Assessing Cyber Security Awareness and organisational preparedness on cyber security in audit firms: The case of the big 4 audit firms -EY, Deloitte, KPMG, PWC [2017 – 2020]

DR DAVID FOYA, +263 772 935084, foyad1965@gmail.com, David.foya@nust.ac.zw ,Department of Business Management, National University of Science & Technology; Zimbabwe

2. Pride Chifodya, + 263 77 212 5138; pridechif1@outlook.com ; UNDP, P. O Box Harare, Zimbabwe

Abstract

The study looked at the level of awareness and state of preparedness for organisations on cyber security. The main objective of the research was to determine the impact of cybersecurity awareness and preparedness of organisations on the security behaviours of employees. Research questions was what is the level of preparedness of organisations in response to cybercrime/attack. The study was significant as it brought out suggestions on critical issues identified on cyber security. The research adopted the qualitative approach as it sought to assess human behaviour in relation to awareness. The interpretivism philosophy was used as well as the multi case study research strategy. The researcher used interviews and questionnaires for data gathering. The major findings of the research where that the firms where ill prepared with regards to cyber security. Another major finding was that the employees where not really aware of the subject understood Resources are dedicated to aspects of the business that authorities deem more important. The researcher recommended that the firms conduct more frequent security awareness programs so that this influences the security behaviour of employees in a positive way. It was also a recommendation that the firms invest in the requisite skill sets to effectively address cyber security issues.

Keywords: **cyber security, awareness, cybercrime, preparedness, firms, hacking, breach, behaviour**.

LIST OF ACRONOMIES

EY ……………………………..	Ernest and Young
KPMG …………………………	Klynveld Peat Marwick Goerdeler
PWC …………………………...	PricewaterhouseCoopers
IT ………………………………	Information Technology
ICT ……………………………	Information Communication Technology
ISS ……………………………..	Information Systems Security
IFAC …………………………...	International Federation of Accountants

ICAZ …………………………...Institute of Chartered Accountants of Zimbabwe

ICAEW ………………………...Institute of Chartered Accountants of England and Wales

ISO ……………………………..International Organisation for Standardization

COBIT …………………………Control Objectives for Information Technologies

VPN ……………………………Virtual Private Network

MAC …………………………..Media Access Control

1 Introduction and background of the study

Cyber security is the art of protecting computers, systems and networks from both internal and external attack. Grustniy (2019), defines cyber security as the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Cyber security is also known as information technology security or electronic information security and focuses on keeping software and devices free of threats. Mehio (2019) states that to avoid possible data theft and hacking, employees of all companies should be oriented on how to be safe online. The key is to instil constant vigilance and promote awareness of the biggest cons of the internet. Mehio (2019) further states that cybersecurity is a global phenomenon representing a complex socio-technical challenge for governments, but requiring the involvement of individuals. Although cybersecurity is one of the most important challenges faced by organisations in present day, the visibility and public awareness remains limited. A lot of people have heard of cybersecurity, however, the urgency and behaviour of persons do not reflect high level of awareness.

In the late 1990s - 2000 most of the initial computer-based attacks were in the form of computer worms and viruses primarily intended to gain notoriety for the malicious code author and to expose vulnerabilities of popular software and hardware makers in order to embarrass them. While these attacks could result in lost data, service interruptions, and lost productivity, they were mostly seen as simple acts of vandalism and great annoyance. These kinds of problems made the job of system security more of a technological problem that focused on vulnerabilities rather than on threats, which eventually led to the now endless cycle of software and firmware updates and patches. Now that there are more purposeful attacks by criminal, terrorist, and state-sponsored threat actors, the human motives and goals of malicious cyber behaviour must be considered in formulating cybersecurity strategies.

The prominence of technology has made management of information a lot easier but there is a gloomier aspect of this. With the world more connected and increased reliance on information technology, businesses have increasingly become vulnerable to cyber-attacks and in the process lose their greatest asset which is information. According to Madondo (2017), as numerous prominent incidents in the recent past show deficits of organisations' information systems security (ISS), they can have severe consequences for society and the economy. A PWC (2018) report states that cyber-attacks from inside the company as well as insider threats and unintentional behaviour committed by employees can cause a broad diversity of damage such as financial loss, loss of customers or business partners, decrease of the firm's market value, loss of reputation or even governmental sanctions.

A recent estimate by the Centre for Strategic and International Studies (CSIS), a think tank, cybercrime and intellectual property theft causes an annual global loss of $445 billion, a sum that roughly equals the GPD on one wealthy European country such as Australia (The economist 2014). It is against this background that cybersecurity awareness has been identified to be one of the most essential prerequisites of information security behaviour and to play a key role in employees' policy compliance. Nurse (2019) state that, past and current efforts to improve information security practices and promote a sustainable society have not had the desired impact. He further states that it is important, therefore, to critically reflect on the challenges involved in improving information security behaviours for citizens, consumers and employees. It is thus, important to consider the challenges from a psychology perspective as it is believed that understanding how people perceive risks is critical to creating effective awareness campaigns. Changing behaviour requires more than providing information about risks and reactive behaviours, hence firstly, people must be able to understand and apply the advice, and secondly, they must be motivated and willing to do so, therefore, the latter requires changes to attitudes and intentions. These antecedents of behaviour change are identified in several psychological models of behaviour (Nurse 2019).

With cyberspace growing at a speed unprecedented by any other commodity, almost 3 billion people are now connected to cyber space through the internet; a figure growing rapidly and expected to reach five billion people, using 50 billion devices by 2020 (Muller 2015). Muller further states that as most of this growth will take place in emerging economies, it is not surprising that the development community is pondering how to leverage the benefits accruing from the use of cyberspace and information and communication technologies (ICTs) through cyber capacity building (CCB). Muller also states that this exercise will however be futile if not backed up by a serious discussion about the need to address the challenges posed by the proliferation of ICT infrastructure and internet applications for sustainable development. This therefore, brings to life the importance of cyber security awareness and preparedness for organisations.

According to Majome (2017), the then Ministry of ICTs, Postal and Courier Services in 2013 drafted the Cybercrime and Cybersecurity Bill in an attempt to keep up with global trends, as it is now necessary for all countries to come up with laws that classify and deal specifically with cybercrimes for, without dedicated statutes, there will be no legal mechanisms on which to prosecute the cybercriminals. This shows how as a country cyber security is being treated and it is also against this background that the researcher wishes to understand the level of preparedness of organisations in the audit industry on cyber security. With the internet now a place where people are involved in all sorts of activities, hackers, criminals and destructors find it as a place to do their operations and as such putting many companies at risks. Many organisations have sensitive data which they cannot afford to lose to "bad guys" and with the different types of attacks that organisations are prone too, it triggered the researcher to assess on the preparedness of organisations for such occurrences and whether or not employee awareness is a contributor to the rising cases of cybercrime.

