British Journal of Multidisciplinary and Advanced Studies:
Engineering and Technology, 3(2),77-104, 2022
Print ISSN: 2517-276X
Online ISSN: 2517-2778
https://bjmas.org/index.php/bjmas/index
Published by the European Centre for Research Training and Development UK

Cybersecurity Challenges and Needs in The Context of Digital Development in Zimbabwe

Tinashe Chingoriwo
Faculty of Technology
Zimbabwe Open University
Corner House, Samora Machel Avenue/
L.Takawira Street Harare, Zimbabwe.
Email: chingoriwot89@gmail.com

DOI: https://doi.org/10.37745/bjmas.2022.0046 Published: 29th November, 2022

Citation: Chingoriwo T. (2022) Cybersecurity Challenges and Needs in The Context of Digital Development in Zimbabwe, *British Journal of Multidisciplinary and Advanced Studies*: Engineering and Technology, 3(2),77-104,

ABSTRACT: *This research was on the cybersecurity challenges and needs of grassroot users of cyberspace in Zimbabwe. A qualitative research methodology was used and was guided by the Interpretivist philosophy. Judgmental sampling was used to select the participants in the study based on their knowledge on cybersecurity matters. The sample was drawn from people from Murewa District of Zimbabwe. A descriptive research design was used to answer the research questions. Both unstructured and structured interviews as well as observations were used to collect data on the cybersecurity needs and challenges of grassroot users of cyberspace. The findings revealed that the challenges that grassroot users are facing include identity theft, poor internet connectivity and infrastructure problems. The research also exposed the need for stronger physical security of ICT assets and cybersecurity legislation. The researcher recommended the use of solar systems as an alternative source of energy and continuous review and alignment of cybersecurity legislation in line with the changing cyber threat landscape.*

KEYWORDS: cybersecurity, challenges, needs, digital. development, Zimbabwe

INTRODUCTION

The exponential growth in the internet over the past decades has brought about numerous benefits to societies (Chertoff, 2008). Consequently, dependence of individuals and organizations on information and communication technologies (ICTs) has also increased. However, threats and vulnerabilities are also part and parcel of the internet that tend to compromise its safety.

Cybersecurity has become an important topic for various organizations across various industries. Cybersecurity is defined as the protection of interests of a person, society or nation, including their information and non-information assets that need protection from the risks that arise from their interaction with cyberspace (van Niekerk and Reid, 2014). The value of information in the form of government, business and personal data warrants the need for an

effective cyber security culture. As such, the security of networks and protection of data from cyber threats has become more imperative than ever, as cyberattacks are on the rise.

Cyber-attacks are threatening every industry that deals with vital data globally. The academic industry, banking industry, airlines as well as governments amongst many others have also been victims of cyber-attacks. Key examples of cyber victims in this regard include The College of Engineering in Pennsylvania State University, University of Maryland multiple Japanese Universities (Ernst and Young, 2016) as well as Makerere University. In Zimbabwe, the National University of Science and Technology and the Harare Institute of Technology also got attacked (Sibanda, 2020).The British Airways (Sillars, 2018), the Ministry of Finance of Uganda, Parliament of Zimbabwe (Sibanda,2020) as well as CBAO GAWB bank in Senegal also had a fair share of cyber-attacks (Africa Cyber Security Report, 2017). Moreover, according to CNBC (2020) other big companies have also been at the receiving end of cyber-attacks. Yahoo was hacked in 2013 and 2014, Friend finder networks in 2016, Marriot International in 2018, First American Financial Corp and Facebook in 2019.In all these instances, millions of records were affected.

In view of the continued increase of cyber-attacks and the subsequent growth of the cybercrime industry, several cyber security frameworks and guides have been crafted as part of key measures to help in the fight against cyber-attacks in some countries. These include the National Institute of Standards and Technology (NIST) Cybersecurity framework which is tailored for improving Critical Infrastructure Cybersecurity (NIST, 2018), the Italian Cybersecurity framework which targets the security of Small to Medium Enterprises in Italy (Italian Cybersecurity Report, 2015) and the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Cybersecurity Version 5 which targets the bulk power system. In the health sector, the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) (Sabillon et al, 2016) was put in place to cushion health systems against cyber-attacks whereas for Information Technology (IT) networks, the Council on Cybersecurity Critical Security Controls was made among many others. On the smart cities front, the NIST Smart Cities and Communities Framework (SCCF) was crafted. Its aim is to avail cities and communities with best practices and technical blueprints for the planning, development and implementation of smart solutions in a secure manner (NIST, 2020).

Similarly, in terms of provision of technical guidelines on cybersecurity, several guides have also been put in place. Some of these include the European Network of Information Security Agency (ENISA) Cyber Security Strategy guide (ENISA, 2019) and the International Telecommunications Union (ITU) Cyber Security guide (ITU, 2011).

Meanwhile, in Africa, legislative initiatives have been made with the idea of improving the continent's cybersecurity posture. According to a November 2016 report of the African Union Commission (AUC) as cited by Kshetri (2019), 11 countries in Africa had specific laws and provisions for dealing with cybercrime. These are, Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia. On the other hand, 12 countries had taken some legislative measures, although limited. It is worth noting that in some

countries, draft cybercrime laws had been prepared and bills presented to Parliaments (Kshetri, 2019).

In Zimbabwe legislative strides have been taken so far in a bid to combat cybersecurity breaches. This is evidenced by the Data protection Act that was put in place (Ministry of Information and Communication Technology, 2020).In addition, the legislative strides have also been supported by the establishment of other important cybersecurity institutions that include the IT Governance and Cyber Security Institute of Sub-Sahara.

The IT Governance and Cyber Security Institute of Sub-Sahara was launched in 2012 as a response to the need for cybersecurity .The reason behind was that of increasing the exchange of information, supporting research and reporting of cyber threats as well as holding episodic ICT security seminars (UNIDIR, 2013). However, despite all the initiatives that have been taken towards cybersecurity in Zimbabwe, it appears that a lot needs to be done in various sectors especially in rural areas with more emphasis on the poor and marginalised members of the society.

Statement of the problem

The absence of a technical blueprint to provide direction and a standard way of dealing with cybersecurity challenges in Zimbabwe is one of the key problems being faced across the ICT spectrum. Zimbabwe's grassroot users of the internet lack technical guidance and direction on how to prevent and respond to cyber-attacks. For this reason, their information and non-information assets are highly exposed to cyber risks.

Purpose of study

The purpose of this research is to unveil the cybersecurity needs and challenges of grassroot users of the Internet in order to develop a cybersecurity framework which ensures that they are secured from cyber threats.

Research objectives

The objectives of this research were to

a) Determine the cybersecurity challenges being faced by grassroot users of the Internet in Zimbabwe
b) Examine cybersecurity needs of grassroot users of the Internet in Zimbabwe

Research Questions

The research questions were:

a) What are the cybersecurity challenges being faced by grassroot users of the Internet in Zimbabwe?
b) What are the cybersecurity needs of grassroot users of the Internet in Zimbabwe?

REVIEW OF RELATED LITERATURE

Cybersecurity and Information Security

The terms cybersecurity and information security are frequently used interchangeably in most circles. This may be due to the fact that there is an overlap between these two, but however

they are different (Van Niekerk and Von Solms, 2013). According to Whitman and Mattord, (2009), International Organisation for Standardization /IEC 27002 (2005) and Fischer (2016), information security can be defined as the protection of information and information systems from illegal access, use, disclosure, disruption, modification, or destruction in order to ensure their confidentiality, integrity and availability.

On the other hand, cyber security goes beyond the margins of information security to embrace not only the protection of information and information assets, but also that of other resources, including the people (Van Niekerk and Von Solms, 2013). Cybersecurity can be defined as the protection of interests of a person, society or nation, including their information and non-information assets that need protection from the risks that emanate from their interaction with cyberspace (Van Niekerk and Reid, 2014).

