

# **Cyber Security Awareness and Education Framework for Zimbabwe Universities: A Case of National University of Science and Technology**

**Belinda Mutunhu, Dr Sibusisiwe Dube, Nolwazi Ncube and Sizalobuhle Sibanda**

Computer Science Department, National University of Science and Technology  
belinda.ndlovu@nust.ac.zw, sibusisiwe.dube@nust.ac.zw, nolwazincub@gmail.com,  
sizalobuhle@gmail.com

## **Abstract**

Internet-related attacks have become prevalent and are expected to increase as the reliance on the internet also increases. Consequently, cyber security has become an essential concept in everyday life and cyber security awareness is key in the protection of people and systems against cyber threats. The study is sought to establish the current levels of cyber security awareness among students and staff in universities and propose a framework for conducting cyber security awareness and education programs. Data analysis was carried out using Statistical Package for Social Sciences (SPSS) and represented in descriptive and frequency ways as well as in percentage form. Based on research findings in this study it has been established that students and staff at universities do not have the requisite knowledge and understanding of the importance of cyber security principles, their practical application in their day-to-day activities, and are not aware of how to protect their data. It is therefore recommended that universities should implement comprehensive awareness and education programs for the adoption of necessary safety measures and a framework for conducting such programs are proposed.

## **Keywords**

Cyber security, Data analysis, awareness, framework, internet.

## **1. Introduction**

The internet has revolutionized everyday communications such that it is now a preferred medium of everyday communications in almost all aspects of people's lives (Zaryn 2013). With the emergence of a global and borderless information society, the internet has brought and continues to bring new opportunities to all countries worldwide as technologies play an important role in social and economic development (ITU 2017). We are currently living in an age where the use of the internet has become second nature to millions of people (Kritzinger and von Solms 2010). In this era of the covid19 pandemic, in almost everything we do, we use the internet. Governments, enterprises, and individuals are increasingly reliant on Information and Communication Technologies (ICTs) as digitalization proliferates fast in both the private and public sectors (Karyda 2017). In businesses, education, and even in the health sector most of the activities have transformed from manual to online. Even on the social side, for example, ordering a pizza, buying a television, sharing a moment with a friend, sending a picture over instant messaging internet is now preferred over the traditional methods. Over and above its communication value, people use the internet for financial and entertainment purposes (PEW Internet 2012). As a result, the dependence of people on the internet has grown and continues to grow.

Although the internet has numerous advantages, it is constantly threatened by many risks such as hacking, identity theft, phreaking, and online cybercrimes that often have serious effects on those who use the Internet (Kortjan 2013; Abbas 2019). Since the use of computers became an integral part of people's lives, the possibility of breach of information has also increased.

The purpose of awareness, as defined by NIST Special Publication (SP) 800-16, Information Technology Security Training Requirements: A Role and Performance-Based Model, "is simply to focus attention on security." Awareness is "intended to allow individuals to recognize IT security concerns and respond accordingly." This is important because the user is the first line of defense for an organization's cybersecurity posture. It is known that

most users, especially students, are active on social media and sometimes post sensitive and confidential information (Saidam n.d). Users share personal data on public social media accounts without hesitation. This can leak sensitive and confidential information that is easily exploited by hackers exposing the university network to cybercriminal attacks (Madyira,2015). Information security awareness can play an important role in facing cyber-attacks by intruders (Samaher and Ibrahim 2016). Cyber security is a sensitive issue to any organization and State Universities in Zimbabwe have been a target of cyber attackers.

University users need to be made aware of basic security mechanisms that need to be applied in their everyday interaction with the internet. The fundamental concept of cybersecurity is not obvious to many, and most users do not know how to manage their data (Kennison and Chan-Tin 2020). An organization becomes more vulnerable as the number of users, technologies, and knowledge increases. College students are becoming a target for phishing attacks at increasingly high rates due to the amount of time spent on the Internet. Students spend a lot of time using the Internet for research, communicating with other students, and participating in-class activities, they are a perfect target for hackers.

A preliminary literature review on cyber security indicated the lack of a clear proposal on how cyber security awareness can be implemented in Zimbabwe as a country especially in universities. Previous literature reviews have been mainly focused on students in universities and little on academic and non-academic staff. In the Zimbabwean context, there is not enough that has been done to equip users with enough knowledge about cybersecurity awareness and education. There are no digital hubs or websites dedicated to cyber security strategies that users can learn from nor does Zimbabwe have awareness strategies developed or implemented. It is against this background that the researcher identified and aims to propose a framework that universities can use to conduct awareness programs for all university students and staff. It is therefore the intent of this study to determine the awareness among university stakeholders and design an education framework for both students and staff. Without such training programs and awareness, there will be negative consequences on IT systems and their application usage, as well as on users' personal security now and in the future.

## 1.1 Objectives

- Investigate the current level of cyber security awareness and education amongst university students and staff.
- Evaluate the initiatives that some developed countries have in place about cyber security awareness and education.
- Identify the key factors for inclusion in the cyber security awareness and education framework specific to the universities in Zimbabwe.