Another factor which acted as a trigger for the researcher to assess organisational preparedness in terms of cyber security is first-hand experience of the researcher where an organisation that he is closely affiliated to was hacked and cost the organisation RTGS$50 000. This raised questions to the researcher on issues of cyber security awareness within employees and its impact on cybercrime.

1.2 Statement of the problem

Zimbabwean institutions have suffered a lot of cybersecurity breaches mostly being government institutions and universities. The audit industry has not been spared as audit firms are facing an increase in cyber-attacks as criminals switch their focus to 'softer targets' and therefore are at particular risk due to the high level of confidential data and valuable financial information they hold. With the rise in cybercrime in Zimbabwe a lot of data and ICT systems are compromised and as result millions of dollars are lost. It is therefore, against this background that the researcher wishes to assess the level of cyber security awareness and preparedness in audit firms and to what extent it affects the security behaviour of employees.

1.3 Objectives of the study

Primary objective

To determine the impact of cybersecurity awareness and preparedness of organisations on the security behaviours of employees.

Secondary objectives of this study are to:

- Assess the attitude/perceptions of employees towards cyber security.

- Evaluate the level of preparedness of organisations in response to cybercrime/attack.
- Examine the effectiveness of cyber security awareness programs in combating cybercrime.
- Examine on the factors that influence adoption of cyber security tools.
- Assess the measures which organisations have put in place to secure their data, computers and networks.

2.0 Interim literature review

2.2.1 Cyber Security

The Committee on National Security Systems (2012) defines cybersecurity as the ability to protect or defend an enterprise's use of cyberspace from an attack, conducted via cyberspace. This is for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure with an intention of destroying the integrity of the data or stealing controlled information. The International Organization for Standardization (2015) on the other hand defines cybersecurity or cyberspace security as the preservation of confidentiality, integrity and availability of information in the cyberspace. In turn, "the Cyberspace" is defined as the complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form. According to Bashay (2018), it is important to guide information security policies within a company. He states that the CIA is one model that can be used for this. The three elements of CIA triangle are confidentiality, integrity and availability which are considered the three most important components of cyber security. According to the model, confidentiality is the security principle that controls access to information. It is designed to ensure that wrong people cannot gain access to sensitive information while ensuring the right people can access it. Integrity assures that sensitive data is trustworthy and accurate. Consistency, accuracy, and trustworthiness of data should be maintained over its life cycle. Sensitive data should not be altered in transit, and security measures, such as file permissions and user access controls, should be taken to make sure that it cannot be modified by unauthorized users. Availability is the guarantee of reliable and constant access to your sensitive data by authorized people. It is best guaranteed by properly maintaining all hardware and software necessary to ensure the availability of sensitive data. The CIA model is presented in the figure below;

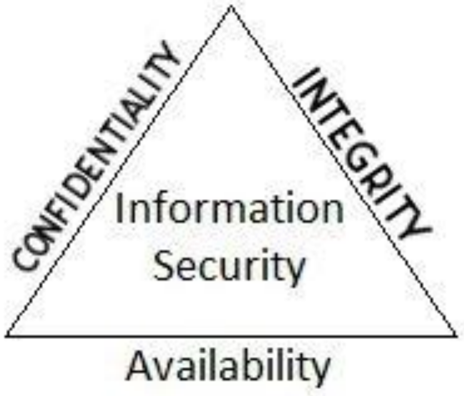


Figure 2.1 Information Security Goals (CIA Triad) (Hilton 2012)

2.2.2 Cybercrime

Tischer (2016) states that cybercrime is used to describe a wide range of offences against computer data and systems such as hacking, computer related forgery and fraud such as phishing, content offences such as disseminating child pornography and copyright offences such as the dissemination of pirated content. Cybercrime has been seen to have evolved from the mischievous one-upmanship of cyber vandals to a range of profit-making criminal enterprises in a remarkably short time

2.2.3 Cyber security awareness

According to Martin (2014), security awareness is knowledge combined with attitudes and behaviours that serve to protect our information assets. Being cybersecurity awareness means, you understand what the threats are and you take the right steps to prevent them. Nurse (2019) agrees with this position by stating that “And the sad truth is that few of these criminals can be described as experts or masterminds. The lack of awareness about cyber security makes most organisations an easy target for anyone trying to hack into their systems.” Nurse (2019) states that an employee awareness and training program tends to address policy, procedures and learning consists of three key elements:

1. Awareness, which is used to stimulate, motivate, and remind the audience what is expected of them.

2. Training, the process that teaches a skill or the use of a required tool.

3. Education, the specialized, in-depth schooling required to support the tools or as a career development process.

Nurse (2019) asserts that operating systems and programmes are more protected these days and attackers have shifted their attention to human elements to break into the organisation's information systems. He further suggests that as the number and frequency of cyber-attacks designed to take advantage of unsuspecting personnel are increasing, the significance of the human factor in information security management cannot be understated. Lee (2017) strongly agrees with the view as he argues that in order to counter cyber-attacks designed to exploit human factors in the information security chain, information security awareness with an objective to reduce information security risks that occur due to human related vulnerabilities is paramount. With cyber threats increasing exponentially, breaches are no longer a matter of “if,” but “when.” Zimbabwe Cyber-Security (2019) states that if there are vulnerabilities in your system, chances are hackers will find them. It is therefore up to you to make sure you are aware of your weak spots and fix them before the bad guys find them and exploit them. Lee (2017) further agrees with this notion as he states that when an enterprise's employees are cyber security aware, it means they understand what cyber threats are, the potential impact a cyber-attack will have on their business and the steps required to reduce risk and prevent cyber-crime infiltrating their online workspace.

Tischer *et al* (2016) state that it is crucial to ensure employees understand their role in protecting data and IT systems. A common hurdle is employees’ belief that data security is something the IT department handles yet some of the greatest vulnerabilities are human, not technological. He further gives an example of typical of hackers referred to as ‘social engineers’ who specialise in manipulating employees to divulge sensitive information. This type of attack doesn’t require a computer, it’s simply a conversation between the hacker and the employee. Undeniably, employees have a critical role to play in securing company information and this can be achieved through effective awareness programs. Tischer *et al* (2016) also support this notion by stating that the subtle danger is that employees will think of data security like fire drills, important but not something they do every day. To change this perception, organisations need to demonstrate that security is a priority from the top down and bottom up hence the importance of awareness.

Furthermore, Lee (2017), states that in order to protect businesses from staff related breaches, businesses undertake security training for employees, with the more serious ones doing it on an ongoing basis and not simply at the point of joining the organisation. Some organisations also test employees, for example sending fake phishing emails, or do physical checks to identify passwords written down and left unhidden or screens that are unlocked. Employees are often obliged to read and accept security policies on an annual basis.

