apau, 2011). This will also enable the organisations to mitigate the cyber security challenges and continue to benefit from the use of social technologies (Chi, 2011).

However, the introduction of social technologies in organisations resulted in the diversification of threats that can cripple organisational activities. The threats range from common elements such as viruses and malware to complex issues such as corporate espionage, phishing, hacking, and cyber bulling and stalking to mention a few amongst many others (Chi, 2011). According to information security breaches survey report of 2014, the size of an organisation does not matter when it comes to cyber attack as victims include the entire spectrum (PWC, 2014). Social technologies have contributed to this as information and or tutorials about attacking systems are made easily available on these platforms. In addition, the profile accounts are also used as a highway into organisational networks hence making it a mammoth task to create a comprehensive cyber security framework. According to Mwenje (2014) there are about 556 million victims of cyber crime every year which translates to over 1.5 million and 18 victims per day and second respectively. He goes on to state that Facebook alone have not less than 600 000 accounts compromised each day. This calls for concern in

business organisations such as universities where large amounts of users connect to Facebook each day through organisational Internet gateways.

Sophos (2010) reports that social technologies have become main targets by cyber criminals especially social networking sites as they are momentous trajectory for losing data and theft of identities. The report also shows that Facebook, of all social technologies, possesses the greatest cyber security risk. This is due to its vast pool of users. It is only natural to find many bad apples in the largest orchard than the smallest. So, Facebook faces the challenge of regulating activities of more that 350 million users. The survey that was carried out at the end of 2009 by Sophos indicates that social technologies are subjected to three major types of attacks which are spam, phishing and malware. Statistics show an increase of 70% of business organisations that have encountered malware and spam through social technologies in 2009. This is because social technology platforms present a significant number of users who are not security cautious and cyber attackers can take advantage of. It is also on these platforms that cyber criminals have found it easy and effective to distribute malware. The power of damage that is packaged in these tools of attack are a cause of concern for business organisations especially educational institutions due to the vast number of social technology users they have at any particular time on their corporate networks. For example in 2005 a worm called Samy was unleashed and it infected 1 million MySpace accounts on its first day of launch (Cavelty, 2008).

Therefore, it should be appreciated that the success of social technologies in organisations comes at a premium as unaware users share the same platform with cyber criminals hence the increase in the cyber security risk (Vanheuangdy, 2010). This escalation of the risk is driven by the over reliance on users to manage the platform as well as creating content. Furthermore, the absence of comprehensive monitoring mechanisms can also be said to contribute to this increase of cyber security risks.

According to Mutero (2014) many businesses in Zimbabwe are faced with the challenge of regulating misconduct with respect to ICT infrastructure especially the use of the internet and related services because of the lack of ICT utilisation policy. This lack of policy to a large

extent entails lack of cyber threats related information and skills that are supposed to be imparted to the users. This increased the cyber security risk of an organisation especially in cases where the misconduct was as a result of accessing an unsafe site which forms the majority of the content that is spammed on social technologies.

2.6 Conceptual Framework

This study is hinged on two major concepts which are cyber security and social technologies. The reviewing of literature has greatly enlightened the researcher on some of the existing relationships of these two components. The generic structure of this study as illustrated in Figure 2.1 indicates that cyber security challenges are core problems that affect the cyberspace. The main target of these threats is the Internet. The million dollar question is why the Internet? It is because social technologies use the Internet as the platform making it easy to attack them. How then do corporate networks fit into this equation? Business corporations are experiencing major cyber security challenges as they are following the trends of connectivity by allowing the accessing of these social technologies through their corporate networks. These challenges are driven mainly by the business corporations' inability to fully and effectively manage the behaviour of both internal and external users of these social technologies. This behaviour is complex as the models used in these interactions is learning together and gives more control to the users rather than administrators.

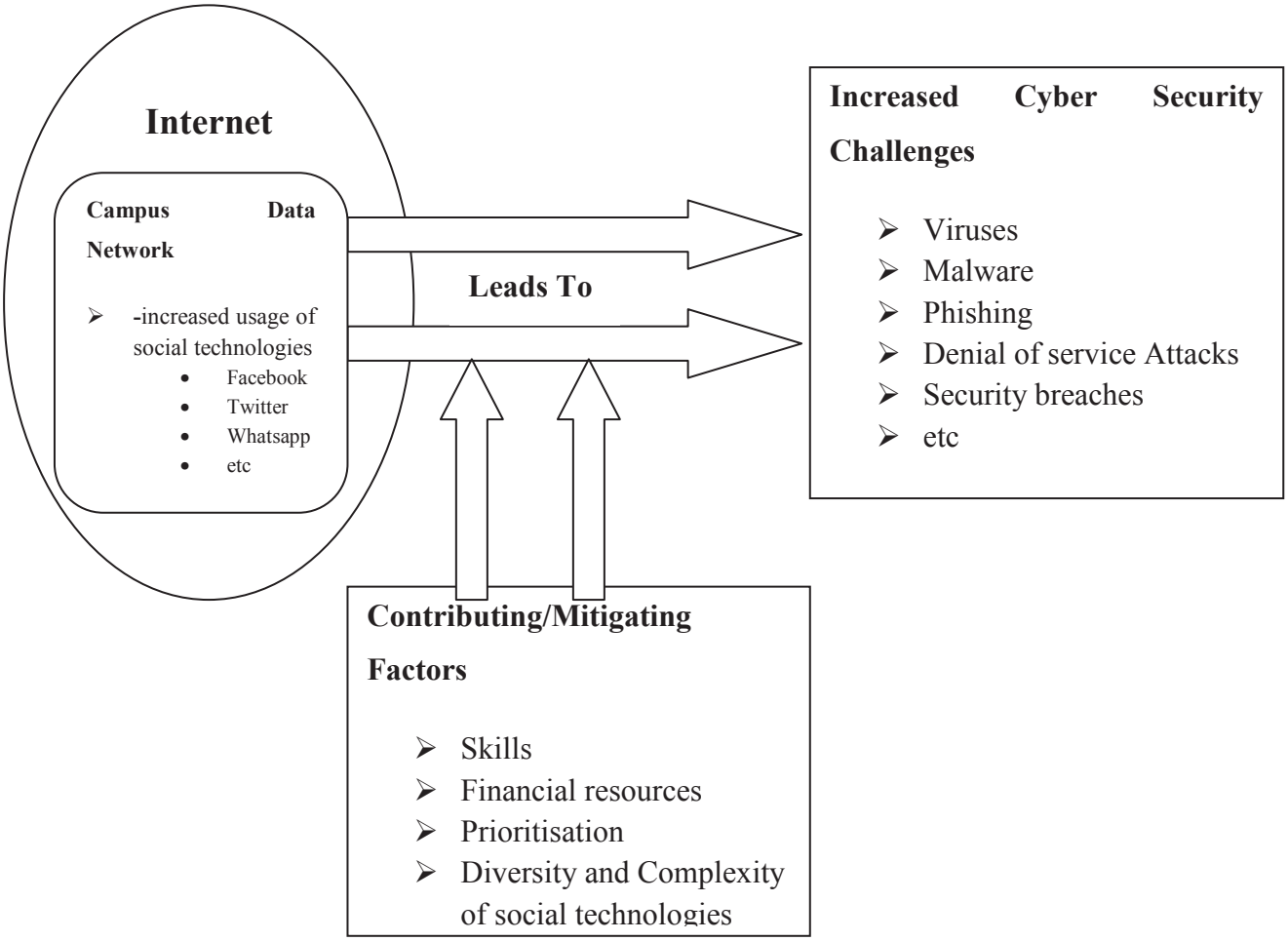

Figure 2.1: Conceptual Framework (Own Diagram)

2.6 Closing Remarks

In summary, this chapter gave the introduction in which two key concepts underpinning the study were defined, that is, social technologies and cyber security. Each of these concepts was then explored with respect to global, African and Zimbabwean contexts. Furthermore, the chapter also gave an account of the known relationship in literature between social technologies and cyber security challenges. Last but not least a conceptual framework key to this study was developed. In the following chapter, the focus will be research methodology in which techniques to be applied in terms of data collection and analysis are justified as well as the associated assumptions presented.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

Research methodology can be defined as a logically organised way of solving a problem (Kumar, 2005). It is an art of specifying how a particular research will be conducted. In an attempt to solve the problem in this study, this chapter will discuss the research methodology approach that has been applied. This includes research design, population and sampling techniques, sources of data, data analysis techniques, research limitations, research ethics and data credibility.

3.2 Research design

According to Burns and Grove (2003:195) research design is "a blueprint for conducting a study with maximum control over factors that may interfere with the validity of the findings". It is the ploy which gives the description as to where, how and when the data will be gathered and scrutinised. The objective is to produce a plan that will enable the researcher to answer questions that are underpinning the study (Polit *et al*. 2001).