Cybersecurity Risk
It is the possible exposure to loss or harm emanating from an organization's information or communications systems (Fischer, 2016). It goes beyond damage and destruction of data or financial loss and includes theft of intellectual property theft, productivity losses and reputational damage.

Cyber Threat
According to ISACA (2012), it refers to a new or newly discovered incident that has the potential to harm a system or your company. It can be a person or event that has the likelihood for impacting a treasured resource in an undesirable manner (Fischer, 2016). Authors point to the fact that a threat is any kind of danger, which can make damage to data or information systems and disrupt the normal operation of an organization or entity. Common examples of cyber threats include malware, phishing, data breaches and even rogue employees. Cybersecurity threats are actualized by threat actors who are either individuals or groups with various backgrounds, motivations and different intentions. As such, a good understanding of cyber threats is important in coming up with effective mitigations and helps to make the right choices in cybersecurity.

Vulnerabilities
These are known weaknesses of assets or resources that can be exploited by one or more attackers (ISACA, 2012). They make threat outcomes a success and possibly even more dangerous (Fischer, 2016). The authors agree on the idea that vulnerabilities are those qualities of resources or their environment that give room for the threat to be realized. Common vulnerabilities include server misconfigurations, sensitive data transmitted in plain text among many others.

Cyber attack
According to Checkpoint (2020), a cyber-attack is an assault launched by cybercriminals utilizing one or more computer devices against a single or multiple computer devices or networks. It can also be defined as any kind of offensive action that targets computer information systems, infrastructures, computer networks or personal computer devices, using numerous means to steal, modify or destroy data or information systems (ISACA, 2012). These

assaults can result in computers getting maliciously disabled data theft, or use a compromised computer device as a launch pad for further attacks. Several approaches to launch a cyber-attacks that include malware, phishing, ransomware, denial of service can be used by cybercriminals.

Information Communication Technology For Development (ICT4D)

The use of Information Communication Technologies for the purposes of developing people socially, economically, politically with particular thrust on helping the poor and the marginalized (Heeks, 2009). Information and Communications Technologies for Development (ICT4D) is the use of digital solutions to amplify the intent of communities to accelerate their social and economic development. Information and communication technologies (ICT) include hardware, software, content, and the design and implementation methodologies required for their successful adoption. ICT4D employs all technology interventions that can assist poor and marginalized people.

Theoretical Framework

A theoretical framework is a guide for a research that is used by a researcher to come up with his/her research inquiry and also serves as a foundation upon which research is built (Grant and Osanloo, 2014). It therefore guides the researcher so that s/he will not move away from the boundaries of the accepted theories in order to make his/her final contribution scholarly and academic (Imenda, 2014).The selection of a theoretical framework/s requires a thorough understanding of the problem, purpose, significance and research questions of the study (Adom and Joe, 2018).

In this research, the theory that guided this study is the National Institute of Standards and Technology (NIST) Cybersecurity Framework. According to the National Institute of Standards and Technology (2018), the NIST Cybersecurity framework was crafted with the aim of reducing cyber risk and improving security of critical infrastructure. It is composed of five core functions which are Identify, Protect, Detect, Respond and Recover as shown in Figure 1 below.

Figure 1: NIST Cybersecurity Framework Core components. Source: National Institute of Standards and Technology (2018)

These core functions are then further split into several tiers which detail practices that organizations can employ.

Cybersecurity challenges

This section outlines the challenges being faced in the cybersecurity realm by developing countries.

Infrastructure

Developing countries inject few resources into cybersecurity infrastructure (International Telecommunications Union, 2009) such that the digital divide will give birth to a cybersecurity divide. In Africa, there are low provisions of security and are inadequate to intercept risks associated with technology and information (United Nations Economic Commission for Africa Policy Brief, 2014).

Inadequate Legal frameworks

Lack of adequate legislation on cybercrime contributes to making developing countries attractive hiding spots for cyber criminals (Norwegian Institute of International Affairs, 2018) and without legislation internet access brings more harm than good (Muller,2015).Size and number of regulations to put within the legal framework is also a major challenge for developing countries (Muller, 2015) and in Africa, most countries are unable to craft the relevant cybersecurity legal frameworks to combat cybercrime (United Nations Economic Commission for Africa Policy Brief, 2014). On the other hand enactment of laws on cybersecurity hasn't been done by some developing countries (Tagert, 2010).

Lack of Harmonization of legislation

Cybercrime is transnational in nature as the perpetrator, victim, tools used to commit cybercrime and the scene may be in different countries. The harmonization of domestic legislation with international standards is still a challenge. Certain country-specific issues have to be addressed first in order to make legislation powerful and enforceable within a local context (Bande, 2018).

Challenges in balancing harmonization and country specific needs

According to the International Telecommunication Union (2012) as cited by Bande (2018), cybercrime legislation must be receptive to the needs and realities of the country as well as the region. Chan (2012) as cited by Bande (2018) refers to this as the 'glocal approach' where countries take initiatives at global level and strike a balance with local circumstances. Drawing a healthy balance between harmonization and country demands is still a problem.

Insecure Systems

Developing countries do not have robust security systems like in other parts of the world. This has inevitably made them attractive cyber targets. For instance, in May 2016, the national bank of Bangladesh was robbed as a result of a cyberattack. The same thing happened to banks in Ecuador, the Philippines and Vietnam in 2015 and 2016 .On the other hand, pirate copies of operating systems and older versions of operating systems are common in developing countries and makes them increasingly vulnerable to cyberattacks and cybercrime (Schia, 2018).

Lack of education and awareness

Developing countries are short of well-trained and competent ICT security experts both in private and public sectors (Tagert, 2010). In Africa, there is a huge cybersecurity technical skills gap that has exposed it to vulnerabilities such as cyberterrorism and cyberespionage (United Nations Economic Commission for Africa Policy Brief, 2014).The lack of training infrastructure also inhibits the dissemination of cybersecurity skills (2016 Cybersecurity report, 2016).

ICT security education and awareness are not in the academic curriculum unlike in developed countries (Schia, 2018).The public's understanding and awareness of cybersecurity is still low in Brazil, Costa Rica, Ecuador and Elsalvador (2016 Cybersecurity report, 2016).
The spreading of information and understanding of cyber hygiene is a challenge. Building cybersecurity awareness is an uphill task especially when the government does not prioritize cybersecurity issues. The lack of understanding of security and technological challenges by governments of developing countries makes the implementation of cyber security difficult (Muller, 2015). In Africa, there is a general lack of cybersecurity awareness by stakeholders such as law enforcement agencies, the judiciary, Information Communication Technology regulators and professionals as well as end users (United Nations Economic Commission for Africa Policy Brief, 2014).

Limited cybersecurity knowledge

The United Nations Economic Commission for Africa Policy Brief (2014) highlights that Africa possess a general deficiency of knowledge and information on matters of cybersecurity.

Affordability and funding challenges

According to IDG connect (2013) as cited by Muller (2015), African governments demonstrate an increased awareness of cybersecurity issues, but existing capacity for deterring cybercrime and monitoring or pursuing cybersecurity has been ineffective. Proposed cybersecurity solutions have to be cost effective for them to be embraced by most developing countries.
The setting up of Computer Incidents Response Teams (CIRTs) and Computer Emergency Response Teams (CERTs) is a good example of an expensive venture that developing countries have to embrace as they tackle cybersecurity challenges (Tagert, 2010). In the end some developing countries end up putting cybersecurity measures that match their budgets but not necessarily the best. Funding to support cybersecurity initiatives is also a major challenge in developing countries (Muller, 2015).