Kingstone and Charles (2019), however, look at awareness from a different perspective. They state that organisations also need to rethink their approach to cyber security training more radically to improve their results. Training is often generic and does not connect good practices with the specific business imperative for following them. Typically, all employees go through some training although specific roles are likely to require very different levels of cyber risk awareness and training. They further give an example of the following; those handling customer data or sensitive commercial data will need high levels of awareness and care in their day-to-day jobs and therefore detailed training may be needed., those in finance functions may be subject to specific attempts of social engineering and fraud on which training could particularly focus whilst others in the organisation may just need general awareness of good security practices.

Khan *et al* (2011) suggest that it is important to measure the effectiveness of information security awareness tools in order to get a comprehensive understanding on the influence these have on employee security behaviour. These methods include, educational presentations, e-mail messaging, group discussions, newsletter articles, video games, computer-based training as well as posters. Khan et al (20111) further give an overview of the five-step ladder model for measuring effectiveness of information security awareness campaigns. There is the knowledge about the information security which influences the attitude towards information security then normative beliefs towards information security, intention for information security and lastly the information security behaviour. The steps are represented in the figure below;

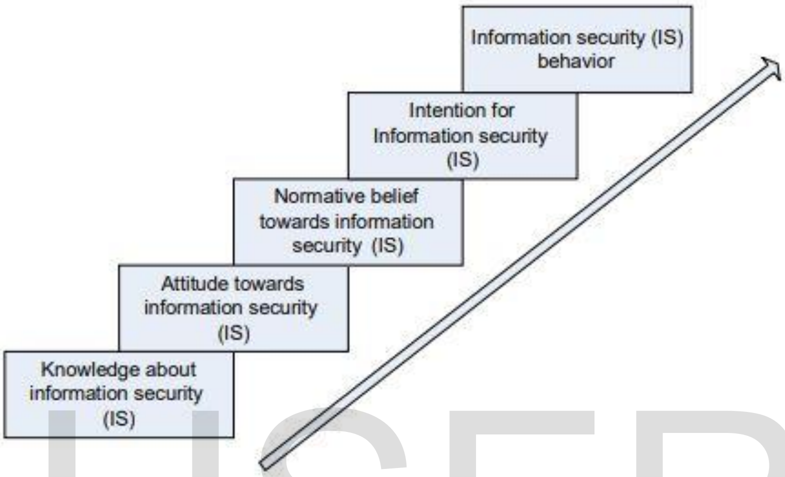

Information security (IS) behavior
Intention for Information security (IS)
Normative belief towards information security (IS)
Attitude towards information security (IS)
Knowledge about information security (IS)

Figure 2.2 Five step ladder model for measuring information security awareness (Khan et al 2011)

2.2.4 Organisational preparedness

Lee (2017) defines organisational preparedness as the ability of providing new measurements of security manager perceptions associated with organisational cyber security readiness. He further states that according to the Health Belief Model (HBM), cyber security preparations would be influenced by security managers' perceived threats of cybercrime and their perceived barriers to making cyber security preparation. Allan (2013: 3) states that "The question is not 'if' your company will be breached, or even when. It has already happened. On the other hand, Hospelhorn (2018), stresses that for organisations to be adequately prepared, they have to do the basics well. This includes investing in effective firewalls, threat detection and anti-virus/malware technologies and management tools that force staff to use strong passwords when accessing business systems. The author, however argues that more important than the capabilities of any security function is the need to keep software up to date with patches and upgrades for all the technology used in the organisation to prevent attackers targeting known vulnerabilities. Janssen (2017) further argues with this view by asserting that ensuring that staff are aware of security issues and support best practice is arguably much more difficult than implementing technical changes. He states that "most data breaches can be traced back to a moment of carelessness or stupidity".

According to Kingstone and Charles (2019), there are three different levels in the organisation to be effectively prepared cyber security wise. The first line is at an operational level, with controls built into processes and local management responsible for their operation in practice thus identifying and managing risks on a day to day basis. The second line is at functional specialism level, for example the role of cybersecurity specialists and a chief information security officer thus providing oversight and expertise. The third line is at the level of internal audit functions or independent assurance providers thus providing assurance and challenge concerning the overall management of the risks.

Jay (2019) states that a survey that sort to find out the state of cyber preparedness of organisations in the United States revealed that 54% of cyber security professionals don't have the tools they need to combat cybercrimes, 55% can't react quickly enough to limit damage, 79% of professionals believe that their organisations cannot access insights to prioritise their response, and 4 in 5 of them believe a breach or a cyber-attack will affect normal functioning of their organisations. Jay further states that the above challenges dramatically impact the ability to defend organisations from cybercrime as they are inadequately prepared therefore unless they are addressed quickly, will expose businesses to significant cyber threats.

Mwila and Lubobya (2018) strongly assert that many organisations are ill prepared as their state that the lack of preparation is magnified by the fact that only 25% of organisations test their cyber security response to a major incident annually. Jay (2019) also supports the view above as he states that organisations do not regularly map their networks and even if they do, they do so with significant time lags. Such delays not only affect the confidence of cyber security professionals in their networks' security, but also keep security flaws hidden from their attention. They further state that over half of all IT decision makers said that they don't test their cyber security response as they are either resource intensive, not part of their budgets or take too much time to complete.

2.1 Cybersecurity in Zimbabwe

Madondo (2017) asserts that Zimbabwe is one of the countries that have been affected by the emergence of cybercrime/attacks. He argues that the main challenge for Zimbabwe is that there is no cyber security in place hence making Zimbabwe very vulnerable to cybercrime. He further notes that Zimbabwe has witnessed significant growth of the internet giving birth to cybercrime in the country with statistics showing a penetration rate of 50% in 2016, according to the Postal and Telecommunications Regulatory Authority of Zimbabwe POTRAZ (2017). Kabata (2018) however disagrees with this view that there is no cyber security in place in Zimbabwe by stating that cyber security measures are being put in place by different organisations but these are inadequate and hence the need of cultivating a culture of cyber security in organisations. He further argues that the lack of a framework to provide direction, focus, guidance and a standardised way of addressing cybersecurity issues in Zimbabwe is one of the challenges being faced in the ICT industry.

Zimbabwe has suffered a number of cyber security breaches on various institutions mostly being government departments. According to the Reserve Bank of Zimbabwe (RBZ) (2015), cybercrime is listed as one of the crimes contributing to the US$1, 8 billion estimated illicit proceeds generated from criminal activity annually in Zimbabwe. RBZ (2015) states that of the 140 cases of cybercrimes reported, 20 where on phishing, 13 on credit card fraud, 10 on identity theft, 24 on unauthorized access, 72 on hacking and 1 case on telecommunications piracy. These statistics are evidence of Zimbabwe's vulnerability to computer and cybercrimes and thus the pressing need for organisations to be well prepared.

According to Njanjamangezi (2014), Munyaradzi Gwatidzo the Chief Executive Officer of Astro mobile also agrees that Zimbabwe is ill prepared on cyber security as he asserts that more than 90% of organisations in Zimbabwe are exposed to cyber security risks. This has been as a result of many factors chief among them being the poor economic performance being experienced in the country prompting organisations to fail to acquire equipment and training that can cushion themselves against these risks.