3.2.1 Research Philosophy

Research philosophy hinges on the development of the study's nature, background and knowledge (Saunders, Lewis and Thornhill, 2009). It is important as it sets the framework for the study. This research follows a positivist approach as it seeks to carry out experimentation exercise hence quantitative research. The pursuance of the positivist approach is based on the adoption of scientific approaches in order to unravel the truth and be able to present the truth empirically (Henning, Van Ransburg and Smit, 2004). The adoption of scientific approaches entails quantitative methods are at play which requires the researcher to set aside emotions,

biases, experiences and perceptions in order to ensure an objective conduct of the study (Cooper and Schindler, 2006). In addition, a survey will be conducted for this research as there is the need to collect and analyse primary data as well as its conduciveness to the data collection methods to be employed.

3.2.2 Research Strategy

Research strategy can be said to be the conventional method that the researcher employs in dealing with the problems that the study seeks to resolve (Saunders *et al.* 2009 and Bryman, 2008). A number of research strategies exist which include participative enquiry, action research, experiment, archival research, survey, longitudinal research, grounded theory, case study and many others (Collis and Hussey, 2009; Saunders *et al*. 2009 and Easterby-Smith, Thorpe and Jackson, 2008). This study adopts a case study approach (by limiting the study to the University of Zimbabwe) in which a survey is conducted by instituting questionnaires as well as analysing relevant organisational documentation. The use of case study has been deemed appropriate for this study first and foremost because of the existence of the three groups which were the main sources of data for this study. Secondly, case studies support the use of surveys and conducting research in real life form like in this study.

3.3 Population and Sampling Techniques

3.3.1 Population

The term population is defined by Parahoo (2006) as "the total number of units from which data is collected". These are all the units that satisfy the benchmark to be included in the study (Burns and Groove, 2003). In this study, the population comprises of the entire University of Zimbabwe community, that is, both students and members of staff. The students are 8 250 and the members of staff are 3 485 which gives a population of 11 735 for the year 2014.

3.3.2 Sampling

According to Polit and Beck (2004) a sample refers to a segment of the population. A sample is drawn from the target population following specific criteria with the objective of creating representativeness with the target population. In this study, the population was divided into three groups which are students, ICT technical members of staff and Non-ICT technical members of staff. The groups of students and Non-ICT technical members of staff were further subdivided into ten subgroups which are faculties they belong to. These subgroups were created in order to ensure equitable representation from all the faculties of the university. The compositions of these groups are 4 participants for the technical group (as there are only 4 technical people dealing with the network), 355 participants for the non-technical group and 842 participants for the students group. This makes a sample size of 1201 participants which is 10.23 percent of the population with the participants randomly drawn except for the technical group. This sample size was adopted in order to satisfy 95 percent confidence level and 2.68 percent confidence interval for the study. The selection of participants randomly was deemed appropriate as this helps to achieve sample representativeness (Durrheim, 2002).

In the technical group, 4 participants were purposively targeted to provide information for the study. Purposive sampling was pursued as it is ideal for eliciting expert information from the target population as it involves the drawing of respondents that will most appropriately help the researcher comprehend the research questions and problem (Crosswell, 2003).

3.4 Sources of Data

In this study, two forms of data sources are being relied on, that is, primary data sources and secondary data sources. This study pursues the collection of primary data as a way of tapping previously unknown information. Primary data is that data that has been collected first hand (Reitz and Wing, 2008). In this case, primary data is collected using questionnaires as explained in the data collection section. Furthermore, it also relies on secondary data. This is

the data that was collected without this study in mind (Booth, Colomb and Williams, 2008). In this regard, the data pertains to system security reports.

3.5 Data Collection Procedure (Research Instrument(s))

Data collection is a crucial element of any research as poor data collection techniques impact negatively on the results (Vuuren and Maree, 2002). Brown and Rogers (2002), state that before attempting anything important with regards to a study, data needs to be collected. It is against this background that this study implements questionnaires (see Appendix 2, Appendix 3 and Appendix 4) as the key data collection mechanism. This research focuses on collecting data from three groups that are categorized, questionnaires were therefore deemed appropriate as there is a broad spectrum of respondents as well as its ability to provide for anonymity of the respondents hence the promotion of confidentiality.

Three questionnaires are designed for the three groups but generally the Students and the Non-Technical Groups respond to the same questions as they all constitute the user base. All the three questionnaires comprise two sections which are Background Information and Social Technologies and Cyber Security. The user base groups have crucial questions that rate the social technologies intensity of use, what purpose the technologies are used for, cyber security awareness, authentication awareness and use, cyber security perceptions as well as technological diversity. These are the vital questions that aid in the determination of the level of usage and the contribution of this usage towards cyber security challenges. These questions are then contrasted with the real campus data network facts as given by the Technical group which has a questionnaire with different questions through some address the same objective of the user base. Further, the Technical group questions go on to assess the factors that impact cyber security challenges which include skills, financial support and prioritization.

3.6 Data Analysis

According to Mouton (2002) data analysis is the application of both mathematical and statistical approaches with the aim of focusing on particular variables in the data collected. The data collected using the instruments mentioned in the previous section will be analysed using Statistical Package for the Social Sciences (SPSS) version 16. SPSS was chosen for this study because of its ability to handle large amounts of data as well as its ability to prepare an in-depth analysis of the available data set. Using this software package the following analysis methods will be applied:-

- Correlation analysis
- Regression analysis
- Trend analysis
- Frequency analysis

3.7 Research Limitations

Security of any entity is a critical and sensitive issue. In this regard, the researcher foresees limited disclosure of certain security elements by information communication technology (ICT) personnel of the target institutions. This has been factored in the design of the questionnaire in which two differently phrased questions have been developed so as to evaluate the credibility of the responses. Furthermore, privacy assurance is given to the respondents with respect to the anonymity and what the data will be used for. In addition, due to the nature of the information that is required pertaining to cyber security challenges, convenience sampling will have to be employed in order to target the ICT specialists in the universities. The targeting of the ICT specialists ensured that reliable data about the technical aspects of the study comes from the right sources.

3.8 Research Ethics and Data Credibility

Ethical issues are embedded in doing what is right or what is wrong. It is one of the major considerations of this research to conduct it in the right way. Crosswell (2003) asserts that when conducting a study, the researcher has the mandate to observe the desires, needs, rights and values of participants. It therefore means that respondents have the ultimate right to make reasonable decisions in as far as responses are concerned (Graziano and Raulin, 2004) as well as ensuring that the respondents identify the findings of the study as their experiences (Streubert and Carpenter, 2011). This will be ensured by adhering to the principles which include:-

- Participants will participate voluntarily and not coerce them.
- Prospective participants will be fully informed about the research and will have to give their consent (see Appendix 1).
- Confidentiality and anonymity will be guaranteed (see Appendix 1).
- Respect will be given to intellectual property.
- Participants will respond to the same key questions.

3.9 Closing Remarks

In this chapter, attention was given to the crucial elements that make up the research methodology that was applied in this study. These key elements include the research design, population and sampling techniques, sources of data, research limitations, research ethics, data credibility and data analysis. In the next chapter, data presentation, the task will be to present the data that has been collected using the instruments discussed in this chapter.

CHAPTER FOUR: RESULTS AND ANALYSIS

4.1 Introduction

This chapter outlines the results of the various statistical analysis that were applied to the data collected through the survey that was conducted for this study. The analysis includes two major categories which are descriptive statistics and inferential statistics.

4.2 Descriptive Statistics

This study included 1 176 participants. This number is made up of three groups of participants which are 3 Technical Staff participants, 348 Non-Technical Staff participants and 825 Students participants. Table 4.1 below illustrates these figures as well as the response rates which are 75.00%, 98.03% and 97.98% respectively for each group.

Table 4.1: Response Summary

Group	Group Size	Responses Received	Response Rate (%)
Technical Staff	4	3	75.00%
Non-Technical Staff	355	348	98.02%
Students	842	825	97.98%
Total	1 201	1 176	97.92%

These responses when analysed by gender indicate that there was 1 female and 2 male responses in the Technical group, 165 female and 183 male responses in the Non-Technical group and 320 female and 505 male responses in the Students group. This translates to a total

contribution of 41.33% for females and 58.67% for males. These statistics are reflected in Table 4.2 including percentage contribution of gender as 33.33% for females and 66.67% for males; 47.74% for females and 52.59% for males; 38.79% for females and 61.21% for males respectively for each group.

Table 4.2: Response Rate by Gender

Group	Females Responses	Female Contribution	Male Responses	Male Contribution
Technical	1	33.33%	2	66.67%
Non-Technical	165	47.74%	183	52.59%
Students	320	38.79%	505	61.21%
Total	486	41.33%	690	58.67%

Further, when these responses are decomposed by age, the age group 20 to 29 years had the major contribution of 58.37%. The youth are regarded by many to be 30 years and younger therefore the contribution rate of the youths in this study are in line with the findings of Okeshola and Adeta (2013) that most of the users of ICTs in Tertiary Institutions are in the youth category. Figure 4.1 illustrates these statistics per age category for this study.