Perceived low susceptibility to attacks

In developing countries, detection of cyber events is often poor since the attackers always try to remain hidden and as a result, justification of cybersecurity becomes difficult until a big incident (Tagert, 2010).Without occurrence of big incidents, developing countries remain under the impression that they have low susceptibility to cyber threats.

Lack of adequate frameworks that speak to cybersecurity needs

The knowledge and frameworks available at the moment do not speak to the cybersecurity postures of developing countries and as such, these countries are left to figure out what to do.

Models that match their developing nature haven't been established and hence they remain stuck (Tagert, 2010).

Challenges in reporting cybercrime

The Republic of Mauritius Cybercrime strategy 2017-2019 (2017) indicates that reporting cybercrime is a problem as the people who are supposed to handle the report do not have cybersecurity knowledge and background to understand the nature of the report and assist the victims accordingly.

Problems in data sharing

The exchange of data between law enforcement agencies from different countries for the purposes of carrying out investigations related to cybercrime is a challenge as the speed of exchange is slow and complexity of exchange is very high (Republic of Mauritius Cybercrime strategy 2017-2019, 2017).

Cybersecurity needs of people

This section will look at the cybersecurity needs of people.

Cybersecurity emergency readiness

Cybersecurity incident reporting mechanisms should be instituted by government so as to improve on the cybersecurity emergency readiness. This is achievable through the setting up of national Computer Security Incidence Response Teams (CSIRTs) as well as sector CSIRTs (Ghana National Cybersecurity Policy and Strategy, 2014). In addition to that, standardized business continuity management guidelines should be in place to assist in the identification of risks and exposure to internal and external threats.Vulnerability assessment programs should also be performed in order to be ready for cybersecurity emergencies. Vulnerabilities are structural faults or defects of a nation's critical information infrastructure and information systems that include human negligence, porous procedures or actions and technical imperfections (Nigeria Cybersecurity Strategy, 2014). According to Republic of Mauritius Cybercrime strategy 2017-2019 (2017), cyber- threat monitoring systems can also be put in place so as to monitor and respond to cyber threats at a national level.

Effective governance and public and private partnership

When it comes to cybersecurity issues and the fighting of cybercrime, individuals, industry and government have a critical role to play and should share the responsibility (Republic of Mauritius Cybercrime strategy 2017-2019, 2017). The centralization of the coordination of cyber security initiatives and the collaboration between the private and public sector players are key ingredients of a cybersecurity blueprint (Ghana National Cybersecurity Policy and Strategy, 2014).

Security culture and capacity building

Government should promote a cybersecurity culture by way of standardizing and coordinating the cybersecurity awareness and education programmes across all arms that monitor availability of critical infrastructure. It should also come up with a way of disseminating

cybersecurity information at national level (Ghana National Cybersecurity Policy and Strategy, 2014).

On the other hand it is important for prosecutors, investigating teams and legal practitioners to be trained adequately on cybersecurity so that they can deal with digital evidence in courts (Republic of Mauritius Cybercrime strategy 2017-2019, 2017). Cybersecurity curricula for institutions of higher learning should be developed so as to groom competent cybersecurity professionals (Kenya National Cybersecurity Strategy, 2014).Models of certifying individuals for high standards of competence in the field of cybersecurity should be introduced to promote relevance and up to date skills (Nigeria National Cybersecurity Strategy, 2014).

Uninterrupted internet connectivity
Intermittent internet connectivity cripples the ability of stakeholders to join forces in the preparation for, or to response to, a cyber-attack. In that regard, there is need for continuous internet connectivity especially in most African countries (Internet Society and African Union, 2017).

Collaboration of network operators and service providers
The cooperation and partnership between several network operators and service providers is an extremely important element of security solutions. From a service provision point of view, it will also bring down service costs and charges and will result in an improved availability of internet services and accessibility to the users (Internet Society and African Union, 2017).

Availability and reliability of electricity
According to the Internet Society and African Union (2017), the availability and reliability of electricity should be improved since recurrent power outages and power cuts have a direct impact on the availability of internet and online services.

Protection of critical internet infrastructure
The Internet Society and African Union (2017) stipulates that governments should play a critical role in protecting its citizens from cyberattacks. One good way of doing this is by means of identifying and protecting critical internet infrastructure as a way of cushioning against catastrophic service disruption.

Cybersecurity awareness
There is great need for awareness of the risks associated with the use of information and communication technologies in Africa (ICTs) (Internet Society and African Union, 2017).

Incorporation of cybersecurity strategy in national strategic plans
There is need for African governments to fuse cyber security strategy in the national strategic plans so as to fully achieve the objective of economic and social prosperity whilst cushioning against the cyber threats that emanate from cyberspace (Internet Society and African Union, 2017).This will also improve confidence in the use of the internet in the African continent as well.

Need for bridging the digital divide among people with disabilities

People with disabilities are not benefiting from the internet due to internet accessibility challenges that come as a result of lack of financial resources since most of them are poor (Kaye, 2000). Governments need to put in place mechanisms that ensure that these people get access to the internet and vital information and are protected in cyberspace.

Local language translation

For people who do not able to communicate in English or whose language is not offered over the Internet, it is tough to make digital information and services valuable to them (West, 2015). There is great need for people to access wide-ranging digital content using their local languages. This will promote better digital literacy and show people the benefits of cyberspace as well as the dark side of it and how to protect their information and non-information assets.

RESEARCH METHODOLOGY

A research methodology is a way of solving a research problem thoroughly and meticulously and includes steps followed in carrying out the research and the reasoning behind (Kothari, 2004). According to Remenyi et al (1998) as cited by Mohajan (2018), research methodology can also be viewed as a procedural or step by step outline or framework within which research is done. In this research, a qualitative research methodology was used in order to fulfill the objectives of this study. The choice of the qualitative research methodology in this research was guided by the underlying *Interpretivist paradigm* that seeks to understand the thought process of respondents in a certain context and generate new concepts or theories. According to Willig (2001) as cited by Hossain (2011), qualitative research is mostly concerned about contextual meaning which blends well with the world views of the Interpretivists that there are multiple realities that exist and have to be studied in contexts.

According to Lather (1986) as cited by Kivunja and Kuyini (2017) a research paradigm gives a reflection of the researcher's opinions or beliefs about the world that s/he exists in or want to exist in. It also speaks of a research culture comprising of beliefs, assumptions and values that a group of researchers has in common in terms of the nature of research and how it should be conducted (Kuhn, 1977). In this research, an *Interpretivist paradigm* was used.The aim of this paradigm according to Guba and Lincoln (1989) as cited by Kivunja and Kuyini (2017) is to understand the viewpoint of the subject under study so as to interpret what the subject is thinking or the meaning that s/he is making of the situation or setting. Cybersecurity is a huge area for consideration and in order to address problems within it, there is need for contextualization. Cybersecurity has to be studied in the context of grassroot users of cyberspace in Zimbabwe in order to develop concepts or even theories that are informed by reality on the Zimbabwean ground. In this research, in order to come up with a cybersecurity framework for grassroot users of cyberspace in Zimbabwe, it was critical to study respondents in detail within their rural context in order derive important concepts.

According to Cresswell and Plano Clark (2007) and Saunders et al (2009) there are two main approaches that can be used in research namely inductive and deductive. These approaches offer strong guidance and direction in coming up with a research design. In this research, an

inductive approach was used. This was due to the fact that the research was driven by the need to come up with a Zimbabwean narrative on cybersecurity in the rural context not to test already established theories that have been crafted elsewhere under different conditions.