## 2. Literature Review

Veale and Brown (2010) define cybersecurity as a concept that covers a wide range of technical and social issues that must be considered to protect networked information systems. Shambhoo and Kumar (2019) define the cyber security concept as processes that are used to secure sensitive data, computer systems, networks, and software applications from cyberattacks. The main aim of the cyber security concept is to maintain the confidentiality and integrity of data and ensure that data is available when needed. The importance of cyber security has long been considered as more technical and more focused on technical personnel. But with the evolving nature of cyber threats and the growth of societal concern on cyber security issues such as social engineering, phishing attacks, and identity theft, it is now a serious concern.

According to Garba et al. (2020), people today are more digitally connected than ever before. With social engineering now a common tactic used by criminals, users should have basic literacy and awareness of cyber security. Moallem (2019) study on cyber security awareness among university students shows that there is a need to make people aware of their various forms of attacks and ensure responsibility towards securing an organization's data. The same study also shows that educational institutions do not have an active approach to improve cybersecurity awareness among students and education on the issues of cyberattacks. With evolving cyber threats, Academic institutions need to hold comprehensive security awareness and training sessions regularly to ensure that all users know how to recognize the most common cyber security threats and vulnerability. Talal and Asifa (2021) concurs with this notion as he states that cyber security awareness and training program for universities should be included in the security management plan and strongly supported by top executives and managers. An investigation

to identify students' awareness and enthusiasm to learn cyber security in Nigerian universities by Garba et al. (2020) revealed that university students lack the basic knowledge of cybersecurity and students want cybersecurity to be incorporated in the programs offered in Nigerian tertiary institutions. Madyira (2015) conducted a study to assess the level of cyber security awareness of users at the University of Zimbabwe. The results of the study suggest that the major problem is due to a lack of security knowledge and most users consider that cyber security is the role of technical people. Alluding to this finding is the study conducted at Bindura university by Matyokurehwa, et al (2020), on cyber security awareness from the student's perspective. The results showed that students need more awareness of various social engineering attacks employed by hackers so that they do not fall into their traps. The same study also shows that social engineering attacks and malware attacks are positively connected to cyber security awareness (CSA). Zimbabwean universities have not been an exception. According to Business Weekly, published, 21 May 2021, the National University of Science and Technology (NUST) and the Harare Institute of Technology (HIT) websites also suffered 5 cyber-attacks on the 21st of June 2020. On the 20th of May 2021, the Harare Institute of Technology suffered cyber-attacks with the hackers demanding more than \$6 billion to restore information to their websites (Chronicle 21, May 2021). The amount of information exposed in this attack was the students and staff email, student information, and research libraries. Kabweza (2014) investigated the website hacks that were occurring in the country on well-known websites and concluded that the hacks were targeting one specific vulnerability on websites designed using Joomla. The hackers seemed to have uploaded malicious files in some directories on the websites. Among the affected sites was the University of Zimbabwe website. According to Bulawayo24, 18 April 2021, Zimbabwe lost more than US\$40 Million to cybercrime in the first four months of 2018 and \$64 Million in 2017. However, in the Zimbabwean context, cybersecurity awareness at universities has neither received sufficient attention nor has the importance of security been prioritized as it should be. Universities should come up with a CSA program that fosters organizational learning, supports the overall organizational mission from the perspective of information security and should be relevant to the user.

### **3. Methodology**

The Research Methodology explains the research philosophy that underpins this study, the associated research design, research method, instruments used for data collection, target population, sampling method, and finally data analysis methods. Part of the aim of this study is to determine the current level of cyber security knowledge, skills, behavior, and attitude of internet users in universities. Factual knowledge gained through data collection will be presented including frequencies and quantities. This is in line with positivist philosophy, which according to Dudovski (2009) adheres to the view that only "factual" knowledge gained through observation including measurement is trustworthy and depends on quantifiable observations that lead to statistical analyses. In this study, the researcher is interested in larger-scale data collection to understand what users know and what they don't know regarding cyber security. A case study strategy was used in this research (Yin 2011). The case study strategy involved collecting data from one Zimbabwean university. This research focused on understanding how well the university population is aware, educated, skilled, and able to protect themselves against cyber-attacks and how knowledge and skill can be impacted to improve resilience to cyber-attacks hence the researcher used the National University of Science and Technology (NUST) as a case study. In this paper, the researcher uses the quantitative research method because the objective is to determine the factual figures of the responses on various concepts of cyber security. The measurement will most accurately be determined by using the facts observed from the participants. One of the goals of quantitative research is to analyse data using a deductive approach (Merriam 2009). In this research, the researcher intended to deduce the level of CSA among Zimbabwean universities based on the findings of the user's behavior and attitude towards cyber threats and vulnerabilities and deduce from the findings key issues that need to be addressed in coming up with a framework that can be used in universities. Therefore, the focus of this research was on the exploration of some issues as well as on how many or how many other issues.