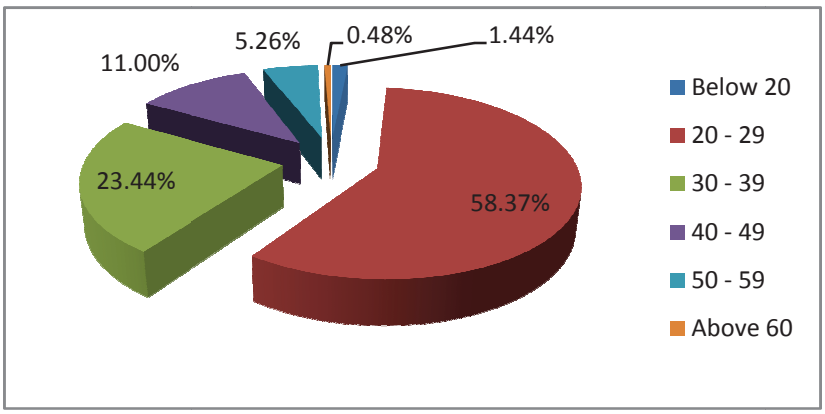

Figure 4.1: Response Rate by Age

One of the key determinants of the study was to assess the level of awareness of cyber security threats that are associated with social technology and the extent to which users of social technologies on University of Zimbabwe campus network are helping to avert the cyber security threats scourge. In this regard, three elements can be assessed which are user awareness of cyber security threats, usage of default security mechanisms and the user perception of cyber security.

Table 4.3: User Awareness of Cyber Security Threats and Authentication Mechanisms

Response	Threats Awareness (Non-Tec Staff)	Threats Awareness (Students)	Authentication Awareness (Non-Tec Staff)	Authentication Awareness (Students)
Yes	74.07%	71.43%	31.48%	22.55%
No	25.93%	28.57%	68.52%	77.55%
Total	100%	100%	100%	100%

Table 4.3 clearly shows that the majority of both Non-Technical Staff and Student users of social technologies on campus are aware of the security threats that are associated with their use. This is indicated by scores of 74.07% and 71.43% respectively. However, what was disturbing are the perceptions of these users in terms of what they do in reaction to them being aware of these threats. This is indicated by their lack of knowledge of the Two Factor Authentication mechanism which is a step higher in securing social technologies accounts. In assessing their awareness of this authentication mechanism it was discovered that these groups consisted of 31.48% and 22.55% of users who were aware of this mechanism which implies that most of the users are using default security mechanisms hence their accounts are vulnerable which increases the security risk of the University of Zimbabwe data network. In addition, Figure 4.2 and Figure 4.3 illustrate the perceptions of these groups with the minority 20.37% and 27.84% being the only perception in which users are actively taking part in securing their accounts with the rest either arrogant or not knowledgeable.

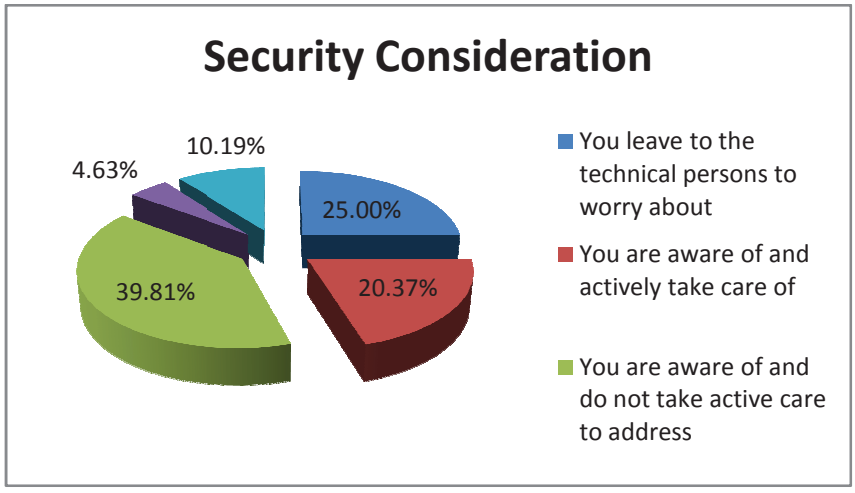

Figure 4.2 Perceptions of Non-Technical Group on Cyber Security

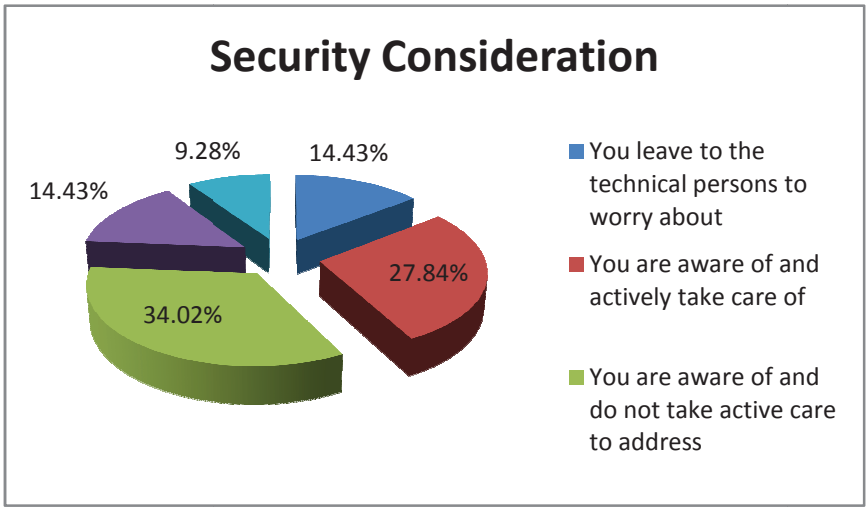

Figure 4.3 Perceptions of Students Group on Cyber Security

In this regard, it was also crucial to assess the intensity of social technologies usage owing to these negative perceptions. In Table 4.4 and Table 4.5, intensity of use being considered to be high in the range scale 5 to 10. The results indicate that there is high usage of social technologies in on campus data network as those considered to be light users are 19.44% and 41.84% for Non-Technical Staff and Students respectively. This has also been affirmed by all participants of the Technical Staff group who indicated that there has been an upsurge of traffic on the data network due to the usage of these social technologies on campus. This intensified use (as indicated in Table 4.4 and Table 4.5) and negative perceptions (as

indicated in Figure 4.2 and Figure 4.3) increases the cyber risk level of the university. This has also been confirmed by the security experts (i.e. Technical Staff) that the usage of these technologies alone increases the cyber security risk of the university.

Table 4.4: Non-Technical Staff Group Level of Social Technology Usage

Scale	Frequency	Percentage	Cumulative Percentage
1	32	9.26	9.26
2	6	1.85	11.11
3	29	8.33	19.44
5	61	17.59	37.04
6	32	9.26	46.30
7	39	11.11	57.41
8	84	24.07	81.48
9	45	12.96	94.44
10	19	5.56	100.00
Total	348	100	

Table 4.5: Students Group Level of Social Technology Usage

Scale	Frequency	Percentage	Cumulative Percentage
1	160	19.39	19.39
2	17	2.04	21.43
3	93	11.22	32.65
4	76	9.18	41.84
5	227	27.55	69.39
6	118	14.29	83.67
7	34	4.08	87.76
8	76	9.18	96.94
9	25	3.06	100.00
Total	825	100	

The increase in cyber security risk can further be affirmed by assessing the usage of authentication mechanisms as they are a step higher than the default security mechanisms for social technologies as shown in Figure 4.4 and 4.5. In the two groups, Non-Technical Staff and Students, 21.30% and 13.27% respectively attribute to those who are aware of these security mechanisms and have implemented them on their social technologies accounts and can safely be said to be security conscious. The remainder of these afore-mentioned group comprises firstly of 10.19% and 10.20% respectively of those who are aware of the authentication mechanisms but they do not use them. These can be referred to as security arrogant users. Lastly the composition of 68.82% and 76.53% are those users who have no idea what the two factor authentication mechanism was. So overall, it can be noted that in both groups the majority of the users are using default security mechanisms which places the institution's risk of cyber security higher.