According to Kothari (2004), a *research design* symbolizes advance planning or a research master plan. This planning caters for the research methods to be used, techniques to analyse the data whilst addressing the objectives of the research and taking into account the resources available. Bougie and Sekeran, (2009) and Kerlinger (1986) as cited in Kumar (2011) define research design as a strategy for answering key questions in a study. In this research a *descriptive research design* was used to answer the research questions:

According to Saunders et al (2009), a research must be bound by time horizons. These horizons are categorised into two namely cross sectional studies and longitudinal studies. This study was *cross sectional* as it looked at the cybersecurity needs and challenges that the rural community of Murewa District was facing. This paved way for the crafting of the cybersecurity blueprint meant to cushion rural communities against cybersecurity threats.

The data was collected using interviews, questionnaires and observations.

A *population* is a full set of elements from which a sample is taken (Saunders et al, 2009). A sample is a share or a part of a population (Etikan et al, 2016) .A sample size is the number of respondents from which the researcher gets the required information (Kumar, 2011).In this research *judgmental sampling (non-probability)* was used by the researcher to select key respondents on the basis of their knowledge on of usage of internet enabled devices and applications as well as cybersecurity. The sample was drawn from people from Murewa District who came to the community information centre as well as students and teachers from schools around Murewa Growth Point. Students and lecturers from Harare Polytechnic College were also part of the sample together with managers and employees of banks as well as telecommunication companies. Representatives from the Ministry of Information Communication Technology, Postal and Courier Services were also part of the sample.

DATA PRESENTATION AND ANALYSIS

According to Marshall and Rossman (1990), data analysis is a process of conveying order, structure and sense to the gathered data. The process happens in a non-linear style (Saunders et al, 2009). Qualitative data analysis is an expedition to relate common statements about associations among groups of data. The process of data analysis in qualitative research also includes data categorization, data break down and synthesis, pattern searching and determining what is essential and what is to be learned and deciding what to convey to others (Bogdan and Biklen, 1982).

Data obtained was presented and analyzed as below:

Cybersecurity challenges faced by grassroot internet users in Zimbabwe

Lack of appropriate supporting infrastructure

Participants reiterated the fact that several computerization programmes had been launched in many rural schools. The sole purpose was that of bridging the digital divide and promoting access to various Information Communication Technologies (ICTs) especially in rural communities.

However, these computerization initiatives had not been equally matched with electrification initiatives such that the computers remained idle due to lack of electricity infrastructure.

A participant had this to say:

"...Our school received many computers from the President as part of his computerization programme some 10-15 years ago. However, load shedding stands as a big stumbling block in the teaching of Computer Studies and cybersecurity especially in our rural communities.

Our schools cannot afford backup options such as generators to power the computer lab due to the fact that the fees that are paid by students are not that much and besides fuel is a challenge these days.

Many students have the zeal to take Computer Studies but however they sometimes end up doing a few practical lessons and many of them end up dropping the subject and taking Agriculture or Fashion and Fabrics instead".

Participants indicated that heavy load shedding was greatly affecting the teaching of computer studies as in most cases, electricity was only available during the night when the schools had closed. Respondents also highlighted that generators are costly to run and affordability is a challenge for most rural schools and as a result the enrolment levels for computer studies subject were very low.

These findings resonate well with those from the Tanzania Country Report (2009). It revealed that ICT supporting infrastructure such as electricity and road networks are still underdeveloped in Africa. This is a huge blow for accessibility and spread of Information Communication Technology for Development (ICT4D) especially in remote rural areas of the country.

The Zimbabwe National Policy for ICT 2016-2020 (2016) also concurs with the findings as it also indicates that the national power grid does not cover all the parts of the country. As such, other parts have to depend on other alternative sources which happen to be more expensive. Those on the national power grid also experience irregular supply and this affects the usage and development of ICTs.

Furthermore, according to The Zimbabwe National Policy for ICT 2016-2020 (2016) infrastructure development had also been affected by lack of investment capital. This was due to the high perceived country risk that has culminated in very high lending rates for foreign borrowings.

Internet connectivity challenges

Respondents reported that internet connectivity was a challenge. They indicated that sometimes it would be down and when up it will be slow when surfing and this was affecting activities

such as researching as well as online transactions. Some card transactions ended up failing due to poor connectivity resulting in the debiting of their accounts without the transactions necessarily having gone through successfully. Participants highlighted that recovering those funds from the relevant service providers was a time consuming exercise and very inconveniencing.

The findings also resonate well with those in the Tanzania country report (2009) which outlines that network connectivity is inadequate in Africa and often results in service unavailability and unreliability. The Zimbabwe National Policy for ICT 2016-2020 (2016) also confirms the phenomenon as it highlights that the communications infrastructure is inadequate. As such, broadband coverage is very low especially in the rural and remote areas of Zimbabwe.

Generally poor connectivity pulls down efforts to use the cyberspace and any initiative towards addressing cybersecurity challenges.

Challenges in prosecuting cybercriminals

Participants indicated that there were some difficulties in tracking the perpetrators of cybercrime and bringing them to book. They felt that the police were not well equipped and knowledgeable on how to handle cybersecurity cases and victims.

As a result, users of cyberspace end up not reporting these cases when cyber breaches occur. A participant had this to say regarding the prosecution of cybercriminals

" ..*Even if you go to the police and tell them that you have been hacked, they will ask you by who and what will you then say? I do not even know how to explain this hacking myself.*

I do not think that the police are even equipped to handle such cases and reporting those cases to them is a waste of time. Some of the police officers do not even understand these cybersecurity matters and they are taught to demand physical evidence as proof of which when it comes to cybercrime the evidence may be electronic."

These findings are in sync with what Olayemi (2014) found out in Nigeria that the absence of proper legislation to deal with online criminality makes it difficult to take legal action against cyber criminals.

The International Telecommunications Union (2007) also adds that digital evidence is difficult to get and there is need for cooperation between legal authorities in different countries as well as requisite legislation in order to combat cybercrime.

On the other hand, according to IDG connect (2013) increased internet access with no proper legal frameworks in place creates more destruction than benefits and cybersecurity legal frameworks are part of key tools for combating cybercrime (United Nations Economic Commission for Africa, 2014).

Criminal and financial identity theft

Some participants pointed out that they had their personal and credit card details stolen through their emails by people they do not know. As a result, some had lost some money in the process. Some pointed out that they sometimes received messages asking them for their pin numbers

from sources that claimed that they were their banking institutions. As a result, some ended up losing money to these cyber criminals. Some respondents reported that social media platforms such as WhatsApp, Facebook and Twitter are now being used for reconnaissance purposes by hackers to gather basic information from end users who may be ignorant.

Pornography

Participants also revealed that unnecessary pop ups of adverts some of which are pornographic disturbed smooth internet surfing and ended up leading the users to more pornographic websites as well as diverting their attention. As a result, some students just ended up abusing the internet by way of just downloading pornographic material on pornographic websites.

A responded had this to say:

"..Raising children in this digital era has become more challenging than ever. The internet can be an excellent educational tool, but without parental control software and careful monitoring and supervision it can be an extremely dangerous place. In most cases the children are more technology literate than the parents and they do as they please.

They have ways of hiding their online activity from parents such as clearing their search history on their internet browsers. However it is very important for parents to be aware of what the children do on the internet and not just pay for internet services. When it comes to the issue of the internet, parental control is difficult. I wish there was a way of restricting what content the children could access on the internet, the same way we restrict certain channels on DSTV".

The evidence above points to the need for child online protection measures. According to the International Telecommunication Union (2017), child online protection is one of the key technical measures in cybersecurity.

It goes a long way in making the children feel safe and comfortable when they are on the internet and less headaches to parents and guardians on issues to do with internet safety.

In Singapore, the Internet Content Providers and Internet Access Service Providers are obliged to comply with the Internet Code of Practice in order to protect children online. On the other hand, the Information Communications Media Development Authority also blocks pornographic websites.