### **4. Data collection**

Positivism research is recognized for its value in Information Systems (IS) for providing an understanding of how and where technology can be fruitfully applied and quantifying social reality and subjecting it to experimental controls (Perry, 1998; Eisenhardt, 1989). As such the researcher of this paper used a quantitative data collection method that utilized questionnaires as the sole form of data collection.

#### **4.1 Questionnaire**

A questionnaire is a set of prepared questions which are distributed to a huge number of selected participants (Senthilkumar and Easwaramoorthy 2017). The questionnaire incorporated both open-ended and closed-ended

questions (Dawson 2002). The researcher chose to use this type of questionnaire to obtain guided responses to some issues and at the same time obtain the respondent's independent opinions on other issues. Oppenheim (1992) states that "a questionnaire is a tool for collecting and recording information about a particular issue of interest." In this study, the researcher is going to make use of questionnaires to extract the relevant data to measure the level of awareness on issues of cyber security, capture opinions of respondent's self-perception of skills, and identify key factors that need to be addressed to come up with a relevant CSA framework. The questionnaire serves to investigate the knowledge on different aspects of cyber security concepts, the behavior as well as reactions of the targeted groups regarding the security concepts within the university system. The questionnaire was organized to obtain the level of cyber security knowledge, self-perception of cyber security skills, and cyber security attitudes and behavior for the targeted participant groups. The researcher also used a questionnaire to gather information, from ICTS personnel, relating to the effects of users' online behavior on university security and to find out what key areas need to be addressed to enable users to interact safely online without putting the university system at risk. The questionnaires were designed using Microsoft forms and accessed using the links (<https://forms.office.com/r/D4C1sj9z6U>), for students and staff and <https://forms.office.com/r/EPmmt2QMYm>, for IT technical staff. Distribution of the questionnaires was done using email links and links sent on mobile applications like WhatsApp to various students and startups over a month. Sample questionnaire and screen short of the response statistics and sample responses from participants are attached to the appendix section of this document.

#### **4.2 Target population**

The target population is "the entire aggregation of respondents that meet the designated set of criteria" (Burns and Grove 1997:236). In this research, the target population is the university students and staff, and they are chosen because they are the main users of the internet at the university and represent the entire population in the university. According to UniRank (2020), NUST's 2020 student enrolment stood at 10000 including both undergraduate (8000) and postgraduate students (4000), and the university boasts of 2500 academic staff and 3500 non-academic staff. The targeted groups include the students who are doing their undergraduate and those doing masters, academic staff, and non-academic staff. The choice of these individual groups, using information systems as part of their day-to-day job demands, had a basis that they are the main internet users, and their vulnerability could pose a huge impact on the university systems.

#### **4.3 Target Sampling method**

Sampling is concerned with the study of the relationships existing between a population and the samples drawn from it (Chisnall 1997). To sample something is to examine a small portion of it, usually to judge the nature and quality of the whole. The techniques used to select participants of the data gathering process fall into two major groups, non-random sampling, and random sampling. In this research, the researcher used a stratified random sampling technique to select the participants within the chosen groups. Random sampling is a sampling technique in which each element in a population has an equal probability of being chosen. A stratified sampling involves dividing the entire population into homogeneous groups called strata. Random samples are then selected from each stratum. The purpose of this study is to propose a CSA framework for universities by identifying key factors that need to be addressed in creating awareness among universities' internet users. Even though exposure and usage of the internet vary among the students doing undergraduate and postgraduate as well as academic and non-academic staff, cyber security involves and affects every member of a university population and with this sampling method, the researcher can represent the entire university population.

#### **4.4 Sample size**

The sample size is a research term used for defining the number of participants included in a research study to represent a population. Determining the sample size is very important in research because if the sample size is too small it will not adequately represent the realities of the population being studied and a large sample size may significantly increase the cost and time for conducting the research. In this study, the total population was divided into 5 different groups which are undergraduate students, postgraduate students, academic staff, Nonacademic staff, and technical staff. These subgroups were created to ensure equal representation of the whole population .

According to UniRank (2020), NUST's 2020 student enrolment stood at 10000 including both undergraduate (8000) and postgraduate students (4000), and the university boasts of 2500 academic staff and 3500 non-academic staff. To calculate sample size, the researcher used a simplified formula for proportions by Yamane (1967) using a 95% confidence level and  $P=.5$ . The calculation formula is sample size=  $N/(1+N(e)^2)$  where N is the population size. Using this formula, the sample sizes to be used are as follows: academic staff (335), non-academic staff (350), undergraduate (364), and postgraduate (350) giving a total sample size of 1360 participants. According to Best and

Khan (1993), a sample is a small proportion of the population selected for observational analysis. As such the researcher used proportionate stratified sampling to come up with a ratio of; 1;7;4;5;5 to get a total sample of 274 as shown in table 1 below. The study employed stratified random sampling selection of participants in each group as this helps to achieve sample representativeness (Durrheim 2002).