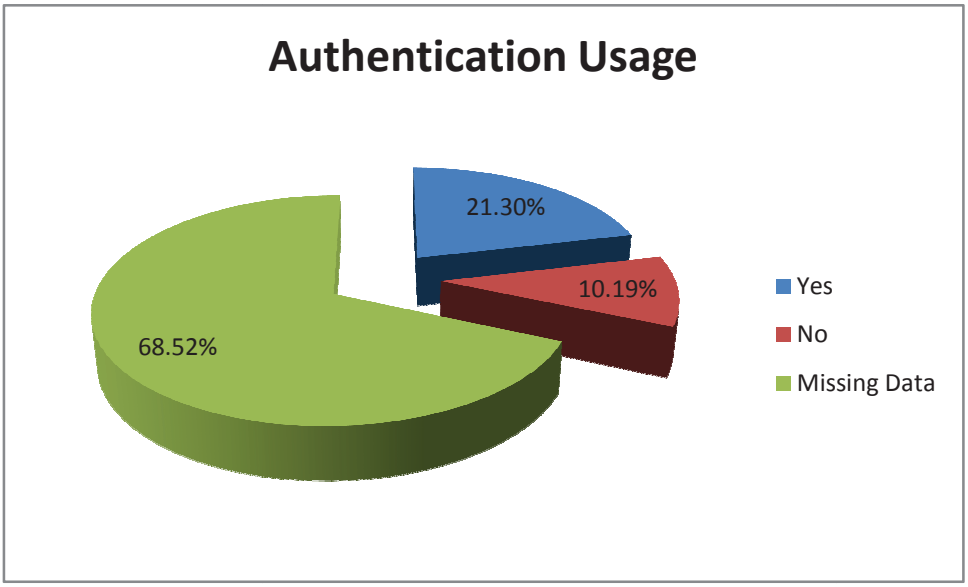

Figure 4.4: Authentication Usages of Non-Technical Staff

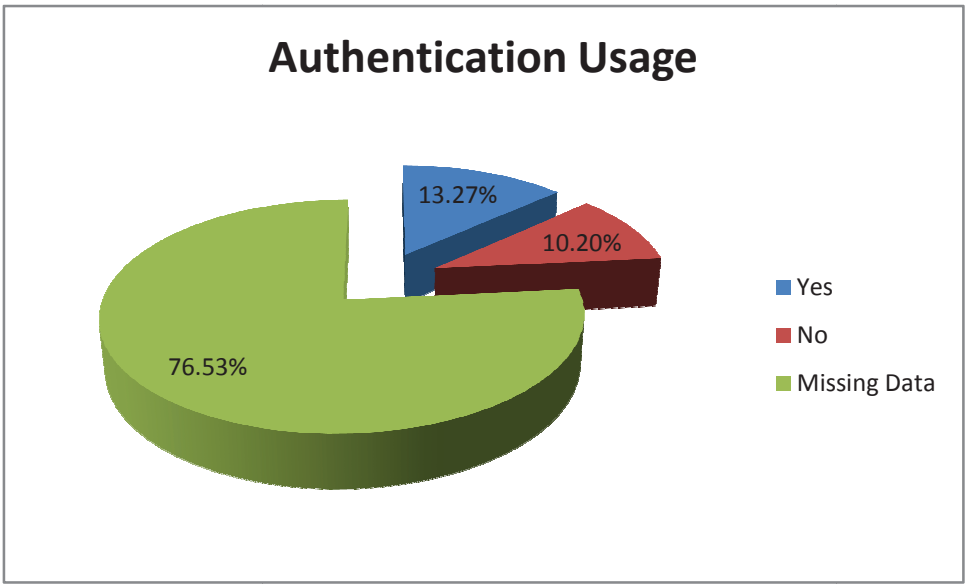

Figure 4.5: Authentication Usages of Students

4.3 Inferential Statistics

This study seeks to infer the results of this study to all universities in Zimbabwe. In order to do this the study applied regression analysis, correlation analysis and model diagnostics.

These were applied to the three distinct groups that were designed for the survey which was conducted and the results from these groups compared.

4.3.1 Regression and Correlation Analysis (Non-Technical Staff and Students)

The first correlation and regression results to be presented pertain to the Non-Technical group and Students group respectively. The analysis had dependent variable as Intensity of Use and three other variables, Age, Threats Awareness and Authentication Awareness being the independent variables. In this analysis, three key outputs will be discussed for these groups, that is, correlations, regression model summary, regression model coefficients and the ANOVA outcome.

Table 4.6: Correlations for the Non-Technical Staff group

		Intensity of Use	Age	Threats Awareness	Authentication Awareness
Pearson Correlation	Intensity of Use	1.000	-.242	.019	-.169
	Age	-.242	1.000	.225	.062
	Threats Awareness	.019	.225	1.000	.401
	Authentication Awareness	-.169	.062	.401	1.000
Sig. (1-tailed)	Intensity of Use	.	.006	.424	.040
	Age	.006	.	.010	.263
	Threats Awareness	.424	.010	.	.000
	Authentication Awareness	.040	.263	.000	.
N	Intensity of Use	348	348	348	348
	Age	348	348	348	348
	Threats Awareness	348	348	348	348
	Authentication Awareness	348	348	348	348

Table 4.6 shows the results of the correlations for the four variables given above with respect to the Non-Technical Staff group. Age variable has a negative weak Pearson Correlation of 0.242 with Intensity of use which implies they are moving in the opposite direction. This is because intensified use is basically clustered in the age groups 20-29 and 30-40. This weak

correlation is the general phenomenon with the other two independent variables though positive which implies there is a positive relationship between the variables although not strong. Threats Awareness and Authentication awareness have a positive significant Pearson correlation of 0.401. This is as a result of the fact that heavy users tend to be aware of both cyber security risks and authentication mechanisms. However, Threats Awareness and Authentication awareness have weak Pearson correlations of 0.019 and -0.169 respectively with intensity of use implying very weak positive relationship and weak negative relationship respectively.

For this Regression Model, the Regression Model Summary for the Non-Technical group, i.e. Table 4.7, shows that at 5% significance level the model is significant given by 0.90% and low variability given by R Square value of 10.50%. The low variation is accepted because the study involved interaction with human beings which are very difficult to predict their behaviour as compared to physical processes.

Table 4.7: Regression Model Summary for the Non-Technical Staff group

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.324[a]	.105	.079	2.479	.105	13.426	3	344	.009

a. Predictors: (Constant), Authentication Awareness, Age, Threats Awareness

The model for the Non-Technical group has the coefficients given in Table 4.8. The coefficients are significant except for Threats Awareness with a value of 11.20% which is above the benchmark of 5% implying insignificant contribution to the model. This may be as result of information and maturity of the Non-Technical Staff. In this regard, the regression model mathematically is as follows:

Intensity of Use = 9.200 + (-0.687) Age + 0.977 Threats Awareness + (-1.215) Authentication Awareness.

This simplifies to:

Intensity of Use = 9.200 – 0.687 Age + 0.977 Threats Awareness – 1.215Authentication Awareness.

Given that Age is β_1; Threats Awareness is β_2 and Authentication Awareness is β_3. The equation for the model will become:

$$Intensity\ of\ Use = 9.200 - 0.687\hat{\beta}_1 - 1.215\hat{\beta}_3$$

Table 4.8: Coefficients for the Non-Technical Group

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	9.200	1.156		7.956	.000	6.907	11.493
	Age	-.687	.246	-.266	-2.796	.006	-1.174	-.200
	Threats Awareness	.977	.609	.167	1.605	.112	-.230	2.185
	Authentication Awareness	-1.215	.561	-.220	-2.166	.033	-2.327	-.103

a. Dependent Variable: Intensity of Use

Table 4.9: ANOVA for the Non-Technical Staff

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	74.800	3	24.933	13.426	.009[a]
	Residual	638.941	344	1.857		
	Total	713.741	347			

a. Predictors: (Constant), Authentication Awareness, Age, Threats Awareness

b. Dependent Variable: Intensity of Use

Table 4.9 shows the results of Analysis of Variance (ANOVA) for Non-Technical Staff group. This study was set at 5% significance level and ANOVA produced a value of 0.90% which signifies that the model was significant for this study since it is less than 5%. The ANOVA outcome for this group will be compared with the outcome of the Students group since the model applied is the same. Therefore, we reject the null hypothesis.

Table 4.10: Correlations for the Students Group

		Intensity of Use	Age	Threats Aware	Authentication Awareness
Pearson Correlation	Intensity of Use	1.000	-.010	-.170	.186
	Age	-.010	1.000	-.164	-.174
	Threats Awareness	-.170	-.164	1.000	.340
	Authentication Awareness	.186	-.174	.340	1.000
Sig. (1-tailed)	Intensity of Use	.	.462	.047	.033
	Age	.462	.	.053	.043
	Threats Awareness	.047	.053	.	.000
	Authentication Awareness	.033	.043	.000	.
N	Intensity of Use	825	825	825	825
	Age	825	825	825	825
	Threats Awareness	825	825	825	825
	Authentication Awareness	825	825	825	825

Table 4.10 shows Pearson correlation results of afore mentioned variables for the students group. The variables Age and Threats Awareness have very weak negative relationship and weak relationship of 0.010 and 0.170 respectively with intensity of use. These two variables are moving in the opposite direction with intensity of use. This is due to very same fact that intensified use with respect to age is clustered with the age groups 20-29 with 58.37% and these are the youths. Threats awareness and Authentication Awareness have a slightly strong positive relationship of 0.340 which implies movement in the same direction. But when we compare the two with age they have weak negative relationships of 0.164 and 0.174 respectively which entails that they move in the opposite direction with Age. Last but not least, Authentication Awareness has a weak positive relationship with intensity of use.