In the case of Zimbabwe, according to the Zimbabwe National Policy for ICT 2016-2020 (2016), the licensing regime in Zimbabwe is now outdated and not in sync with technological developments. It therefore does not support an Information Society. As a result, most kids are exposed to pornography since there is no restriction on what content they should access

Social media hacks

Some respondents also indicated that they had their Facebook accounts hacked and the hackers ended up posting pornographic material on their timelines and to their friends. Some reported that these incidents happened after they had clicked some links that popped whilst they were surfing the internet.

In an interview with some of the respondents, one participant had this to say:

"…I received several calls from my friends asking me why I had sent them some pornographic links and clips on Facebook. I was surprised to hear about this and I checked my Facebook account and later on someone told me that my Facebook account had been hacked and they helped me close the account, apologize and notify my friends that my account had been hacked".

The findings reveal that cyber hygiene is very important for everyone who uses cyberspace and failure to practise it normally results in falling prey to cybercriminals. The International Telecommunication Union (2007) encourages cyber hygiene as a means of avoiding incidences of hacking since most cyber criminals capitalize on mistakes or carelessness by users of the cyberspace such as weak passwords and saving passwords on internet browsers.

Limited cybersecurity courses in the education curricula

Some participants from the education fraternity highlighted that the Zimbabwean education system offers zero or limited cybersecurity courses on cybersecurity. Thus at primary or secondary level, there is no solid education on cybersecurity and yet the people who fall in these age groups frequently visit the cyberspace.

This then makes them more exposed to a myriad of cyber-attacks that are often perpetrated on cyberspace. Cultivating a culture of cyber security becomes difficult if there is no early foundational cybersecurity topics covered.

These findings go along with what the Zimbabwe National Policy for ICT 2016-2020 (2016) highlights. In one of its desired policy outcomes, it clearly stipulates that Zimbabwe needs to step up in the provision of ICT enabled training and education countrywide especially in remote and rural areas. This will go a long way in improving digital literacy rate especially in rural communities.

Inadequate research in cybersecurity

Some respondents from the higher education sector indicated that research in cybersecurity is still in its infancy in Zimbabwe. In addition there is overreliance on outdated information in higher learning institutions. In some instances, there is no proper IT equipment that necessitates a practical cybersecurity learning approach.

A student from Harare polytechnic college had this to say:

"…At the present moment those doing IT related diplomas, higher national diplomas or certificates have the privilege of doing one or two IT security related courses, otherwise the rest pass through the academic system without being taught anything to do with IT security.

To a certain extent the lack of adequate IT infrastructure and funding derails cybersecurity research."

Research and Development programmes are very important when it comes to cybersecurity capacity building (International Telecommunications Union, 2017). Kritzinger and von Solms (2012) also concur with the results and add that dedicated cybersecurity research in Africa for

Africa is vital. It leads to the birth of new cybersecurity answers for the continent's cybersecurity problems.

The Zimbabwe National Policy for ICT 2016-2020 (2016) also confirms these findings. Local ICT research and development in Zimbabwe is limited due to the absence of a research and development framework. In that regard, there is no room for innovation and exploitation of the full potential of ICTs. However strides have also been taken to nurture research through the establishment of institutions such as the Research Council of Zimbabwe (RCZ) and the Scientific and Industrial Research and Development Corporation (SIRDC).

Cybersecurity skills deficiency

Respondents also reiterated the fact that there is a massive cybersecurity skills gap in Zimbabwe. There is only a few people pursuing information security or cybersecurity as a course or career.

Brain drain is also a major contributing factor to this cybersecurity skill gap as those skilled in cybersecurity or information security go to nearby countries or abroad in search for greener pastures.

A respondent had this to say:

"…Information security and cybersecurity professionals are on high demand. With our Zimbabwean economy that is not performing well, these professionals will just go outside this country to where they will be paid well and we will continue to lose these professionals. There is a huge demand of skilled cybersecurity and information security professionals globally."

Findings by the Africa Cyber Security Report (2018), United Nations Economic Commission for Africa (2014) and Information Systems Audit and Control Association (2019) also confirm that Africa and the world at large are in short supply of local cybersecurity skillsets and technical experience. These few technically skilful professionals demand high remuneration and are very difficult to retain.

In the case of Zimbabwe, according to the Zimbabwe National Policy for ICT 2016-2020 (2016), the country has a shortage of skilled ICT professionals. This is a challenge when it comes to the implementation of ICT programmes or projects and this has negatively impacted on digital literacy.

Fake news

Respondents reported that fake news was a pain as it was causing unnecessary panic amongst citizens. In some cases, it was causing destruction of property through inciting violence in Zimbabwe. Participants also revealed that fake news had also contributed to some marriage breakdowns and also defamation of character.

They also reported that it is also difficult to determine whether the information they come across is fake or authentic since the social media platforms generate a lot of content.

These results confirm findings by the Africa Cyber Security Report (2018) that in most cases, the public is not well equipped to differentiate between true and fake information.

The WhatsApp platform is the most used platform to spread fake news. In Kenya, during the 2017 election, videos and pictures of the 2007/2008 post-election violence were being circulated for the purposes of inciting violence.

It is important to take note that misinformation can be very costly and extremely difficult to reverse and respond to .This is normally the case when trust and confidence are undermined.

However it may be handy to put in place legislation that makes the spreading of fake news or misinformation a punishable offence so as to make the public desist from generating and spreading fake news.

Lack of ministerial role clarity on cybersecurity matters

Some respondents highlighted that in Zimbabwe, there is a lack of ministerial role clarity on cybersecurity matters.

An official from the Ministry of ICT, Postal and Courier Services had this contribution to make:

"… It is not very clear to us as to the ministry responsible and accountable for cybersecurity and driving the cybersecurity initiatives in the country. The cybersecurity responsibilities are shared between the Ministry of Defense, Ministry of Home Affairs and Ministry of ICT, Postal and Courier Services.

As such it's not very clear as to which Ministry does what and ends where. This is not good because it then affects the planning and implementation of cybersecurity programmes as there may be lack of clarity and confidence as to whether certain roles fall under our purview or of some other ministries".

In some circles cybersecurity is regarded as an ICT problem or technical problem and yet it is more social than technical. However, cybersecurity cuts across several government ministries and they should work together.

The Norwegian Institute of International Affairs (2015) also adds its support to the results by pointing out that the lack of clarity of ministerial roles in cybersecurity matters may also create conflicts of interest within ministries in governments.

The findings however contradict to what is out there in some other countries. The ministry responsible for cyber security is clearly spelt and the relevant structures are in place. For instance, in Italy, the Italian Ministry of Defense defined cyber security as a threat to national defense and security and admitted that cyberspace is now another sphere of warfare. As such an Italian Cyber Command was formed under the Ministry of Defense (Cyber Readiness Index 2.0, 2016).

Limited policies and regulations to counter cyber threats

Participants also indicated that there were no well-developed policies and regulations to counter cyber-attacks.

The International Telecommunications Union (2007) supports the idea that security policies can help to combat against cyber-attacks. However, they have to be simple and easy to

understand and must be periodically reviewed, improved and modified in line with rapid technological changes for them to remain effective.

Shortage of cybersecurity staff in schools

Some school heads indicated that the biggest challenge they were facing was that of lack of skilled ICT staff who could teach Computer Studies and cybersecurity.

A senior teacher had this contribution to make:

"*Another factor that is contributing to the shortage of ICT teachers in rural schools is that generally most of them do not want to be in rural areas. Most of them prefer to teach at schools close to towns. They are interested in teaching at schools where there is internet access of which most rural schools here do not have that because of financial reasons. Over the years we have seen them transferring to urban schools and some even go to offer their services outside the country".*

Limited cyber security capacity building for teachers

Some rural school teachers complained about the lack of ICT and cybersecurity capacity building initiatives such as workshops and trainings.