Madondo (2017) highlights that the Ministry of ICTs, Postal and Courier Services in 2013 started to draft the Cybercrime and Cybersecurity Bill in a bid to curb cybercrime and have legislation that allows for prosecuting those who violet the bill. Madondo (2017) further asserts that the bill was an attempt to keep up with global trends, as it was at the time necessary for all countries to come up with laws that classify and deal specifically with cybercrimes for, without dedicated statutes, there will be no legal mechanisms on which to prosecute the cybercriminals. Majome (2017) however strongly disagrees with Madondo on the purpose of the bill as she argues that the Zimbabwean government had ulterior motives as the bill was drafted to infringe the rights of its citizens and ensure that the government of the day had control over its citizens and what they could say.

According to the Zimbabwe Democrats Institute ZDI (2018), the Cybercrime Bill's envisioned purpose was to focus more on criminalising social media use and giving the state interference and surveillance powers. It therefore has little or no focus on the need for protecting individual liberties or accountability in the processes of combating cybercrime. According to the ZDI (2018), the absence of expressed intention to safeguard basic human rights raises fears that the Cybercrime Bill was solely intended to police internet use at the expense of people's freedom. Majome (2017), further concludes that the Cybercrime Bill has, in fact, an adverse impact on the human rights entitled to the citizens of Zimbabwe.

2.5 Importance of Cybersecurity

Pribanic (2018) argues that cybersecurity is important to all businesses and as such should be taken seriously as it has immense benefits for not only companies but also their employees. He however argues that despite the important of cyber security, organisations do not like to talk about it but security breaches are constantly happening to businesses, sometimes multiple times a month. The importance of cybersecurity for a business is not just about their information being protected but also the information of their employees and customers. With companies having a lot of data and information on their systems it adds to the importance of security, whether it is data security, information security or cybersecurity in general.

Patel (2019) strongly argues that with regards to cybersecurity, it is important for a company to not only train and inform the high level employees but every employee, of the benefits of cybersecurity. Pribanic (2018) strongly agrees with the view above as he further argues that when a company trains all of its employees about the benefits of cybersecurity, the company itself has less exposure to cybersecurity risks in the first place. A company will save money with cyber related loss and severity of cybersecurity incidents when they offer their employees proper cybersecurity training. Pribanic (2018) further states that another benefit of training employees is the time saved thus when a company has fewer cybersecurity threats, the employees of that company will spend less time tracking down the threat, fixing it and possibly having to redo any affected work. Patel (2019) therefore concludes that a well trained work force develops a more positive company culture with regards to cyber and information security.

Patel (2019) on the other hand in contrast to Pribanic (2018), looks at the importance of cyber security not only on protecting sensitive data but also improving the speed of systems. He states that one of the reasons why cyber security is important in modern day society is that it holds a major impact in improving your cyber speed. This is so because probable cyber threats for your system such as viruses or malware end up not only stealing sensitive information but in reducing the speed of your systems as well. This is one major reason for an enterprise to lose clients because as soon as a user notices that your system is intolerably slow for them, they might drop the idea and desire to use the same system again. Warner (2019) however differs with this view as he states that clients are more interested in the service provided despite the speed of the system. He strongly argues that efficiency of a system depends on a number of factors which may include poor connection from the clients' desk. Warner (2019) therefore concludes that users are not likely to abandon a service that they can acquire online because the system is allegedly slow. People are more interested in the service and not the way they acquire the service.

3.0 Research Methodology

The researchers adopted the qualitative approach in this study as the study encompasses human interaction relationships. The choice of the qualitative approach was necessitated by the fact that the researcher wanted to provide a comprehensive research detailing human relational data. The study adopted the case study research design because it is considered to be the best fit where issues of human relation data are concerned. Basically, a case study is an in depth study of a particular situation rather than a sweeping statistical survey. The researchers adopted the interpretivism approach as this study looked at the perceptions of employees towards cyber security and also the impact/relationship between awareness and security behaviours of employees. The researcher targeted both ICT personnel and non

ICT personnel as the population. The total population comprised of four ICT staff from the four firms (Deloitte, EY, KPMG, PWC) and a total of 360 non ICT personnel for the four firms.

Sampling Techniques

The researchers employed the convenience sampling technique for the non ICT staff as this technique allowed him to select his respondents from those who were available at the time of study. Purposive sampling therefore selects participants according to the needs of the study or it deliberately selects a certain group which possess similar attributes. The study used purposive sampling on the ICT staff as the researcher deliberately wanted to interview the ICT managers so as to find out how well their organisations are prepared for cyber-attacks and what motivates or influences them in adopting certain technologies that help combat cybercrime.

The researchers used a combination of questionnaires and interviews in the collection of data from the respondents. The researchers used WebEx and Zoom meeting platforms which allowed for the sessions to be recorded in administering the interviews. This allowed the researcher to carefully analyse the data collected without any distortions.

4.0 Findings

The purpose of this section of the paper is to present the detailed findings of the research as well as an analysis and interpretation of the data collected.

4.2.1 Participants age range

The age range of respondents who participated the most the in research is the 21-30 years' group. 66.7% of the 254 respondents belonged to this age range. In audit firms, the majority of employees are those training to be Chartered Accountants and therefore this is the reason why the age range of 21-30 has the highest responses. Students on average leave University at the age of 22/23 years and then are absorbed in training firms from that age to about 27 when they complete their training. This therefore means that in the audit firms the majority of employees are still in their youthful age and this is an important aspect in the nature of responses and discoveries made during the research. The other age range of 31-40 years made up the second highest number at 30.3% of the total responses. The least number of respondents came from the 41-50 years' group contributing 3% of the responses. The researcher therefore throughout his research managed to gather information from three age groups which are 21-30 years at 66.7%, 31-40 years at 30.3% and 41-50 years at 3%.

With cyber security being a fairly new topic in Zimbabwe, it is therefore a topic that seems to be common within the younger generation and this is proved by the age demographics which show that only people between 21-40 years took part in the study. The higher age group could have just ignored the questionnaire soon after they noticed that the subject understudy is not really of their interest and that they maybe do not possess the right knowledge to complete the questionnaires. On interviews the researcher managed to gather data from four IT managers from Deloitte, KPMG, EY and PWC. These where aged 36, 42, 39 and 41 respectively. These where targeted because of their specialised IT skills and knowledge.

The chart below summarises the demographics analysed above.