The regression analysis had also Regression Model summary as another crucial outcome which is shown in Table 4.11. Of importance are Significance Change and R Squared values. At significance level of 5% the value of 2.20% for Significance Change affirms that the model is significant for this study. But, when at R Squared which measures the variation explained by the Regression Model the ideal is a higher variation of over 50%. In this case it

is 9.7% which is acceptable as this study involved interaction with human beings which are very difficult to predict their behaviour as compared to physical processes.

Table 4.11: Regression Model Summary for the Students Group

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.311[a]	.097	.068	2.206	.097	29.269	3	821	.022

a. Predictors: (Constant), Authentication Awareness, Age, Threats Aware

Therefore, the coefficients for this study with respect to the Students group are given in Table 4.12 with all variables except one (i.e. Age) which can be dropped as its contribution to the model is not significant because of its value of significance of 9.57% which is greater than the benchmark for this study of 5%. This is the same trend that was witnessed with the Non-Technical Staff group as explained in previous sections. So, mathematically the model for this study can be represented as follows:

Intensity of Use = 3.586 + (-0.033) Age + (-1.334) Threats Awareness + 1.502 Authentication Awareness.

This simplifies to:

Intensity of Use = 3.586 – 0.033 Age – 1.334 Threats Awareness + 1.502 Authentication Awareness.

Given that Age is β_1; Threats Awareness is β_2 and Authentication Awareness is β_3. The equation for the model will become:

$$Intensity\ of\ Use = 3.586 - 0.033\hat{\beta}_1 + 1.334\hat{\beta}_2 + 1.502\hat{\beta}_3$$

Table 4.12: Coefficients for the Students Group

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	3.586	1.790		2.003	.048	.031	7.141
	Age	-.033	.611	-.005	-.054	.957	-1.246	1.179
	Threats Awareness	-1.334	.528	-.265	-2.526	.013	-2.382	-.285
	Authentication Awareness	1.502	.573	.276	2.622	.010	.365	2.639

a. Dependent Variable: Intensity of Use

The ANOVA for the Students group produced a value of 2.20% at the same significance level for the Non-Technical Staff group of 5% which affirms that the regression model is significant for both groups and this strongly supports the rejection of the null hypothesis. This is shown in Table 4.13.

Table 4.13: ANOVA for the Students Group

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	48.909	3	16.303	29.269	.022
	Residual	457.499	821	0.557		
	Total	506.408	824			

a. Predictors: (Constant), Authentication Awareness, Age, Threats Awareness

b. Dependent Variable: Intensity of Use

4.3.2 Regression and Correlation Analysis (Technical Staff)

The analysis of the Technical group was based on sample value of 3 since the university has 4 technical people dealing directly with the data network hence the inability of the researcher to expand the sample. This entails lack of diversity in the responses of the participants. The development of the Regression model for this group involved having Threats Detection as the dependent variable and 5 other variables as independent. The independent variables are Protection Confidence, Financial Resources, Prioritisation, Diversity and Complexity and

Limited Skills. The first outputs to be discussed are the Pearson correlation associated with these variables which are shown in Table 4.14. The variable Protection Confidence has a perfect positive relationship with Financial Resources reflected by a Pearson correlation value of 1.00 and negative relationships with Threats Detection, Prioritisation, Diversity and Complexity and Limited Skills reflected by negative Pearson correlation values of 0.500, 0.756, 0.500 and 0.500 respectively. These negative values of correlations are the same with respect to Financial Resources as it is perfectly related to Protection Confidence. The perfect relationship entails that these two variables (Protection Confidence and Financial Resources) are moving together in the same direction. In essence, lack of Prioritisation and lack of Financial Resources results in greater cyber security challenges for the University of Zimbabwe.

Prioritisation variable has a strong positive almost perfect relationship with Threats Detection of 0.945 and very strong negative relationship of 0.756 with both Protection Confidence and Financial Resources. With the other two, Limited Skills and Diversity and Complexity Prioritisation have a very weak negative relationship of 0.500. The near perfect relationship between Prioritisation and Threats Detection entails that these two variables are moving in the same direction. This entails that lack of prioritisation may result in an increase in the threats detection frequency.

Furthermore, Diversity and Complexity have a perfect positive relationship with Limited skills reflected by a Pearson correlation value of 1.00. This entails that the more diverse and complex the social technologies become, the more technical people are limited in skills since diversity and complexity are linked to the rapid development of technology. Since these two are perfectly related, they will have the same Pearson correlation values of -0.500 with Threat Detection, Protection Confidence and Financial Resources but with Prioritisation have a very weak negative relationship given by a Pearson correlation value of 0.189.

Table 4.14: Correlations for the Technical Group

		Threats Detection	Protection Confidence	Financial Resources	Prioritisation	Diversity and Complexity	Limited skills
Pearson Correlation	Threats Detection	1.000	-.500	-.500	.945	-.500	-.500
	Protection Confidence	-.500	1.000	1.000	-.756	-.500	-.500
	Financial Resources	-.500	1.000	1.000	-.756	-.500	-.500
	Prioritisation	.945	-.756	-.756	1.000	-.189	-.189
	Diversity and Complexity	-.500	-.500	-.500	-.189	1.000	1.000
	Limited skills	-.500	-.500	-.500	-.189	1.000	1.000
Sig. (1-tailed)	Threats Detection	.	.333	.333	.106	.333	.333
	Protection Confidence	.333	.	.000	.227	.333	.333
	Financial Resources	.333	.000	.	.227	.333	.333
	Prioritisation	.106	.227	.227	.	.439	.439
	Diversity and Complexity	.333	.333	.333	.439	.	.000
	Limited skills	.333	.333	.333	.439	.000	.
N	Threats Detection	3	3	3	3	3	3
	Protection Confidence	3	3	3	3	3	3
	Financial Resources	3	3	3	3	3	3
	Prioritisation	3	3	3	3	3	3
	Diversity and Complexity	3	3	3	3	3	3
	Limited skills	3	3	3	3	3	3

The model summary given in Table 4.15 shows two independent variables are significant for the model (Limited Skills and Prioritisation) while the rest have been dropped. The significance level is 0% which is less than the benchmark for the study hence setting the basis for the rejection of the null hypothesis. This level of significance coupled with R Square value of 100% advocates that the model is perfect since it has no error.

Table 4.15 Model Summary for the Technical Group

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	1.000[a]	1.000	.	.	1.000	.	2	0	.

a. Predictors: (Constant), Limited skills, Prioritisation

b. Dependent Variable: Threats Detection

Therefore, the regression model for the Technical group has coefficients for Prioritisation and Limited Skills only being significant. These are shown in Table 4.16 with a significance level of 0%. Mathematically this model will be as follows:

$$\text{Threats Detection} = 0.500 + 0.333(\text{Prioritisation}) + (-0.167)\ (\text{Limited Skills})$$

Given that Prioritisation is α_1 and Limited Skills is α_2 the model will be represented as follows:

$$Threats\ Detection = 0.500 + 0.333\hat{\alpha}_1 - 0.167\ \hat{\alpha}_2$$

Table 4.16 Coefficients for the Technical Group

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	.500	.000		.	.	.500	.500
	Prioritisation	.333	.000	.882	.	.	.333	.333
	Limited skills	-.167	.000	-.333	.	.	-.167	-.167

a. Dependent Variable: Threats Detection

NB: These are spurious results due to inadequate number of items for statistical analysis (which are two in this case) so the sig value is very small and SPSS represents it as a missing value

However, when it comes to the ANOVA outcome, as shown in Table 4.17, the significance level is zero and hence the model can be said to be significant for this study. But when we look at the degrees of freedom where from this sample of 3 elements were applied in the computation, there is the subject of lack of diversity as well as the suggestion of collusion on part of the respondents since the questionnaires analysed were responded to by individuals who work together in the same department and are governed by the same organisational code of secrecy hence the likelihood of collusion.

Table 4.17 ANOVA for the Technical Group

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.667	2	.333	.	.[a]
	Residual	.000	0	.		
	Total	.667	2			

a. Predictors: (Constant), Limited skills, Prioritisation

b. Dependent Variable: Threats Detection

Reliability of Regression and Correlation Results for Technical Group

In order to validate the results of the ANOVA for the Technical group, Cronbach's Alpha and Friedman's tests had to be conducted so as to determine what led to the dropping of the other variables. Table 4.18 shows that the Cronbach' s Alpha is -0.750 and suggests the violation of model assumptions but when we look at the Friedma's test results with respect to Kendall's coefficient we find that it is a midpoint value of 0.517 suggesting no collusion as predicted earlier advocating for the current status quo which led to the agreement in the responses.

Table 4.18: Reliability Statistics

Cronbach's Alpha[a]	Cronbach's Alpha Based on Standardized Items[a]	N of Items
-.750	-2.235	13

a. The value is negative due to a negative average covariance among items. This violates reliability model assumptions. You may want to check item codings.