A rural teacher had this to say:

"..There are no existing guidelines that call for teachers to obtain ICT and cyber security-based trainings yet they are required to defend their personal, school and student data with high importance and also give responses to intuitive questions from their students".

Another rural teacher had this to say:

".. *The new education curriculum is encouraging the use of ICTs in teaching and learning but unfortunately the government which is our employer is silent and not doing anything about the issue of training on the part of the teacher who is supposed to teach the students".*

The creation of the ICT clubs has for some time now served as a platform through which students (club members) obtain the pertinent skills needed when dealing with cyber-related issues and the computer world in general. However, there is still a lot that needs to be done in order to keep up to date with vectors of attacks and how to safeguard ourselves.

These results are consistent with those of the International Telecommunications Union (2017) which also acknowledges that cybersecurity capacity building in the form of education and training courses or programmes is essential.

The Africa Cyber Security Report (2018) also reveals that some African governments have supported the inclusion of ICTs in the education sector. However, they have not equally invested in the implementation of trainings on cyber based threats amongst teachers, students and citizens.

British Journal of Multidisciplinary and Advanced Studies:
Engineering and Technology, 3(2),77-104, 2022
Print ISSN: 2517-276X
Online ISSN: 2517-2778
https://bjmas.org/index.php/bjmas/index
Published by the European Centre for Research Training and Development UK

Limited understanding of ICT and cybersecurity issues

The researcher noted that most participants were not well conversant with issues to do with ICTs in general and cybersecurity was a big word to them.

A participant had this to say:

"..We know how to use computers, particularly typing using MS Word and Excel, browsing the internet and sending emails. We just hear people talking about hacking but we do not really know how it happens and what it is."

These observations are in line with findings by the IDG Connect (2013) which point to the fact that in many developing countries, there is inadequate understanding of the significance and relevance of cybersecurity.

Users do not have an appreciation of the steps they can take to better protect themselves online. This is also supported by United Nations Economic Commission for Africa (2014) which indicate that stakeholders have limited awareness. These include ICT regulators and professionals, users, law enforcement agencies and the judiciary.

Cybersecurity needs of grassroot users of internet in Zimbabwe

The researcher found out that the users of cyberspace had the following needs:

Cybersecurity awareness

Participants indicated that cybersecurity awareness programmes needed to be conducted frequently at grassroot level. This would go a long way in raising awareness in Zimbabwe as it forms the first layer of security against cyber-attacks. Awareness promotes thoroughness and cautiousness in the conduct of cyber activities in the cyberspace.

A participant had this to say:

". .People need to be made aware of the internet, its dangers and how to use it responsibly.

For example, the awareness campaigns that are being done by the Postal and Telecommunications Regulatory Authority of Zimbabwe are very good. However, Zimbabwe is very big and POTRAZ needs support from a lot of stakeholders for them to be effective. The Mobile Network Operators need to also take an active role in these awareness programmes as a way of giving back to the community."

This resonates well with findings by the International Telecommunications Union (2017) about Belarus where a partnership between the mobile operator MTS and the Ministry of Education in the teaching of children about safe internet practices has resulted in the improvement of awareness levels in the country.

In the same vein, according to West (2015), in India, instructional classes are conducted with a view to train adults especially from rural areas, senior citizens and poor people on safe internet usage. The Information Systems and Audit Control Association (2019) also supports security awareness programs as they can significantly reduce risk by addressing the behavioral

aspects of security. This is through education and regular application of awareness practices. These security awareness programmes should address usual concerns such as web browsing safety, email usage and password selection for different users.

Cybersecurity technical measures

Participants echoed the need for adoption of technical measures that are implementable in our Zimbabwean environment. These range from internet and social media policies, backups, antiviruses, access controls as well as other physical and logical security measures.

These results are also consistent with what Kritzinger and von Solms (2012) unraveled. They revealed that Africans lack latest technical security measures such as anti-virus packages and many of the operating systems used are not regularly patched.

However, the International Telecommunications Union (2017) propose technical measures such as National Computer Incident Response Team (CIRT), Government Computer Incident Response teams or Sectorial Incident Response Teams. In Egypt, a computer emergency response team (EG-CERT) was set up to tackle cyber threats. In the same vein, in terms of the setting up of Computer Emergency Response Teams (CERTs) a participant from the Ministry of ICT, Courier and Postal Services had this to say:

"*..Other countries have done very well in the setting up of Computer Emergency Response Teams .Here in Zimbabwe we are yet to do that. These are very important when it comes to matters of cybersecurity and I hope the Ministry will scale up efforts along those lines because cyber threats are real."*

On the other hand, Luxembourg also has a Governmental Computer Emergency Response Team (GOVCERT.LU) that is designed to protect government computer systems and infrastructures.

In Sri Lanka, a Financial Sector Computer Security Incident Response Team (FINCSIRT) was established for the sake of handling cybersecurity incidents affecting the financial services sector.

The Information Systems and Audit Control Association (2019) also support the need for Computer Emergency Response Teams as they help in threat intelligence. This will give insights and advanced information on possible or existing attacks that threaten institutions, organizations or nations at large.

Cybersecurity skills training

Respondents indicated that Cybersecurity skills gaps should be addressed so as to reduce errors that may lead to cyber breaches and compromised security.

A participant had this to say regarding the issue of cybersecurity skills training

"..The Government of Zimbabwe should take a vested interest in the training of cybersecurity skills through approaches like offering tax rebates to companies that can train professionals in cybersecurity or giving rebates on all cybersecurity training equipment that may be

imported. This can go a long way in growing the cybersecurity training industry and this will be good for the country."

These findings confirm what the Africa Cyber Security Report (2018) revealed. It indicated that governments should contemplate on the idea of giving grants or tax breaks to corporations and organizations that specialize in the training of cybersecurity professionals.

This is also supported by the International Telecommunications Union (2017) which highlights that a home grown cyber security industry is an essential ingredient of capacity building in cybersecurity. For that reason, efforts around nurturing it are extremely important. A good example in this regard is that of Ireland which is leveraging on incentives such as favorable low taxes and business environment to grow its cybersecurity industry.

Cybersecurity education

Participants reiterated the fact that there is need for the introduction of mandatory cybersecurity courses at certificate, diploma and degree levels.For non-graduates, the courses could be introduced at primary and secondary level. The more the subject of cybersecurity is known, the higher the chances of remaining protected because security software alone cannot provide a cushion against the cyber risks.

A participant had this to say regarding cybersecurity education.

". The subject of cybersecurity must be taken seriously. Right now in Zimbabwe we only have the Harare Institute of Technology offering a Bachelor's degree that is related to information assurance and cybersecurity. Other universities do not offer certificates, degrees or diplomas in cybersecurity. Instead security related courses are only offered as part of ICT related degree programmes. Clearly something has to be done to address the supply side of cybersecurity professionals if we are to enhance our cybersecurity posture as a nation."

These findings go well with those by the United Nations Economic Commission for Africa (2014) which point to the fact that the rapid growth in the use of cyberspace in Africa is not in phase with education initiatives especially on internet safety .There is great need for National Education programmes as well as academic curricula that support cybersecurity (International Telecommunications Union, 2017).The Africa Cyber Security Report (2018) also supports the need for academic institutions to include cybersecurity courses in their curriculum with laser focus on practical hands-on learning for ICT related programs. This may require interaction with employers to get the actual needed security skills on the market.

Hands-on education can be fostered through hackathons and internships. In Kenya, as at November 2018 there were only three bachelor's degree programs, four masters programs, two post graduate diploma programs and one doctor of philosophy programs in the area of information security. To further support the findings, Muchiri (2019) also reveals that in East Africa, only 5% of the Universities offer undergraduate degree programmes in ICT with a specialization in cybersecurity. The findings all point to the need for efforts to be channeled towards cybersecurity education.