Table 1. Sample composition

| Group                  | Population   | Sample size | Sample composition |
|------------------------|--------------|-------------|--------------------|
| Technical staff        | 4            | 4           | 4                  |
| Post Graduate Students | 4000         | 350         | 50                 |
| Undergraduate Students | 8000         | 364         | 100                |
| Academic Staff         | 2500         | 335         | 50                 |
| Non-Academic Staff     | 3500         | 350         | 70                 |
| Total                  | <b>18000</b> | <b>1360</b> | <b>274</b>         |

In this research, a mixed-method research strategy was used (Table 1). The sampling technique used in this research is the stratified random sampling technique to select the participants within the chosen groups. A combination of two data gathering methods namely questionnaires and literature survey, was used. Quantitative analysis methods were used to analyze data. This research study was conducted ethically and the ethical considerations that were made have been given in this chapter.

## 5. Results and Discussion

This study was carried out to examine the level of knowledge on cyber security among university students and staff, evaluate initiatives that developed countries have about cyber security, and also to identify key factors for inclusion in the awareness framework. This chapter will discuss the findings revealed in the previous chapter. Focus is made on discussing the findings of the research about the research questions and comparison with the findings of the literature reviewed.

### 5.1 Numerical Results

This study included 274 participants and a total of 222 responses. This number is made up of 5 groups of participants which included 78 undergraduate students, 45 postgraduate students, 50 academic staff, 70 non-academic staff, and 4 Technical Staff participants.

### 5.2 Validation

In determining reliability of the test, Cronbach alpha was used. This test was applied to 6 questions based on a five Likert scale (1 = “strongly disagree”, 5 = “strongly agree”). When using Cronbach alpha to test reliability of the questionnaire, reliability statistics table gives you your Cronbach’s alpha coefficient. For high internal consistency the score must be over .7 and, in this case,  $\alpha = .7481$ , which shows the questionnaire is reliable and is significant and acceptable for further research. The statements generated a mean score  $> 3$ , indicating a significant level of agreement with the statements.

### 5.3 What is the level of cyber security awareness among university students and lecturers in Zimbabwe?

One of the objectives of this study is to determine the level of cyber security awareness among university students and staff based on key security concepts. As described by NIST Special Publication (SP) 800–16, the use of multifactor authentication is an important way of mitigating cyberattacks. However, in this study, 42% of the respondents did not know what two-factor authentication (2FA) is and an additional 24% had no idea what it was. The study also revealed that 70% had not enabled this mechanism on their accounts when it became available. which

is consistent with the findings reviewed in literature where Alharbi and Tassaddiq (2021) point out that people do not know how to use two-factor authentication and some of those who know do not adopt it because they believe it is annoying to use and difficult to deal with.

The password is one of the aspects considered as a basic and important security aspect that protects data and information and provides access to authenticated systems. Therefore, the researcher examined the students' knowledge of the principles of password security and examined how they manage their passwords. 56% of the respondents used strong passwords which were at least 12 characters and included alphanumeric symbols and 67% did not contain any personal information. Of similar view is the finding on reviewed literature that shows that a strong password should include at least 12 characters long, including alpha and numeric characters, and a mix of both uppercase and lowercase letters with at least one special character, Moallem (2019). However, 43% had a simple password which did not include key characteristics of a strong password. This concurs with the literature reviewed which highlighted that user have the same password for all their accounts, or a simple default password because they sometimes feel that having a strong and long password is not important, Garba (2020). This is an indicator that users are not aware of the importance of strong passwords as a concept of cyber security hence there is a need for awareness and education about the importance of strong passwords cyber security risks that can occur because of their behavior.

Of concern is also a larger percentage of the statements which received 'disagree' and 'Strongly disagree': knowledge about cyberattacks (54%); Phishing and social engineering attacks (71%). These responses implied that the respondents cannot identify phishing email attacks and such knowledge deficits can lead to unsafe practices and can be exploited by cyber-criminals in turn exposing the university to cyberattacks. This concurs with the results obtained from technical staff who indicated that the users have little ability to recognize such threats suggesting the need for CSA in universities. Of the same view are the findings from the reviewed literature which shows that the fundamental concept of cybersecurity is not obvious to many, (Kennison and Chan-Tin 2020) and that most participants do not have the requisite knowledge to identify phishing emails or understand the importance of information security principles and their practical application in day-to-day work.

To determine users' attitudes towards cyber security issues, the research findings show that 25% consider cyber security as something they leave to technical staff to worry about. Of similar view is the reviewed literature of the study conducted by Madyira (2015) which shows that due to lack of knowledge on cyber security concepts, most users consider that cyber security is the role of technical people. This represents an unsafe or harmful attitude. On the same question, 40% indicated that they are aware of the concept of cybersecurity, but they do not know what to do about it. This concurs with the literature reviewed which indicated that participants do not have the requisite knowledge and understanding of the importance of information security principles and their practical application in day-to-day work, and they have no clue what to do in order to 'get safe online'.