Table 4.19: ANOVA with Friedman's Test

		Sum of Squares	df	Mean Square	Friedman's Chi-Square	Sig
Between People		.667	2	.333		
Within People	Between Items	15.692[a]	12	1.308	19.026	.088
	Residual	14.000	24	.583		
	Total	29.692	36	.825		
Total		30.359	38	.799		

Grand Mean = 1.79

a. Kendall's coefficient of concordance W = .517.

4.4 Closing Remarks

The focus of this chapter was to present the key findings of the study. These findings stem from the analysis that was carried out on the data which was collected from the participants. The findings were presented in two main categories which are descriptive statistics and inferential statistics. Inferential statistics were applied separately to each of the three groups from which data was collected and a model developed for each group. In the next chapter, the focus will be to give conclusions and recommendations of this study in line with the key findings presented in this chapter. This will also include validation of the hypothesis stated in chapter 1 as well as proposing areas of further study.

CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter will present the conclusions and recommendations that were drawn in line with the key findings of this study. Topics that are covered include conclusions, validation of the hypothesis, recommendations and areas of further study. At the end of the chapter, closing remarks are given to conclude the dissertation.

5.2 Conclusions

During this investigation, data was collected from three groups which comprised of 825 students, 248 non-technical staff and 3 technical staff participants. The gist of the exercise was to determine the level of usage of the social technologies through campus Internet service and how this usage contributes to the cyber security challenges at the University of Zimbabwe.

Base on the results obtained, the following conclusions can be drawn:

1. There is an increased use of social technologies on the University of Zimbabwe data network and this has resulted in an increase in the challenges associated with cyber security.

2. The increase in these challenges can be attributed to the contribution of several key factors which include, financial resources, technical skills, cyber security perceptions of users, diversity and complexity of social technologies at play, the level of cyber security awareness amongst the university community social technology users, resource prioritisation and the threat detection frequency.

3. There is a positive correlation between the use of authentication mechanisms and the intensity of use of social technologies on campus. In simple terms, the study concluded that in this intensified use of social technologies, the majority of the social

technologies accounts of the users are not fully secure as most of them are using default security settings. This has resulted in an increase in the cyber security risk for the University of Zimbabwe.

4. Furthermore, it was concluded that being aware of security threats and security as arrogance has been observed in the results of the survey. This phenomenon coupled with the cyber security perceptions of users helped to solidify the conclusion that cyber security is considered by the majority of the users to be the role played by the technical people.

5. Lastly, it was concluded that the majority of the users are in the 25 to 35 age range. This confirms that the heavy users of social technologies are youths.

5.3 Validation of Hypothesis

This research study was based on the following hypothesis:

H0: The increased usage of social technologies did not result in increased cyber security challenges at the University of Zimbabwe.

H1: The increased usage of social technologies resulted in increased cyber security challenges at the University of Zimbabwe.

This study rejects the null hypothesis and accepts the alternate hypothesis. The rejection of the null hypothesis is based on the discovery that there exists an increase in the usage of social technologies at the University of Zimbabwe which are accessed through the campus data network. This has led to an escalation of security threats detection frequency and an increase in the traffic on the campus data network. These and other key factors which include limited financial resources, prioritisation and limited skills have resulted in the institution facing increased cyber security challenges mainly because of its inability to match runaway technological development.

5.4 Recommendations

It is hereby recommended that during the induction of employees and orientation of students, the university should include cyber security related activities which address the use of social technologies rather than just accessing campus digital resources. This ensures that the users that are being introduced to the data network are well versed with the issues of security and this helps in involving users so that they play their part in properly securing their social technology accounts and hence contribute to the reduction in the cyber security risk of the University of Zimbabwe.

In addition, it is also recommended that the university should also make it a routine to frequently hold symposia, seminars and public lectures on this topical issue of cyber security. This enables non technical staff, students and the members of the community to be educated on the issues of cyber security. It also helps in changing the perception of users so that they appreciate that cyber security requires collective action rather than just perceiving it to be an ICT technical role. This effort will not only see the reduction in the cyber security risk for the University of Zimbabwe but is also an effort that will help in controlling this scourge in the Zimbabwean context.

It is also important for the university executives as well as ICT practitioners to prioritise their efforts towards the combating of cybercrimes. These efforts include acquisition of state of the art equipment for defending unauthorised access as well as ensuring that the technical people are constantly trained in line with the rapid development in technology and cyber threats. This will ensure the bridging of the gap between development in technology and ICT expertise and advances in cybercrime sophistication.

However, for further study, the researcher recommends a different research design type. The recommendation is that of triangulation research design. This recommendation stems from the observation that the number key technical people who deal with cyber security issues in the institution was very small, 4 to be precise. With this sample of 4, the study got 3

responses and this small number has limited statistical computation that can provide rich information as it lacks diversity. So, in order to address this issue, the use of qualitative data collection and analysis techniques are deemed appropriate for the group in question and quantitative data collection and analysis techniques restricted to the social technology user groups entailing triangulation.

Furthermore, the study recommends the use of two or more cases in the Zimbabwean context for the study. This ensures more reliability and the ability to infer the results to the wider Zimbabwean context. In addition, the usage of more cases will also ensure that there is diversity in the responses which entail diversified statistical computations that can be applied to the data.

5.5 Limitations and Areas of Further Study

The researcher encountered challenges in trying to analyse data collected from the Technical Staff group due to its small size and the recommendations have been highlighted in the previous section. It is vital to note that the study did not explore on the causes of the various perceptions on cyber security that were exhibited by the social technology users. This is an area of further study in which the relationship between user perceptions on cyber security and cyber security challenges can be investigated.

In addition, quality assurance is a crucial pillar of tertiary institutions. In this regard, it is also important to explore the net impact of the escalade usage of social technologies which has resulted in an increase in cyber security challenges on the quality standards of the universities in Zimbabwe.

5.6 Closing Remarks

In summary, this chapter gave an introduction in which this chapter's discussion was projected in brief. Furthermore, conclusions and recommendations were laid down in line with the findings discussed in chapter 4. Last but not least, the hypothesis stated in chapter 1 was validated and areas of further study proposed.

REFERENCES

Ajao, K. R. (2008). *Investigation of Valves Uses and Inflows-liness in Nigeria National Petroleum Company Depot.* University of Ilorin, Department of Mechanical Engineering. Ilorin: Oke-Oyi.

Akogwu, S. (2012). *An Assessment of the Level of Awareness on Cyber Security Crime Among Internet Users in Ballo University.* Ahmadu Bello University, Department of Sociology. Zaria: Ahmadu Bello University.

Akuta, E., Ong'oa, I., & Jones, C. (2011). Combating Cyber Crime in Sub-Saharian Africa: A Discourse on Law, Policy and Practice. *Journal of Peace, Gender and Development Studies , 1* (4), 129-137.

Apau, N. E. (2011). *Best Practices on Social Networking Sites.* Cyber Security Malaysia. Cyber Security Malaysia.

Aunger, R. (2010). Types of Technology. *Technological Forecasting and Social Change , 77* (5), 762-78.

Belk, R., & Noyes, M. (2012). *On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy.* Havard Kenedy School, US Department of Defense. Havard Kenedy School.

Berg, J., Berquam, L., & Christopher, K. (2007). Social Networking Technologies: A Poke for Campus Services. *Educause Review* .

Booth, W. C., Colomb, C. G., & Williams, J. M. (2008). The Craft of Research. Chicago: University of Chicago Press.

Bughin, J., Beyer, A. H., & Chui, M. (2011). How Social Technologies are Extending the Organisation. *Mckensey Quarterly* .

Burns, S. N., & Grove, S. K. (2003). *Understanding Nursing Research* (3 ed.). Philadelphia: Saunders.

Calverty, M. D. *Cyber Security and Threat Politics: US Effort to Secure the Information Age.* London: Routledge.

Chi, M. (2011). *Security Policy and Social Media Use.* SANS Institute, GIAC (GSEC) Certification. InforSec Reading Room.

Chitauro, G. (2015, February 4). *Cyber Laws Vital for Zimbabwe.* Retrieved February 6, 2015, from TechnoMag: http://www.technomag.co.zw

Cisco;. (2014). *Cisco Enterpride Mobility Solutions: Device Freedom Without Compromising the IT Network.* Cisco Systems.

Cole, K., Chetty, M., LaRosa, C., Schmitt, D. K., & Goodman, S. E. (2008). *Cyber Security in Africa: An Assessment.* Sam Nunn School of International Affairs. Atlanta: Georgia Institute of Technology.

Collis, J., & Hussey, R. (2009). *Business Research: A Practical Guide for Undergraduate and Postgraduate Students.* New York: Palgrave Macmillan.

Cooper, D. R., & Schindler, P. S. (2006). *Business Research Methods.* Boston: McGraw-Hill Irwin.

Crosswel, J. W. (2003). *Qualitative, Quantitative and Mixed Methods Approaches.* Califonia: Sage.