Cybersecurity capacity building for law enforcement agencies

Respondents pointed out that the Zimbabwean law enforcement agencies need to be equipped through training and education in order to handle cybercrimes. This will empower them to protect people in their communities against cyber-attacks. They will also become prepared to handle cybercrime committed within or outside national boundaries and to handle victims of cybercrime.

These findings resonate well with current practices in Mauritius where it conducts training for law enforcement personnel and members of the judiciary services (International Telecommunications Union, 2017). The International telecommunications Union (2007) also support this idea as it reveals that there is a gross mismatch between the skills of cybercriminals and resources available to the law enforcement agencies for prosecution.

Generally, there is low usage of ICTs by these agencies and they rely heavily on conventional crime investigation methods which are not suitable for cybercrime.

Physical Security of ICT Assets

Participants from schools revealed that strong physical security of ICT assets was required because vandalism and theft of computers and computer accessories was quite rampant in some primary and secondary schools in Murewa. This was primarily as a result of weak physical security controls.

A teacher had this to say:

"*..We had a scenario whereby the computers that had been donated under the Presidential Computerization Programme were vandalized .The hard drives and RAM were stolen and it is suspected that some teachers had a hand in that. The main reason why this happened is that there was no secure room for storing these desktop computers. When they were delivered, they were kept in a library because there was no better place to keep them. After the incident, a strong room had to be constructed to avoid such occurrences. However, things being normal, a computer laboratory has to be in place where students will go for lessons. In our current set up, a few desktops have to be taken from the strong room during a computer studies lesson and then returned after the lesson and this only happens when there is electricity."*

These findings resonate well with recommendations from the International Telecommunications Union (2007) which stipulate that physical security is the most essential ICT system control. Computers need physical protection against accidents such as fire and water damage as well as unauthorized access. Proper air conditioning and electricity supply panels have to be installed in rooms that house ICT equipment.

Special Call Centre for reporting cybercrimes

Some respondents pointed out the need for a dedicated cybersecurity call centre where cyber incidents can be reported and relevant assistance can be offered.

A participant had this to say:

"..I wish we had a call centre of some sort that will be manned by cybersecurity experts where we could report any cybercrime anytime or even a toll free number that we could call, just like the toll free number for Zimbabwe Revenue Authority for reporting any act of corruption."

These findings are fully supported by United Nations Economic Commission for Africa (2014) which emphasize the need for a dedicated call center for reporting cybercrime. This will go a long way in giving assurance to victims of cybercrime that there is somewhere they can turn up to in times of need and get the necessary assistance. This special call centre has to be staffed by adequately trained and well-informed cybersecurity professionals. Reporting channels can also be widened to include a website and a toll free number that cyber victims can use to report cybercrimes conveniently.

Cybersecurity knowledge sharing and management

Participants reiterated the need for knowledge sharing particularly on issues to do with cybersecurity.

A teacher from one of the rural schools had this to say:

"..Cybersecurity knowledge has to be shared. Maybe for a start, pamphlets or magazines or books can be distributed to our rural schools so that the students can read and get to appreciate some of the issues to do with cybersecurity. For your own information, most students are very keen to learn about computer related issues".

These findings are solidly supported by Microsoft (2019) which highlight that information and data sharing between public and private sectors is a key ingredient to the fight against cybercrime.

Cybersecurity legislation

Participants revealed the need for cybersecurity legislation as a way to tackle some of the cybersecurity challenges being faced in Zimbabwe.

A respondent had this to say:

"..One key aspect that we have not yet managed to put in place as Zimbabwe when it comes to cybersecurity issues is legislation. We just have a draft bill that has not been put into law."

These findings are fully supported by the Zimbabwe National Policy for ICT 2016-2020 (2016).It stipulates that legislation in line with consumer protection, child online protection, intellectual property protection and copyright as well as data protection and privacy need to be fast tracked for the benefit of the citizens.

On the other hand, the United Nations Economic Commission for Africa (2014) also reiterates that the lack of cybersecurity legislation affects business negatively. As such, in order to ensure confidence and trust in the use of the internet, particularly in doing online transactions, legislation has to be there to govern how stakeholders do business (International Telecommunications Union, 2017).

CONCLUSIONS

The following conclusions were drawn from the research findings:

(a) Cybersecurity efforts in rural Zimbabwe should be complemented immensely by ICT supporting infrastructure such as electricity and base stations

(b) School teachers in rural Zimbabwe are not knowledgeable in the field of cybersecurity and hence it's hard for them to teach the pupils.

(c)There is a huge affinity among grassroot people to use the internet but however there is limited understanding of the harm that it can bring

(d) Cybersecurity awareness campaigns being coordinated by the Ministry Of ICT, Postal and Courier Services are bearing fruit in rural communities in Zimbabwe. However, more support from the private sector players is required to sustain the momentum.

(e) There is a gap in the Zimbabwean education curriculum in the area of cybersecurity

(f) Police in Zimbabwe are ready to handle cybersecurity cases and victims in their communities

(g) Cybersecurity research is still in its infancy in Zimbabwe.

(h) Lack of electricity is a major barrier to the proper teaching of cybersecurity

RECOMMENDATIONS

Based on the fore going conclusions, this research proffered the following recommendations:

(a) Solar systems should be adopted for use as an alternative source of energy so as to address electricity problems

(b) The education curricula should incorporate cybersecurity courses at both primary and secondary level in order to foster responsible use of cyberspace.

(c) Government of Zimbabwe should embark on capacity building workshops and training in cybersecurity for teachers to stimulate the learning of cybersecurity.

(d) The cybersecurity legislation in Zimbabwe should be continuously reviewed and realigned with the changing cyber threat landscape.

Acknowledgement

The author acknowledges and appreciates the Zimbabwe Open University (ZOU) for supporting this research work.

Funding

The author did not receive financial support for the research, authorship, and/or publication of this article.

Conflict of Interest

There is no conflict of interest related with this publication.

References.

Angelini et al (2017). CRUMBS: a Cybersecurity Framework Browser.

ACS(2016).Cybersecurity: Opportunities, Threats and Challenges

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

Bada, M and Sasse ,A (2014).Cyber Security Awareness Campaigns: Why do they fail to change behaviour*? Global Cyber Security Capacity Centre: Draft Working Paper*

Bougie T.R & Sekeran (2009) Research Methods for business, 3rd edition New Jersey: John Wiley

Bax, S. (2013) Cambridge marketing handbook, London: Kogan Page.

Bryman, A and Bell, E (2011) Business Research Methods,3rd Edition Oxford University Press

Burns, N. and Grove, S.K. (2001) *The Practise of Nursing research: Conduct critique and utilization*, 4th edition, Philadelphia: WB Saunders.

Burns, R. B, and Burns, R. A. (2012) *Business Research methods and statistics using SPSS*, London .Sage Publishers.

Cooper, R. D and Schinder, P.S (2013) Research Methods, 6th Edition, McGraw-Hill:Boston

Concierge (2018). Concierge Security Report. Cybersecurity: Trends from 2017 and Predictions for 2018

Cooper, R. D. & Schindler, S. P. (2014). *Business Research Methods*. Boston: Irwin McGraw Hill.

Coyne MM, Hooper M.J, Sicchitano K J. (2017). Insight That Internal Audit Brings to Cybersecurity Culture

Creswell, J.W. (2009) *Research Design: Qualitative, quantitative and mixed methods* .4rd edition, Thousand Oaks CA Sage.

Creswell, J.W. (2014) *Research Design: Qualitative, quantitative and mixed methods* .4rd edition, Sage Publications,Inc.

Daniel, S. and Sam, G. (2011), *Research Methodology*. Gyman Publishing House.

Da Veiga A. (2016) .A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument.