The research findings show that 89% of users are being cautious online because of their cyber security knowledge. This however does not correspond with findings of the way respondents behave online where 58% indicate that they have never rejected an app from accessing their data on their devices and 10% would send their personal information to a familiar sender requesting them. This does not show cautiousness on the part of the users, and this indicates an overly trusting behaviour that can be easily exploited by the hackers

Users could not correctly identify situations that would enable a hacker to automatically install a spamming program on their device. This is shown by 23% Incorrect and 35% partially correct answers. This corresponds with the finding in the literature reviewed in this paper that highlights that users' degree of preventative measures is very low Moallem (2019). Evidence from the findings presented shows that students and staff at universities do not have the requisite knowledge and understanding of the importance of cyber security principles, their practical application in their day-to-day activities, and are not aware of how to protect their data. Meaning the level of awareness of cyber risks is very low amongst university students and staff.

#### **5.4 How have developed countries improved cyber security awareness and education amongst users?**

To improve users' safety online, developed countries have digital resource hubs for hosting resources for individuals, families, and businesses. For example, the United Kingdom's National Cyber Security Centre (NCSC), is a single point of contact for all businesses and citizens to report cyber incidents and addresses issues of cyber

security knowledge. United Kingdom's "Get Safe Online", a comprehensive online portal hosting curated resources for individuals, families, and businesses on how to safely navigate the online world. Get Cyber Safe in Canada that addresses users with topics including "how cyber threats work," "how cyber threats affect you," "how to protect yourself online," "how to protect your small business," and "how to work together.

Findings in the literature reviewed show that other developed countries have set aside days/months for national awareness campaigns initiatives for creating awareness among users. For example, "Safer Internet Day" in New Zealand in February has been supported by public organisations, civil society, and private industry. October Cyber security awareness month in the USA, Canada, and Jamaica.

Other countries run cyber security challenges in schools and colleges to provide learning experiences focused on topics such as data sharing, personal information security among others. These challenges provide a series of immersive learning experiences, intended for high school students, focused on topics like data sharing, personal information security, and cryptography. Examples of such countries are Cyprus and Australia run cyber security challenge competitions in schools and colleges. Roadshows and professional development opportunities in New Zealand to help teachers prepare to incorporate the cyber security curriculum in their classrooms. Net Safe in New Zealand focused on promoting awareness of online safety issues facing children and youth. Developed countries recommend that organisations in cyber security comply with internationally accepted standards to protect critical assets against cyberattacks, (Fade, 2020), for example, standards defined in the European Union' Network and Information Security (NIS) and the US National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF). In most developed countries cyber security is among other national priorities and definite steps have been taken in the direction of cyber security both from a strategy and implementation point of view.

### **5.5 How can cyber security awareness and education be improved among Zimbabwean university students and staff?**

This study was objectively meant to investigate how cyber security awareness and education can be improved among users. Data collected from the research finding collaborates with the literature reviewed to determine awareness among students and staff on the issues of cyberattacks. From the literature reviewed universities lack awareness of cyber security concepts as was noted that all respondents (100%) indicated that educational institutions do not have an active approach to cyber security awareness. Findings from this study have shown interest by students and staff to be taught cybersecurity awareness skills and that cybersecurity be incorporated in the programs as highlighted by Garb *et al.* (2020) in a study to establish cyber security awareness at a Nigerian University. This agrees with the response in this study that shows that 92% of users would prefer that universities offer programs that will make users aware of cyberattacks and ways to mitigate them. It is also discovered from the finding of the research that 100% of the technical staff strongly agree that the university should have cyber security awareness and education programs for all internet users.

The findings from this research indicate that the technical staff's proposed ways in which CSA can be incorporated in universities are through the following options:

- Students should be taught about defense mechanisms at first year
- Offer online simulated cyber security teachings
- Mass lectures for everyone students and employees

As equally indicated in the literature review, the success of an awareness program relies on how it is delivered to the user. Students are often presented with cybersecurity awareness and education through games and simulations whereas, organisations through training and mass lectures, Hueca *et al.* (2020). Surveys to determine the most preferred delivery method for awareness and education programs show that 100% strongly agree with simulation delivery method and findings on a video-based show that 75% strongly agree and 25% are neutral about it. Paper-based delivery method shows that 75% strongly disagree and 25% agree to this method. Online methods have 75% agree to it and 25% strongly agree while instructor-led exhibited 50% strongly agree, 25% agree and 25% disagree. Reviewed literature connects well with the research findings in this study whereby it highlights that delivery method and overall awareness program should be relevant to the audience's daily activities. Universities, while pursuing daily activities, they will most definitely be using online platforms in both the academic setting and in their private or personal lives hence a cybersecurity awareness program should be delivered using online platforms, Mierzwa, *et al.*, (2021). To improve cyber security awareness in universities and based on the findings of the study and the review of related literature the next subsection presents the proposed framework.