Deloitte (2014). *Cyber Security in Switzerland: Finding the Balance Bettween Hype and Complacency.* New York: Deloitte.

Derksen, M., Vikkelso, S., & Beaulieu, A. (2012). Social Technologies: Cross-Disciplinary Reflections on Technologies in and from the Social Sciences. *Theory and Psychology , 22* (2), 139-147.

Durrheim, K. (2002). *Research Design* (2 ed.). Cape Town: University of Cape Town Press.

Easterby-Smith, M., Thorpe, R., & Jackson, P. R. (2008). *Management Research* (3 ed.). London: Sage Publications.

Goverment of India. (2011). *Framework and Guidelines for Use of Social Media for Government Organisations.* Ministry of Communications and Technology, Department of Information Technology. Ministry of Communications and Technology.

Government of Zimbabwe. (2015, January 15). *Nigeria, Kenya, Zimbabwe, South Africa Account for 74% of Africa's Fraud Cases*. Retrieved February 11, 2015, from E-Government and Cyber Security Services: http://www.gisp.gov.zw

Graziano, A. M., & Raulin, M. I. (2004). *Rsearch Methods: A Process of Inquiry* (5 ed.). Boston: Pearson.

Hansen, L., & NissenBaum, H. (2009). Digital Disaster, Cyber Security and the CopenHagen School. *International Studies Quarterly , 53*, 1155-1175.

Henning, E., Van Ransburg, W., & Smit, B. (2004). Finding Your Way in Qualitative Research. Pretoria: Van Schaik.

Herselman, M., & Warren, M. (2004). Cyber Crime Influencing Businesses in South Africa. *Journal of Issues in Informing Sciences and Information Technology , 1*, 253-266.

Hungwe, K. N. (n.d.). Emergent Literacies: Raising Questions About the Place of Computer Technologies in Education and Society in Developing Country: The Case of Zimbabwe. *XXIX(ii)* . Zambezia.

Isaacs, S. (2007). *ICT in Education in Zimbabwe, Survey of ICT and Education in Africa: Zimbabwe Country Report.*

Janson, W. (2011). Understanding Cyber Crime in Ghana: A View from Below. *International Joournal of Cyber Criminology , 5* (1), 736-749.

Jason, P. (2010). Science of Cyber Security. *The Mitre Corporation* . Virginia: McLean.

Jones, K. (2007). Connecting Social Technologies with Information Literacy. *Journal of Web Librarianship , 1* (4), 67-80.

Kumar, R. (2003). Cyber Laws, International Property and E-Commerce Security. New Dehli: Dominant Publishers and Distributors.

Kumar, R. (2005). *Research Methodology - A Step-by-Step Guide for Beginners* (2 ed.). Singapore: Pearson Education.

London, S., & Stytz, M. R. (2005). Overview of Cyber Security: Crisis of Prioritisation. *IEEE Security and Privacy , 3* (3), 9-11.

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatiuschtschenko, E. (2013). Comprehensive Study on Cyber Crime. New York: United Nations Office on Drugs and Crime.

McConnell International. (2000). *Cyber Crime...And Punishment? Archnaic Laws Threaten Global Information.* McConnell International LLC.

Mhlanga, B. (2006). Information and Communication Technologies (ICTs) Policy for Change and the Mask for Development: A Critical Analysis of Zimbabwe's E-Readiness Survey Report. *Electronic Journal on Information Systems in Developing Countries , 28* (1), 1-16.

Microsoft Corporation. (2011). *Cyber Security: More than a Good Hesdline.* Microsoft Corporation.

Mouton, J. (2002). Understanding Social Research (3rd Impressions). Pretoria: Van Schaik.

Mutero, E. (2014, December 1). *Authenticating Electronic Record-Based Evidence in Zimbabwean Labour Disputes.* Retrieved December 27, 2014, from Nehanda Radio: http://www.nehandaradio.com

Mwenje, T. (2014, August 8). *Cyber Security Threats, Worrisome.* Retrieved December 20, 2014, from TechnoMag: http://www.technomag.co.zw

Ncube, X. (2014, August 27). *Laws on Cards to Curb Cyber Crime.* Retrieved September 5, 2014, from The Zimbabwe Mail: http://www.thezimmail.co.zw

Njanjamangezi, E. (2014, May 16). *90% of Zim Firms Exposed to Cyber Crime* . Retrieved September 5, 2014, from The Zimbabwe Mail: http://www.zimmail.co.zw

Nkatazo, L. (2009, December 11). *Zimbabwe Promises New Law on Cyber Crime*. Retrieved December 7, 2014, from New Zimmbabwe: http://www.newzimbabwe.com

Odumesi, J. O. (2006). *Combating the Menace of Cybercrime: The Nigerian Approach (Project).* University of Abuja, Department of Sociology, Abuja.

Okeshola, F. B., & Adeta, A. K. (2013). The Nature, Causes and Consequenses of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research , 3* (9).

Olayemi, O. J. (2014). A Socio-Technological Analysis of CyberCrime and Cyber Security in Nigeria. *International Journal of Sociology and Anthropology , 6* (3), 116-125.

ORF Cyber Monitor. (2013, December 5). Cybersecurity Focus at ITU Telecom World 2013. *1(5)* . Bangkok.

Parahoo, K. (2006). *Nursing Research: Principles, Processes and Issues* (2 ed.). Houndsmill: Palgrave Macmillan.

Polit, D. F., Beck, C. T., & Hungler, B. P. (2001). *Essentials of Nursing Research: Methods Appraisals and Utilisation* (5 ed.). Philadelphia: Lippincott.

Polit, D., & Beck, C. (2004). *Nursing Research: Principles and Methods* (7 ed.). Philadelphia: Lippincott, Williams and Wilkins.

PWC. (2011). Decoding Deals in the Global Cyber Security Industry. *Cyber Security M&A Review* .

PWC. (2014). *Information Security Breaches Survey: Technical Report.* Retrieved December 20, 2014, from PWC: http://www.pwc.com

Reitz, E. J., & Wing, E. S. (2008). Zooarchaeology. Cambridge: Cambridge University Press.

Robb, D. (2014, December 14). *Sony Hack: A Timeline.* Retrieved December 28, 2014, from Deadline: http://deadline.com

Simon, M. K. (2011). *Dissertation and Scholarly Research: Receipts for Success* (2011 ed.). Saetle: Dissertation Success.

Siphos. (2010). Security Threat Report. Siphos.

Skarzauskien, A., Pitrnait-Zilnie, B., Leichteirs, E., & Paunksnie, Z. (2014). Social Technologies for Developing Collective Inteligence in Networked Society. (C. I. 2014, Trans.)

Skarzauskiene, A., Tamosiunaite, R., & Zaleniene, I. (2013). Defining Social Technologies: Evaluation of Social Collaboration Tools and Technologies. *The Electronic Journal of Information Systems Evaluation , 6* (3), 232-241.

Streubert, H. J., & Rinaldi Carpernter, D. (2011). *Qualitative Research in Nursing: Advancing the Humanistic Imperative* (5th ed.). New York: Wolters, Kluwer, Lippincott, Williams and Wilkins.

Treem, J. W., & Leonardi, P. M. (2012). Social Media Use in Organisations: Exploring the Affordances of Visibility, Editability, Persistence and Association. *Communication Year Book , 36*, pp. 143-189.

Tsokota, T., Chipfumbu, T. C., Mativenga, M., & Mawango, T. I. (2013). ICT4D and the Challenges of Vandalism in Zimbabwe. *International Journal of Science and Technology , 2* (8).

Van Vuuren, D., & Maree, A. (2002). *Survey Methods in Market and Media Research. In M. Terrence Blanche and K Durrheim, Research in Practice.* Cape Town: University of Cape Town Press.

Vanheuangdy, V. *Security Threats of Web 2.0 and Social Networking Sites.* Research Report for ACC626 (Prepared for Proffessor Malick Dardina).

Waziri, F. (2009, March 1). Antigraft Campaign: The War, The Worries, The Punch. p. 1.

Zananwe, N., Rupere, T., & Kufandiribwa, O. (2013). Use of Social Networking Technologies in Higher Education in Zimbabwe: A Learner's Perspective. *International Journal of Computer and Information Technology , 2* (1).

Zimucha, T., Zanamwe, N., Chimwayi, K., Chakwizira, E., Mapungwana, P., & Maduku, T. (2012). An Evaluation of the Effectiveness of E-Banking Security Strategies in Zimbabwe: A Case Study of Zimbabwean Commercial Banks. *Journal of Internet Banking and Commerce , 12* (3).

APPENDICES

Appendix 1: Questionnaire Cover Letter

Dear Sir/Madam

RE: MBA Research Questionnaire

I am a University of Zimbabwe Graduate School of Management student pursing Master of Business Administration degree. I am carrying out research on the following topic:

Social Technologies and Cyber Security Challenges in Zimbabwean Universities: A Case of the University of Zimbabwe.