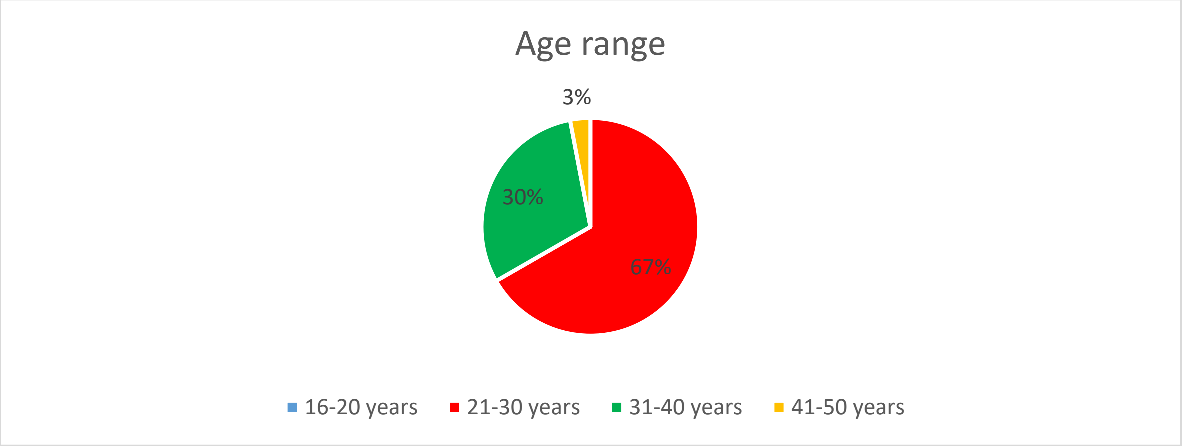


Figure 4.1 Respondents age range

4.2.2 Questionnaire response rate

The researchers managed to distribute a total of 90 questionnaires including an online version to each firm. The total responses received from all the firms from both the physically distributed questionnaires and online questionnaires are shown in the histogram below:

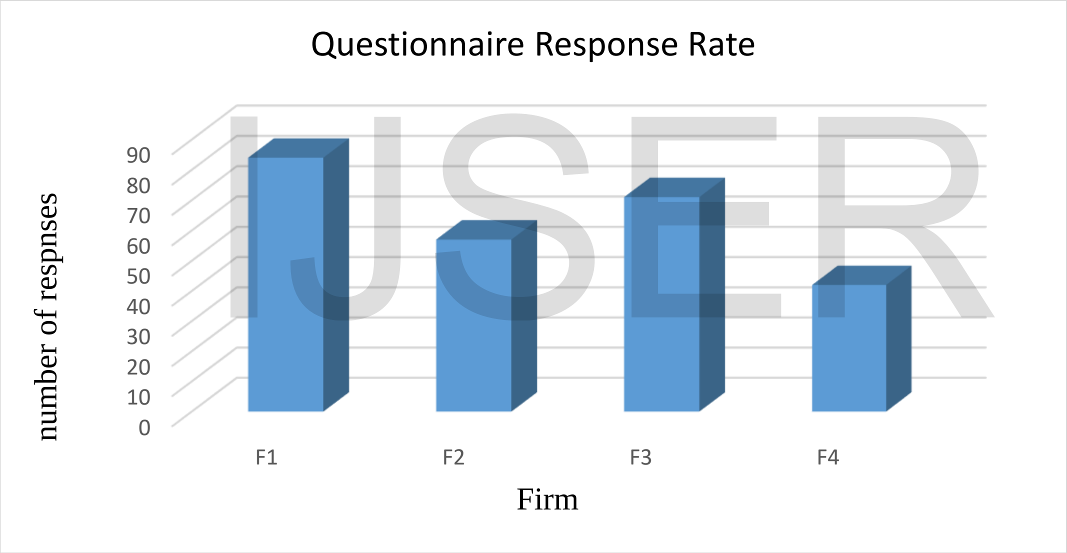


Figure 4.2 Total responses received from questionnaires

The table below shows in detail the total number of physical questionnaires returned to the researcher and total number of those completed and submitted online.

Table 4.1 Detailed questionnaire response rate

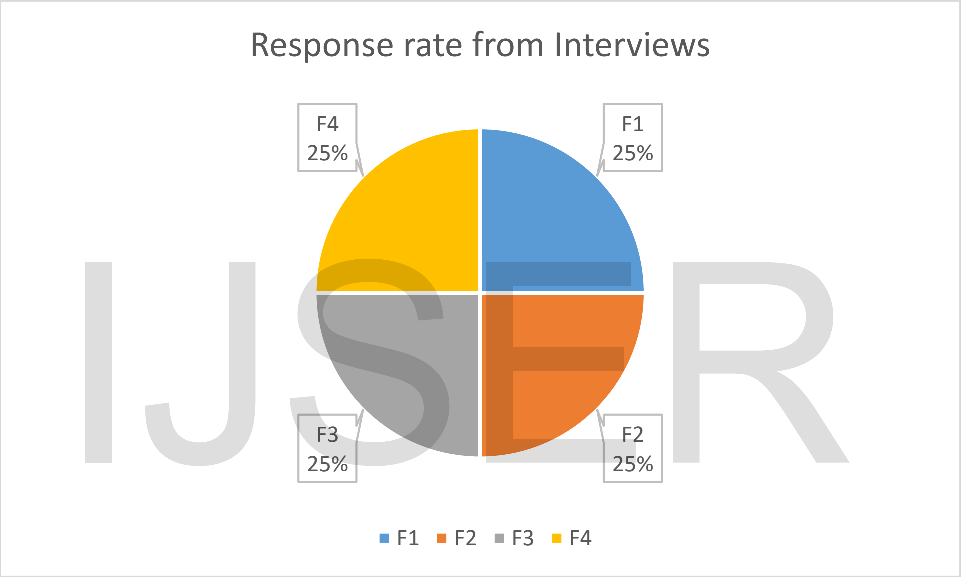
Audit Firm	**Physically Distributed Questionnaires**	**Returned Questionnaires**	**Online Responses**	**Total Responses**
F1	90	19	65	**84**
F2	90	24	33	**57**
F3	90	31	40	**71**
F4	90	13	29	**42**
Total	**360**	**87**	**167**	**254**

Table 4.1 above shows that the researchers managed to get a total of 254 responses from a target of 360 respondents. This translates to a response rate of 70.5% after the initial 21.2% attained from the physically distributed questionnaires which the researcher grew to the 70.5% by distributing online questionnaires as well. The low response rate from F2 and F4 can be attributed to the social distancing measures that organisations have put in place as measures to combat the spread of the covid-19 virus which has caused pandemonium across the world. As a result, the majority of employees where working from home and hence their access to the internet was limited. This affected the research as the online questionnaire required the respondents to be connected to the internet in order to complete it.

Interview response rate

The researchers managed to interview one IT manager from each firm each representing 25% of the targeted population thereby translating to a 100% response rate as all four IT managers from the different firms where interviewed.