### 5.6 Graphical Results/ Proposed Framework

Security awareness efforts are designed to change behaviour or reinforce good security practices among users, and it is intended to allow individuals to recognize IT security concerns and respond accordingly. Findings from the literature reviewed show that to come up with a relevant CSA program, start by identifying the audience and identifying awareness needs among the audiences. In this research, findings show that most users are not aware of security threats and vulnerabilities, and how to respond and protect themselves against such threats. Once needs are identified, the next step is to identify role players, assign responsibilities to them and then develop training material that is relevant to the target audience. Choose the delivery method, implement the program, and finally establish processes for monitoring and reviewing the program. Figure 1 shows the proposed framework.

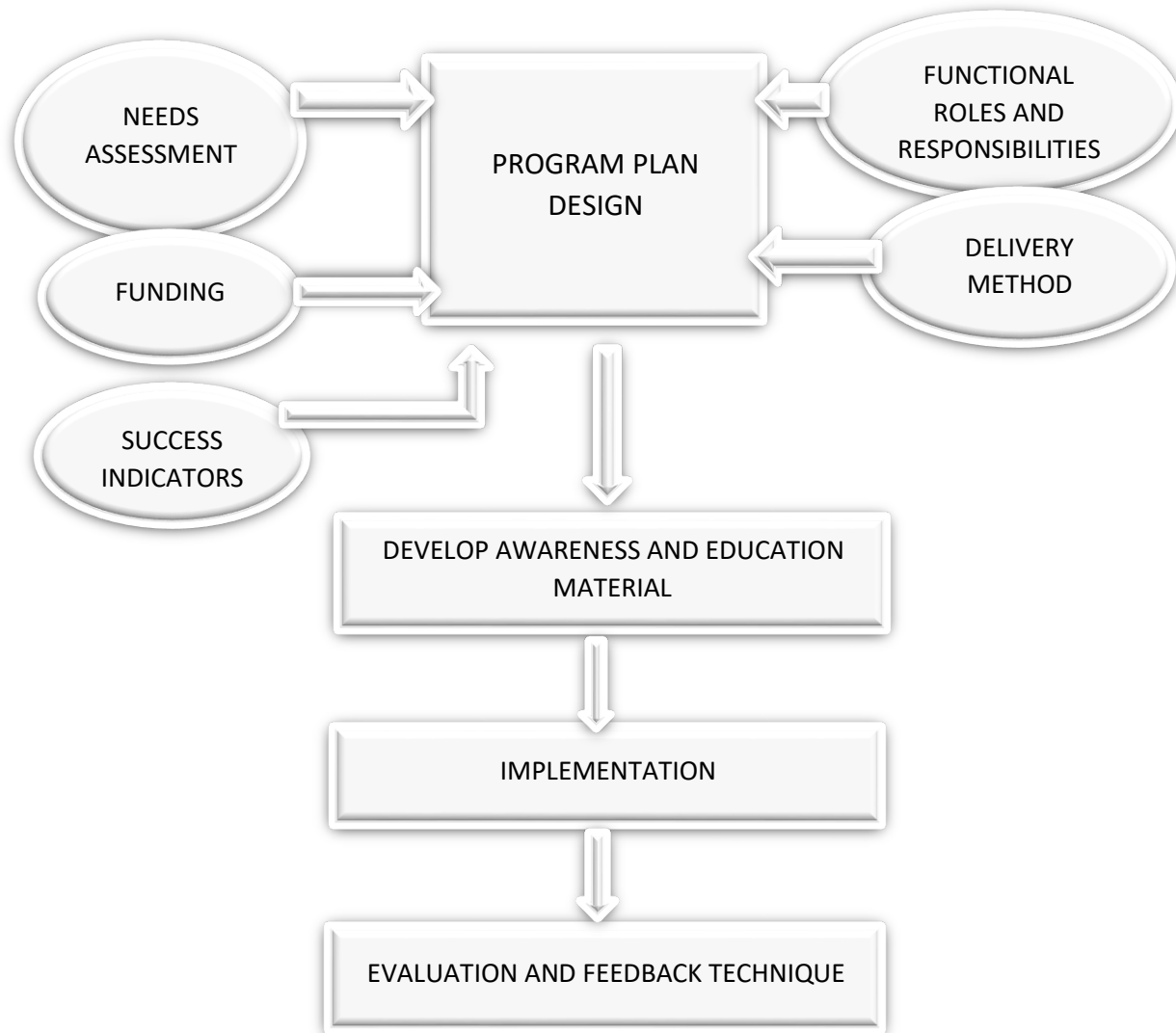


Figure 1. Proposed cyber security awareness and education framework.

These steps can be grouped in four phases to come up with a comprehensive framework:

1. Program plan Design
2. Developing the awareness and training material,
3. Program implementation
4. Evaluation and feedback technique

From the discussion, it is evident that users at the university are not aware of cyber security risks and threats as such there is a need for training and awareness. In the next chapter, the researcher gives a recommendation in relation to the objectives of this research and a proposed framework is drawn from the findings of this research.