Dilshad M.R, Latif I, M.(2013) Focus Group Interview as a Tool for Qualitative Research: An Analysis. *Pakistan Journal of Social Sciences (PJSS) Vol. 33, No. 1 (2013), pp. 191-198*

Dlamini IZ, Taute B and Radebe J. (2011*). Proceedings of Southern African Cyber Security Awareness Workshop*Ernst and Young (2015). Cybersecurity and the Internet of Things

Fehling C, Leymann F, Retter R ,Schupeck W , Arbitter P.(2014). Cloud Computing Patterns. Fundamentals to Design, Build, and Manage Cloud Applications. Springer-Verlag Wien .

Gcaza, N., Solms, R. Von, & Vuuren, J. Van. (2015). An Ontology for a National CyberSecurity Culture Environment. *In Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015) (1-10).*

Grant C and Osanloo A. (2014). Understanding, Selecting and Integrating a Theoretical Framework in Dissertation Research. Creating the Blueprint for 'House' . Administrative Issues Journal. Connecting Education, Practise and Research .pp 12-24

https://consulting.ey.com/cybersecurity-in-higher-education-the-changing-threat-landscape/

https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021

http://www.ictministry.gov.zw/

http://sciencenordic.com/poor-countries-are-more-vulnerable-cyber-attacs

http://www.zarnet.ac.zw/

https://doi.org/10.6028/NIST.CSWP.04162018

Heeks, R.(2009).The ICT4D Manifesto: Where next for ICTs and International Development? Development informatics Working Paper series,(42) pp.1-35

International Telecommunication Union, 2008. Global Security Report.

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

Health Information Trust Alliance, 2014. Introduction to the HITRUST Common Security Framework

Hossain D, M (2011).Qualitative Research Process in Postmodern Openings. Year 2 Volume 7, September 2011 pp 143-156

Hancock B., Windridge K., and Ockleford E. (2007). An Introduction to Qualitative Research. The NIHR RDS EM / YH, 2007

Hancock D.R, Algozinne B.(2006). Doing Case Study Research.Teachers College Press, NewYork

https://ccis.no/cyber-security-versus-information-security/

International Telecommunication Union (2017).Global Cybersecurity Index (GCI)

International Telecommunication Union, 2008. Global Security Report.

Kothari, C (2004) *Research Methodology Methods and Techniques,* 2nd Edition. New Age International Publishers

Kabweza LSM. (2017).”WannaCry Ransomware: Zimbabwe among countries hit by massive cyber-attack”

Kumar, R. (2011) *Research Methodology: A step by step guide for beginners* 3rd ed. London: Sage Publishers.

Kortjan, N. & Von Solms, R. 2014. A conceptual framework for cybersecurity awareness and education in SA. *South African Computer Journal, 52, 29-41., 2014(52), pp.29–41.*

Kothari C.R.(2004) .Research Methodology Methods and Techniques 2nd Revised Edition .New Age International Publishers

Kritzinger and Von Solms (2012).A framework for cybersecurity in Africa. *Journal of Information Assurance and Cybersecurity*

KPMG (2018).Clarity on Cybersecurity. Driving growth with confidence

Kivunja C and Kuyini B (2017).Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education. Vol 6 No 5;2017*

Magee, C. S. (2013). Awaiting the cyber 9/11. Joint Force Quarterly, 70, 76–82. Retrieved from http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-70/JFQ70_76-82_Magee.pdf

Malyuk and Miloslavskaya (2016). Cybersecurity Culture as an Element of IT Professional Training

Marczyk G, DeMatteo D, Festinger D (2005).Essentials of Research Design and Methodology. John Wiley & Sons, Inc

Ministry of Information, Communications and Technology (2014).National Cybersecurity Strategy.

Ministry of Technology ,Communications and Innovation (2017).Republic of Mauritius Cybercrime Strategy (2017-2019)

Ministry of Information Communication Technology and Cybersecurity (2016). Zimbabwe National Policy for Information Communication Technology (ICT) 2016-2020

Mohajan H, K (2018).Qualitative Research Methodology in Social Sciences and Related Subjects. *Journal of Economic Development, Environment and People. Volume 7 Issue 1, 2018 pp 23-48*

Muller P.L (2015). Cybersecurity Capacity Building in Developing Countries. Opportunities and Challenges. *Norwegian Institute of International Affairs*

Nassaji H (2015). Qualitative and descriptive research: Data type versus data analysis. *Language Teaching Research 2015, Vol. 19(2) 129–132*

Nigeria National Cybersecurity Strategy(2014)

National Institute of Standards and Technology (2018).Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

Oracle and KPMG (2018). Oracle and KPMG Cloud Threat Report. Keeping pace at scale: The Impact of the Cloud-enabled Workplace on Cybersecurity Strategies.

Pearson M,L, Albon S,P, Hubball H (2015).Case Study Methodology: Flexibility, Rigour and Ethical Considerations for the Scholarship of Teaching and Learning. *The Canadian Journal for the Scholarship of Teaching and Learning.Vol6, Issue 3 ,2015*

POTRAZ,(2017).Abridged Postal & Telecommunications Sector Performance Report Third Quarter 2017

Pricewaterhouse Coopers (2016).PwC Financial Services Technology 2020 and Beyond. *PwC's 19th annual Global CEO Survey, January 2016*

Reid R, Van Niekerk J (2014). From Information Security to Cyber Security Cultures

Remenyi, D et al (2008) *Doing research in business and management: An introductioto process and method*, SAGE: LA

Sabillon et al (2016).National Cybersecurity Strategies: Global Trends in Cyberspace. *International Journal of Computer Science and Software Engineering(IJCSSE),Volume 5,Issue 5,May 2016*

SA Government gazette, 2011. Draft National Cybersecurity-Policy Framework for South Africa. , p.33. Available at: http://www.cyanre.co.za/national-cybersecurity-policy.pdf.

Symantec(2016).Cybercrime and cybersecurity trends in Africa

Sawahel W. (2017).Universities face an age of cybercrime. *Issue No:475.....http://www.universityworldnews.com/article.php?story=20170922080*

Sharma R (2012).Study of Latest Emerging Trends on Cybersecurity and its Challenges to Society. *International Journal of Scientific and Engineering Research .Vol 3 Issue 6, June 2012*

Shah S.R, Al-Bargi, A (2013).Research Paradigms: Researchers' worldviews, Theoretical Frameworks and study designs. *Arab World English Journal. Volume 4 No4.2013*

Tshuma A. (2017).Hackers hijack Nust Website and demand $6 billion to restore it. http://www.chronicle.co.zw/universities-hit-by-cyber-attacks/

United Nations Economic Commission for Africa. (2014).Tackling the challenges of cybersecurity in Africa.

United Nations (2014).Policy Brief. Tackling the challenges of cybersecurity in Africa

Van Niekerk, J.F. & Von Solms, R., 2010. Information-security culture: A management perspective. Computers & Security, 29(2010), pp.476–486.

Williams, B. T. (2014). The joint force commander's guide to cyberspace operations. Joint Force Quarterly, 73(2), 12–19. Retrieved from http://ndupress.ndu.edu/ Portals/68/Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf

Wamala, F. (2011). ITU National Cybersecurity Strategy Guide. Chemistry & Geneva, Switzerland. http://onlinelibrary.wiley.com/doi/10.1002/cbdv.200490137/abstract

Walliman N. (2011).Research Methods the basics. *Taylor and Francis e-Library*

http://www. nerc.com/page.php?cid=1|15

https://www.symantec.com/content/en/us/enterprise/other_resources/b-nerc_cyber_sercurity_standard_21171699.en-us.pdf

2015 Italian Cybersecurity Report(2016).A National Cybersecurity Framework

Zimbabwe National Statistics Agency (2012).Census 2012 National Report.