Figure 4.3 Interview response rate



Source: Researcher's data

4.3 Attitude and perceptions of employees towards cyber security

It was the researchers' objective to find out on the attitude of the employees on cyber security and how they perceive it so that the cyber risks that they face can be clear to the firms and the researcher. On asking the respondents what they understood by cyber security, the responses where quite revealing for the researcher as the majority of the respondents seemed to have a fairly good understanding of the subject.

4.3.1 Understanding cyber security

The responses varied from firm to firm and it was discovered through the research that in some firms' employees seemed to know more about cyber security as compared to others. In F2 for instance 90% of the 52 respondents demonstrated a good understanding of cyber security as compared to F1's 70% of the 84 respondents and F4's 70% of the 42 respondents who showed a good understanding of cyber security. F3 had the lowest percentage of employees who demonstrated a good understanding of cyber security where only 50% of the 76 respondents showed a good understanding of the subject matter. The research also discovered that from the total 254 respondents 30% of the respondents demonstrated a poor understanding of what cyber security was about. An example is where some respondents said that cyber security is all about hiding your identity while you operate online.

The reason why some firms seem to have employees with a better understanding of cyber security can be attributed to the level of awareness on issues of cyber security within the specific firm. Ongoing education to all employees on technology risks ensures that everyone in the organisation understands the subject and hence behave in a safe manner while carry out their responsibilities. Cyber security education would also result I potential security breaches being mitigated as a result of education and policies being promulgated to all levels of staff. This will ensure that all employees are on high alert and subsequently stay informed on the subject. While the majority of respondent showed that they have good knowledge of cyber security they were those who demonstrated an exceptional understanding of the subject explaining that it involves corporate espionage, hacking, theft of proprietary information and unauthorised access to computer systems and networks.

4.3.2 Importance of cyber security

All 254 of the respondents said that they think cyber security is of importance to their organisation. This is however contrary to the findings obtained from F1, F2, F3 and F4 where 30% of the respondents gave feedback that they do not know much on cyber security. These findings do not match the responses on understanding what cyber security is all about. The irony of this is that the 30% who do not understand what cyber security is, believe that it is important to their organisations. Most responses attribute the importance of cyber security to the protection of company data. This therefore shows that there is a common understanding of the subject matter amongst the majority of the respondents. The 30% of the respondents who seem not to understand much about cyber security but say it is important could be understood as failure to express themselves or inability to explain or demonstrate their understanding of the subject.

4.3.4 Awareness on cyber breaches or attacks

The results indicate that the majority of employees in audit firms did not know the types of breaches or attacks that they may be subjected to. 68% of the respondents said that they are not aware on what constitutes a potential breach or what attack they may be prone to in their work environment. This maybe as a result of no or poor security awareness programs within the organisations so that employees are informed and are in the knowhow of potential breaches and cyber-attacks. It is important for people in an organisation to know specifically the things that they have to look out for with regards to cyber security so that they become more effective in ensuring that these breaches do not happen. From the study a paltry 32% of the respondents stated that they were aware of the breaches or attacks that they may be subjected to within their organisations. The respondents went on to give examples of the attacks that they think they maybe be subjected to within their working space and these include hacking, virus attacks, phishing, identity theft, DoS, exfiltration, as well as systems breach. The few respondents who have outlined the security breaches that they think they are subjected too maybe be those who have a bit of Information Technology background considering the technical terms that they used is outlining the breaches. The majority who rely on the organisation's efforts to equip them with information on how to react to these potential breaches and attacks have no information and as a result are oblivious of the subject understudy.

4.4 Level of preparedness of organisations in response to cybercrime/attack

From the interviews that where conducted, the researchers got a detailed understanding on the state of preparedness of audit firms with reference to cyber security. The four firms have a number of common security mechanisms that are in place to deal will potential cyber-attacks. According to information gathered all four firms use leading anti-virus software with F1 using Avast for business, F2 using Kaspersky and both F3 and F4 using Eset Endpoint antivirus software. The interviewees all alluded to the fact that their antivirus software' are all licensed and kept up-to-date all times. All firms make use of remote management to monitor all client's machines so that they ensure all are up to date save for F3 which does not make use of remote management. They only rely on clients who report if their machines seem not to be updating the antivirus.

The researchers also found out that 75% of the 4 interviewees said that their organisations do not use any physical firewall device. F4 was the only firm that had a physical firewall installed on their network.

A firewall basically stops Trojan horses, stops hackers, stops key loggers (spyware software that cybercriminals try to put on your computer so they can target your keystrokes), monitors traffic entering and leaving your network. Since information is sent over networks in packets, these packets are what the firewall investigates to determine if there is something they contain that is potentially hazardous to the network's security. This therefore clearly shows us that the 3 firms are already vulnerable and ill prepared for cyber-attacks as they lack on the primary protection.

The researchers posed further follow up questions to the IT managers on why their organisations do not use such an important security tool. Responses varied among the 3 firms as two managers gave lack of funding as the major reason and the other said that they do not need the firewall as it is an unnecessary expense as they believe they are not at risk of being attacked by anyone. The researcher therefore noted that the two IT managers from F1 and F3 knew what needed to be done but their challenge was convincing the authorities on the need of such a security tool. The IT manger from F2 showed ignorance as he was adamant that the firewall is a waste of resources as he does not see any potential danger that their firm is exposed to.

4.4.1 Alignment of IT processes to international standards

The researchers through the interviews with the IT managers from the 4 firm also sought to understand if the firms use any IT international standard frameworks in their IT processes. Examples of international standards that can be used in IT include the International Organisation for Standardization (ISO) and Control Objectives for Information Technologies (COBIT). The interviewee from F1 advised the researcher that the firm in the past invested money on the ISO standard but the partners of the firm did not realise much benefit from it and hence they discontinued the alignment of their IT processes to the framework as more resources where needed in the training of staff on how to apply the standard. This could have been because the partners do not appreciate that it is difficult to derive direct benefit or measure the benefits of adopting the framework.

International frameworks or standards enable organisations to keep up with international best practises and hence guide the firm on IT security processes and procedures. The benefit is therefore indirect for example you cannot quantify the benefits of not being hacked or the benefit of having international acclaimed IT processes which will in turn allow the smooth flow of IT processes and ensure that firms abide by the minimum expected state of preparedness on cyber security issues. If a framework states that every network has to protected using a firewall device, it becomes easier for organisations to align with such requirements so that they mitigate against any potential loss or damage through cyber-attack.

The interviewee from F3 advised the researcher that their organisation currently was not using any international standard framework however the COBIT standard is the most appropriate for their organisation. The interviewee seemed to understand the benefits and showed appreciation on the need to adopt an International Standard. The interviewee alluded to the fact that the costs required for the IT personnel to get training on the standard has hindered its adoption. The requirement of foreign currency was cited as the major stumbling block and this has led to the proposal for the adoption of the standard to be at the least of the firms' priorities.