## 6. Conclusion and Recommendations

In conducting this research, data were collected from 5 groups of respondents which comprised students, both undergraduate and postgraduate students and staff members. The gist of the research was to determine the level of cyber security awareness and education among the universities students and staff and propose a framework for CSA. Based on the results the following conclusions can be drawn:

- The university staff and students do not know the basic concepts of cybersecurity or of the best practices of protecting themselves from various forms of attack.
- The practice of key principles of online safety is very limited amongst universities. Cautiousness is not practiced, many users still use default or weak passwords, do not use 2FA, and do not hesitate to post their personal information online.
- The students and staff have a desire to learn cyber security concepts for their safety and that of the university.

### 6.1 Recommendations

The Researcher is drawing the following recommendations based on the research findings and reviewed literature as aligned to the research questions of this study. The first recommendation is that universities need to implement comprehensive cybersecurity awareness and training sessions regularly to ensure that all users know how to recognize the most common cybersecurity threats and vulnerabilities. They should promote knowledge on common cybersecurity concepts, including vulnerabilities, attacks, and incidents, to their students and staff to strengthen their security position. The second recommendation is that universities should incorporate cyber security-related activities which address safety practices, vulnerabilities, incidents, and attacks during the induction of employees and orientation of students. This ensures that the users that are being introduced to the data network are well equipped with the issues of security and this will enable users to play their part by interacting safely online hence contributing to the reduction in the cyber security risk of the University. It is also recommended that universities should also make it a routine to occasionally hold symposia, seminars, and public lectures on this topical issue of cyber security. This enables students and staff 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 universities but is also an effort that will help in controlling this scourge in the Zimbabwean context. There is a need to integrate more proactive methods, such as training and interviews. A combination of both methods would be more effective and highly recommended. The delivery methods for cybersecurity awareness and training programs can be video-based, text-based, or game-based, as the target here is adult students. Security awareness must be taught at an early age to develop sustainable cybersecurity behavior among users.

The research involved conducting a study at one university to ascertain the current level of cyber security knowledge of both students and staff and propose an awareness and education framework on cyber security concepts, risk, and vulnerabilities. The objectives that were set were met. Answers to the research questions were obtained from the data that was gathered. These answers included the current level of knowledge, skills, attitude, and behaviour of users online and ways in which cyber security awareness and education can be incorporated in Zimbabwean universities. The challenges that were identified assisted the researcher to suggest ways in which available knowledge, skills, and behavior of students and staff, about cyber security can be improved. Finally, a framework for implementing cyber security awareness in universities was proposed.

## References

- Alhamad, H. and Donyai, P. , The Validity of the Theory of Planned Behaviour for Understanding People's Beliefs and Intentions Toward Reusing Medicines. London: Academic Press, 2021.
- Alharbi, T. and Tassaddiq, A. , Assessment of Cybersecurity Awareness among Students of Majmaah University. *Big Data and Cognitive Computing*. Oxford: Oxford University Press, 2021.
- Al-Janabi, S. and Al-Shourbaji, I, A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & Knowledge Management*, 15(01), p.1650007.2016.
- Al-Janabi, S. and Al-Shourbaji, I, A Study of Cyber Security Awareness in Educational Environment in the Middle