May you kindly please spare a few minutes of your time to give your opinions on this issue. Please note that your name is not required and this research is purely for academic purposes only and will be treated with the strictest confidentiality. The findings of this survey will not be used for any other purpose besides that intended for this research.

Your cooperation is essential for the results of the survey to be valid and reliable.

Yours Faithfully

Farai Francisco Madyira

Appendix 2: Technical Staff Questionnaire

University of Zimbabwe

Graduate School of Management

Research Topic:

Social Technologies and Cyber Security Challenges in Zimbabwean Universities: A Case of the University of Zimbabwe.

Section A (Background Information)

NB: There is no right or wrong answer so feel free to answer in a way that expresses your most objective opinion in each case.

1. Specify your gender

   Male [ ] Female [ ]

2. Specify your age category

   Under 20 [ ] 20 – 29 [ ]

   30 – 39 [ ] 40 – 49 [ ]

   50 – 59 [ ] above 60 [ ]

3. Which department do you belong to?

   IT Computer Centre [ ]

   IT Main Administration [ ]

   IT Library [ ]

Section B (Social Technologies and Cyber Security)

4. Given the current development of social technologies, do you perceive a change in the traffic on the University of Zimbabwe data network?

Increase	[ ]	Same	[ ]
Decrease	[ ]	Don't Know	[ ]

5. The use of social technologies on the campus data network increases the cyber security risk of the University of Zimbabwe.

Strongly Agree	[ ]	Agree	[ ]
Neither Agree/Disagree	[ ]	Disagree	[ ]
Strongly Disagree	[ ]		

6. From the time social technologies have been introduced on your data network, what can you say about the threats detection frequency?

Increase	[ ]	Same	[ ]
Decrease	[ ]	Don't Know	[ ]

7. As a result of social technologies usage on your campus network, what can you say about the cyber security risk of the University of Zimbabwe?

Increase	[ ]	Same	[ ]
Decrease	[ ]	Don't Know	[ ]

8. Has the increased use of Social Networks resulted in your paying more attention to the Cyber Security threats they might cause.

Yes	[ ]	No	[ ]

9. What is your level of confidence that University of Zimbabwe data network is fully protected from cyber security risk?

We are very secure	[ ]	We are good	[ ]
We are ok	[ ]	We have problems	[ ]
We are not secure	[ ]	Don't know	[ ]

10. How informed are your users of social technologies on campus with regards cyber security threats

Well informed [ ] Relatively informed [ ]

Not well informed [ ] Not informed [ ]

11. Can you rate how informed are your executive leaders of University of Zimbabwe on the current level and business impact of cyber security risk to your organisation.

Well informed [ ] Relatively informed [ ]

Not well informed [ ] Not informed [ ]

12. Limited financial resources are a limiting factor to proper implementation of cyber security for the University of Zimbabwe.

Strongly Agree [ ] Agree [ ]

Neither Agree/Disagree [ ] Disagree [ ]

Strongly Disagree [ ]

13. Lack of prioritisation is a limiting factor to proper cyber security for the University of Zimbabwe.

Strongly Agree [ ] Agree [ ]

Neither Agree/Disagree [ ] Disagree [ ]

Strongly Disagree [ ]

14. Diversity and complexity of social technologies being used on campus data network are limiting factors to proper cyber security for the University of Zimbabwe.

Strongly Agree [ ] Agree [ ]

Neither Agree/Disagree [ ] Disagree [ ]

Strongly Disagree [ ]

15. Limited skills are a limiting factor to proper cyber security for the University of Zimbabwe.

Strongly Agree	[ ]	Agree	[ ]
Neither Agree/Disagree	[ ]	Disagree	[ ]
Strongly Disagree	[ ]		

Appendix 3: Non-Technical Staff Questionnaire

University of Zimbabwe

Graduate School of Management

Research Topic:

Social Technologies and Cyber Security Challenges in Zimbabwean Universities: A Case of the University of Zimbabwe.

Section A (Background Information)

NB: There is no right or wrong answer so feel free to answer in a way that expresses your most objective opinion in each case. Please use a tick to select the appropriate answer where applicable.

16. Specify your gender

Male	[ ]	Female	[ ]

17. Specify your age category

Under 20	[ ]	20 – 29	[ ]
30 – 39	[ ]	40 – 49	[ ]
50 – 59	[ ]	above 60	[ ]

18. Which faculty do you belong to?

NB: *Administration include all non faculty sections of the university such as Computer centre, Main Library and student affairs.*

Agriculture	[ ]	Arts	[ ]
Commerce	[ ]	Education	[ ]
Engineering	[ ]	Law	[ ]

Medicine	[ ]	Science	[ ]
Social Studies	[ ]	Veterinary	[ ]
Administration	[ ]		

Section B (Social Technologies and Cyber Security)

19. Which social technologies do you use (eg Facebook, Twitter, Whatsapp, etc)

.....

.....

.....

.....

.....

.....

.....

.....

.....

20. How do you access these technologies when you are on campus?

Through campus Internet service	[ ]
Through other telecommunications service providers	[ ]
Both	[ ]

21. On a sliding scale of 1 to 10 how can you rate your usage of social technologies that you access through campus internet service (with 1 being the weakest usage and 10 being intensified usage)

1	[ ]	2	[ ]
3	[ ]	4	[ ]
5	[ ]	6	[ ]
7	[ ]	8	[ ]
9	[ ]	10	[ ]

22. What do you use social technologies for when you are on campus?

Business [ ] Socialisation [ ]

Both [ ]

23. Are you aware of social technologies security threats?

Yes [ ] No [ ]

a. If Yes, has your awareness of the cyber security threats led in your

Improving the security on the applications you use [ ]

Your reduced use of the social network [ ]

Both [ ]

b. If yes, how do you rate your knowledge of these threats?

Well informed [ ] Relatively informed [ ]

Not well informed [ ] Not informed [ ]

24. Are you aware of the two factor authentication security mechanism?

Yes [ ] No [ ]

a. If Yes, are you using it as security mechanism on your social technologies accounts?

Yes [ ] No [ ]

25. Do you consider cyber security threats on social technologies to be something that :-

You leave to the technical persons to worry about [ ]

You are aware of and actively take care of [ ]

You are aware of and do not take active care to address [ ]

You are not aware of but which bothers you [ ]

You are not aware of and do not bother you at all. [ ]

Appendix 4: Students Questionnaire

University of Zimbabwe

Graduate School of Management

Research Topic:

Social Technologies and Cyber Security Challenges in Zimbabwean Universities: A Case of the University of Zimbabwe.

Section A (Background Information)

NB: There is no right or wrong answer so feel free to answer in a way that expresses your most objective opinion in each case. Please use a tick to select the appropriate answer where applicable.

26. Specify your gender

Male	[ ]	Female	[ ]

27. Specify your age category

Under 20	[ ]	20 – 29	[ ]
30 – 39	[ ]	40 – 49	[ ]
50 – 59	[ ]	above 60	[ ]

28. Which faculty do you belong to?

Agriculture	[ ]	Arts	[ ]
Commerce	[ ]	Education	[ ]

Engineering	[ ]	Law	[ ]
Medicine	[ ]	Science	[ ]
Social Studies	[ ]	Veterinary	[ ]

29. Which year of study are you in?

1st	[ ]	2nd	[ ]	3rd	[ ]
4th	[ ]	5th	[ ]	6th	[ ]
7th	[ ]				

Section B (Social Technologies and Cyber Security)

30. Which social technologies do you use (eg Facebook, Twitter, Whatsapp, etc)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

31. How do you access these technologies when you are on campus?

Through campus Internet service	[ ]
Through other telecommunications service providers	[ ]
Both	[ ]

32. On a sliding scale of 1 to 10 how can you rate your usage of social technologies that you access through campus internet service (with 1 being the weakest usage and 10 being intensified usage)?

1	[ ]	2	[ ]

3	[ ]	4	[ ]
5	[ ]	6	[ ]
7	[ ]	8	[ ]
9	[ ]	10	[ ]

33. What do you use social technologies for when you are on campus?

School	[ ]	Socialisation	[ ]
Both	[ ]		

34. Are you aware of social technologies security threats?

Yes [ ] No [ ]

a. If Yes, has your awareness of the cyber security threats led in your

Improving the security on the applications you use [ ]

Your reduced use of the social network [ ]

Both [ ]

b. If yes, how do you rate your knowledge of these threats?

Well informed	[ ]	Relatively informed	[ ]
Not well informed	[ ]	Not informed	[ ]

35. Are you aware of the two factor authentication security mechanism?

Yes [ ] No [ ]

a. If yes, are you using it as security mechanism on your social technologies accounts?

Yes [ ] No [ ]

36. Do you consider cyber security threats on social technologies to be something that:-

You leave to the technical persons to worry about [ ]

You are aware of and actively take care of [ ]

You are aware of and do not take active care to address [ ]

You are not aware of but which bothers you [ ]

You are not aware of and do not bother you at all. [ ]