The interviewee from F2 understood the importance of adopting the standards but however insisted that the nature of their business does not really require them to certify with an international standard as they do not major in IT service provision. This revealed to the researcher a knowledge gap within the IT personnel as alignment of IT processes to international practise is not peculiar to IT service providers but across all types of business. The interviewee from F4 seemed to not quite understand the benefit and need to align IT processes with international standards. The researcher noted the lack of knowledge on good international standard practise within the organisation judging from the reluctance and attitude of the staff towards adoption on international standards.

4.4.2 Security breach tests and network monitoring mechanisms

The interviewee from F4 advised the researcher that their organisation does comprehensive security breach tests on their employees every quarter of the year so that everyone remains conscious of the security aspect in their day to day operations. The interviewee volunteered to show the researchers the recent report of the security breach tests done in May 2020 which showed impressive statistics. The report showed a 5% (mostly the senior employees) level of employees who fell for the breach tests and this meant 90% of the staff where conscious about security risks and therefore protecting the organisations from potential loss. The interviewee advised that these tests are done for example by randomly sending emails to employees requesting them to send back their passwords that they use to login to their computers. The majority of the employees according to the report are conscious about the security risks and hence do not fall for these emails.

The interviewee from F1 advised that the breach tests are done every 6 months and employees are frequently advised to be alert of any attempt from anyone trying to extract confidential information from them. The interviewee also advised that from past tests that have been conducted the major group which seems to be falling for the tests are the older generation. He however told the researcher that efforts are being made to conscientise them on the need to be alert of potential data and network security breaches so that they are not the weakest links for hackers. The researcher also discovered through the interview with the IT manger from F2 that they do not conduct network or data security breach tests. The interviewee advised that researcher that they mainly focus on sending out security tips and they believe that the employees as a result will conduct themselves in a reasonable manner should they be faced with such situations.

According to the interviewer these security tips are sent out on a monthly basis. From the information provided by the interviewee the researcher gathered that this means the firm does not evaluate of the impact of the tips that they send out since they do not conduct any breach tests. It would be ideal for the firm to conduct these tests so that they measure that effectiveness of the method that they use lest this does not impact the employees in any way and the security risks remain high. Data gathered from the F3 interview was similar to that of F2 as the interviewee advised the researcher that the departments sends out emails with awareness information on how employees should conduct themselves when doing their work. The researcher discovered that like F2, the firm does not go that extra mile to test and see whether the information that they share with the employees on cyber security is put to use or practised. This leaves the organisation potentially in danger as they will not be aware of the potential behaviours of their employees when faced with potential security breaches.

The researcher also sought to understand the level of education for the IT personnel especially with regards to professional qualifications. Of the four firms only F3 had amongst their IT personnel a Certified Information Systems Auditor. At the time of research F1, F2 and F4 only had under graduate degreed IT personnel save for the IT manager of F1 who had a Masters' in Business Administration. The trend noted by the researcher showed that the firms are under equipped in terms of specialised skill sets for their IT personnel. This as a result exposes the security aspect of the firms as they rely on IT personnel who are not specifically trained on network security issues which are the primary security points in the prevention of cybercrime.

The researchers through the interviews also sought to find out if the firms have any security breach mechanisms in place. The results of the study showed that all four firms did not have any security breach monitoring mechanism within their networks. Security breach monitoring involves collecting and analysing information to detect suspicious behaviour or unauthorised system changes on the network subsequently defining which types of behaviour should trigger alerts and therefore ensuring that the firms take necessary action before damage is done. The absence of such tools in the firms means that the IT personnel will not be able to detect any breach on their network until actual damage has been done.

4.4.3. Training on cyber security best practices

It was revealed from the research that F1, F3 and F4 who constitute 75% of the firms' understudy had not conducted any training on cyber security best practices within the three years under review. According to the interviewee, F2 representing 25% was the only firm that adopted the COBIT standard within the 3 years under review but this was however discontinued in the past year because of the licensing costs. Training on cyber security best practises allow organisations to keep up with current trends and as such ensure that they adopt the most appropriate tools to mitigate against cyber-attacks.

International best practice helps brings to the attention of IT managers trending attacks and the various means in which hackers and cyber criminals use to cause havoc in networks and computer systems. Training on International best practise therefore ensures that IT practitioners remain vigilant of what is happening in their external environment and hence ensure that they stay prepared appropriately for potential harm as hacker's work day and night to cause security breaches. The lack of this sort of training in the firms under study could be because the IT personnel is not very much exposed to the issues of cyber security and therefore cannot convince higher offices on the need to take part in these trainings. Another reason could be that since these training sessions cost a lot of money many organisations do not see any value is investing resources on that aspect of the business. The potential danger for the lack of such trainings is that firms will remain ill prepared in terms of methods and tools adopted to combat cybercrime and ensure that the firms are safe from security breaches.

4.5 Effectiveness of cyber security awareness programs

The researchers discovered that F2 and F3 had the highest number of employees who said that they had taken part in the awareness programs at 90% and 82% respectively. 55% of the staff members from F1 indicated that they have participated in awareness programs within the 3 years under study while only 30% of the staff members from F4 said that they have taken part in awareness training programs. This showed the researcher how unprepared the firms especially F1 and F4 as it is standard IT practise to make sure that employees in an organisation participate in cyber security awareness programs so that they stay alert and know how to deal with potential breaches. This will ensure that they protect both themselves and the organisation from potential loss. The high percentages from F2 and F3 may be as a result of low staff turnover as it is quite rare for some employees to take part in the training while other do not. This therefore may mean that those who said they have never taken part on the awareness programs could be new employees who may have recently joined the firms. On the other hand, the low percentages from F1 and F4 could be attributed to high staff turnover which means that the majority of the staff members who responded to the questionnaires where new and had not taken part in any cyber security awareness programs. The above analysis means that firms do not conduct the cyber security awareness programs as frequent as they should so that everyone is imparted with the relevant information pertaining to cyber security awareness and how employees should behave in keeping the organisation and themselves safe from cyber-attack.