- East. *Journal of Information & Knowledge Management*, 15(01), p.1650007.2016.
- Newton, A. (2021). Data Visualization & Analytics. *BI Blog*. Available at: <https://www.datapine.com/blog/data-analysis-methods-and-techniques/#definition>. [Accessed 28 August 2021]. .2021
- Chandarman, R. and Van Niekerk, B., Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. *The African Journal of Information and Communication*, (20), pp.133-155, 2017.
- Composition des Publications , *Cybersecurity guide for developing countries*. Available at: <http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-e.pdf>. [Accessed 28 Aug. 2021], 2017.
- Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., and Sheikh, A. (2011). The case study approach. 10<sup>th</sup> ed. New Jersey: Pearson, 2011.
- de Joode, A. , Effective corporate security and cybercrime. *Journal of Systems and Network Security*, 2011(9), pp.16-18, 2011.
- Dudovskiy, J. , *Positivism - Research Methodology*. Research-Methodology. Available at: <https://research-methodology.net/research-philosophy/positivism/>. [Accessed 2 Aug. 2021], 2009.
- Efthymiopoulos, M.P. ,A cyber-security framework for development, defense, and innovation at NATO. *Journal of Innovation and Entrepreneurship*, 8(1), 2019.
- Feigl, H, Positivism. Definition, Characteristics, History, & Facts. In: *Encyclopædia Britannica*. Available at: <https://www.britannica.com/topic/positivism>. [Accessed 3 Aug. 2021], 2018.
- Garba, A., Maheyazah, B, Siti. H and Dauda. I. (2020). Cyber Security Awareness Among University Students: A Case Study. *Journal of Science Proceedings Series*, 2(1), pp.82-86, 2020.
- Geer, D. (2015). Six Key Areas of Investment for the Science of Cyber Security. New York: Berghahm Books, pp 10-15, 2015.
- Glen, S., *Cronbach's Alpha: Simple Definition, Use and Interpretation*. Available at: <https://www.statisticshowto.com/probability-and-statistics/statistics-definitions/cronbachs-alpha-spss/>. [Accessed 30 Aug. 2021], 2021.
- Grant, C. and Osanloo, A, Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for Your "House". *Administrative Issues Journal Education Practice and Research*, 4(2)., 2014.
- Hall, C. , Security of the internet and the known unknowns. *Communications of the ACM*, 55(6), pp.35–37, 2012.
- Hunt, T. , *Cyber Security Awareness in Higher Education*. Central Washington University: Scholar Works. N.D.
- Kabanda, G. , Bayesian Network Model for a Zimbabwean Cybersecurity System. *Oriental journal of computer science and technology*, 12(4), pp.147–167, 2020.
- Kabdul P. , Cyber Risks in Electronic Banking: Exposures and Cybersecurity Preparedness of Women Agro-entrepreneurs in South- South Region of Nigeria. *Journal of Business Diversity*. 20(3), 2020.
- Karyda, M, Fostering Information Security Culture in Organizations: A Research Agenda. *MCIS 2017 Proceedings*. Available at: <https://aisel.aisnet.org/mcis2017/28>. [Accessed 28 Aug. 2021], 2017.
- Kennison, S. and Chan-Tin, E. , Taking Risks with Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. London: Macmillan Press.
- Kortjan, N. ,*A Cyber Security Awareness and Education Framework for South Africa*. Available at: <https://core.ac.uk/download/pdf/145053774.pdf>. [Accessed 28 June. 2021], 2013.
- Kortjan, N. and Von Solms, R. (2014). A conceptual framework for cyber security awareness and education in SA. *South African Computer Journal*, 52, 2014.
- Kritzing, E. and von Solms, S.H. ,Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security Journal of South Africa*, 29(8), pp.840–847, 2010.
- Kshetri, N. and Nir, F. , Cybersecurity and Development. *Markets, Globalization & Development Review*, 1(2), p.3. Available at: [https://libres.uncg.edu/ir/uncg/f/N\\_Kshetri\\_Cybersecurity\\_Development\\_2016.pdf](https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Cybersecurity_Development_2016.pdf). [Accessed 2 Sep. 2021], 2016.
- LaMorte, W. , *The Theory of Planned Behavior*. [online] sphweb.bumc.bu.edu. Available at: <https://sphweb.bumc.bu.edu/otlt/MPH-Modules/SB/BehavioralChangeTheories/BehavioralChangeTheories3.html>. [Accessed 2 Sep. 2021], 2019.
- Madyira, F. F. , Social technologies and cyber security challenges in Zimbabwean universities: A case of the University of Zimbabwe. (Unpublished Masters thesis). University of Zimbabwe, 2015.
- Moallem, A., , Cyber Security Awareness Among College Students. *Advances in Intelligent Systems and Computing*, pp.79-87, 2018.
- Veale, M. and Brown, I. , Cybersecurity. *Internet Policy Review*. 9(4). , 2020 <https://policyreview.info/concepts/cybersecurity>
- von Solms, R. and van Niekerk, J., From information security to cyber security. Canberra: ABARE, 2013.

## Biography

**Dr. Sibusisiwe Dube** is a lecturer in the Computer Science Department at the National University of Science and Technology in Zimbabwe. She is a Ph.D. holder in Information Systems from the University of Cape Town in South Africa. She has an h-index 5 and i10-index 3. She holds a Master of Science in Information Systems from the National University of Science and Technology in Zimbabwe and a Bachelor of Science Honours Degree in Information Systems from Midlands State University. She has over 10 years of experience in the academic sector and has published in several accredited journals and conferences. Her research interests are in the Paradox of the second-order digital divide in a high literate country's higher education institution, ICT4D, Digital divide, ICT in education. Research Awards: NUST RIO grant 2014, 2016; UCT conference travel funding, 2016.

**Belinda Mutunhu Ndlovu** is a lecturer in the Computer Science Department at the National University of Science and Technology in Zimbabwe. She is also a Ph.D. in Information Systems student at the University of South Africa. She holds a Master of Science in Information Systems, Bachelor of Science Honors Degree in Computer Science, Post Graduate Diploma in Higher Education all from the National University of Science and Technology in Zimbabwe. Belinda has over 7 years of experience in the banking, telecommunications, retail industry as a Software Consultant. She holds international certifications in Java, Mobile Application Development, WebSphere Portal, and Webservices. She has 5 years of academic experience, and her research interests include ICT4D, 4IR, and Health Informatics.

**Nolwazi Ncube** is a tutorial assistant in the Computer Science Department at the National University of Science and Technology in Zimbabwe. She holds a Bachelor of Science Honors Degree in Computer Science from the National University of Science and Technology in Zimbabwe. She is currently pursuing a Master of Science in Data Science.

**Sizalobuhle Sibanda** is a Master of Science in Information Systems student at the National University of Science and Technology in Zimbabwe