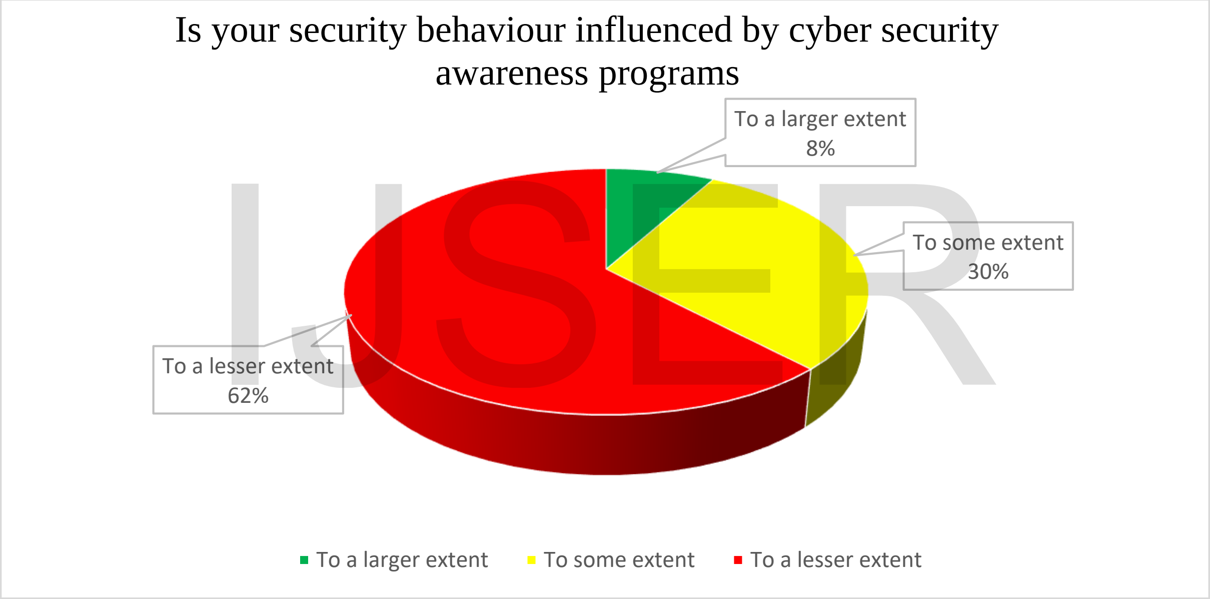
4.6 Value derived from cyber security awareness programs

The respondents who advised that they had taken part in cyber security awareness programs where further asked to what extent they believed that the awareness programs where of any value to the organisations they represented. 74% of the respondents from F2 who said they have taken part in awareness programs and 68% of respondents from F3 who also said they have taken part in these programs suggested that the do not believe that much value is derived from the awareness programs. On the one hand the remaining 26% and 32% of the respondents from firm F2 and F3 respectively managed to demonstrate how they think these awareness programs are beneficial to the organisations and themselves as they stated that the programs helped them maintain information integrity and also made them cautious when working on the internet. Of the 55% of respondents from F1 who said they have taken part in cyber security awareness programs only 25% said they think these programs add significant value to the organisation. 63% of the 30% respondents who said they took part in awareness programs from F4 said that they derive value from the cyber security awareness programs. The poor percentages shown above show a common trend amongst respondents that they do not believe that the cyber awareness programs are of any value to the organisation. This discovery could be because the awareness programs are repetitive and as a result become less effective as the sessions become redundant.

4.7 Cyber security awareness programs and impact on security behaviours of employees

The researchers also sought to understand if there was a relationship between the cyber security awareness programs and the security behaviours of employees. From the four firms a total of 168 out of 254 respondents as represented by the above statistics where 55% from F1, 90% from F2, 82% from F3 and 30% from F4 said they took part in cyber security awareness programs. There was consensus amongst these respondents as the majority highlighted that the nature of the awareness programs that they are exposed to did not affect or influence their security behaviours. The respondents argued that most of the awareness programs do not speak to their needs and tend to be repetitive in nature. The responses of the 168 respondents who answered this section of the questionnaire is shown on the figure below;

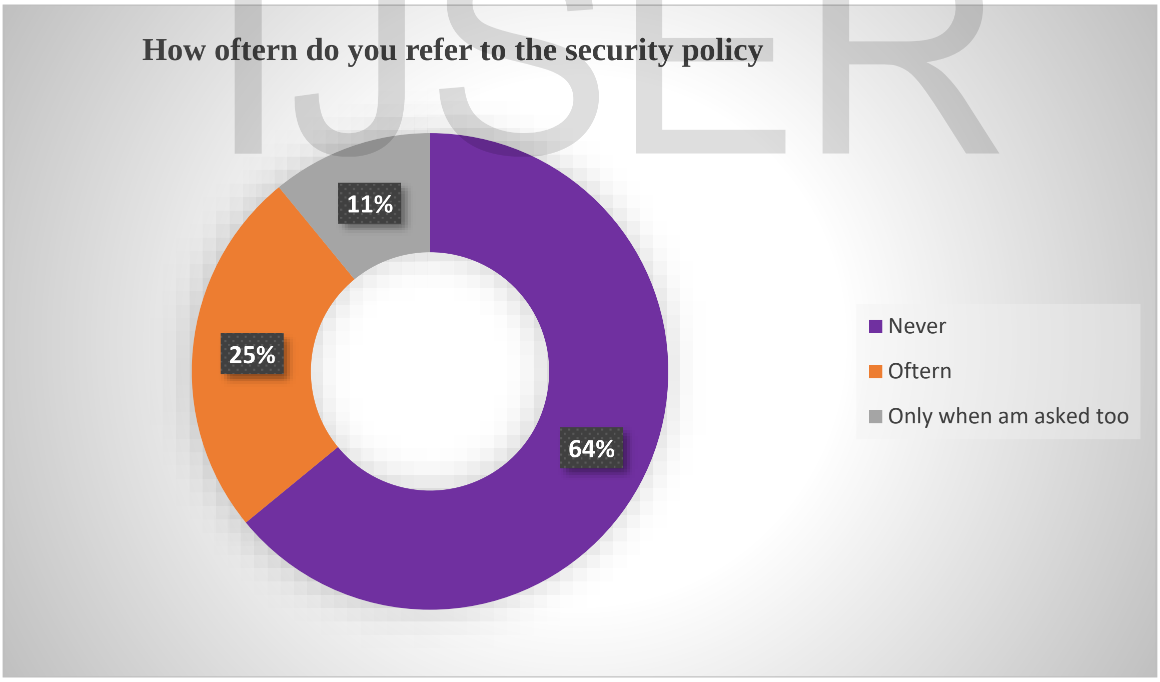
Figure 4.4 influence of awareness programs on security behaviour



The graph above the researchers depicted that there is something not right with the type of awareness programs conducted that is why the majority of the respondents said that those programs influenced their security behaviour to a lesser extent. Of the 168 respondents, a paltry 8% of the respondents believed that their security behaviour was indeed influenced by the cyber security awareness programs. 30% of the respondents said that their security behaviours are influenced to some extent and this may mean that they are not sure of the impact of the awareness programs but in turn acknowledge that there are instances where their security behaviours are influenced by the awareness programs that they take part in. 62% of the respondents stated that these awareness programs influence their security behaviours to a lesser extent. The researchers also got the opportunity to interview the IT managers of the firms who gave similar responses that the main challenge on their cyber security awareness programs is that they are designed at international level instead of national level. They said that for instance the firms have their parent organisation or main headquarters in other countries and hence the programs are designed as a one size fits all thus if a program is designed in USA it is that same program that is used around the world by all its subsidiaries. This is a major challenge as operating environments differ from country to country and therefore using the same awareness programs in different countries causes ineffectiveness in terms of value of these programs. The researcher therefore discovered that the type of cyber security awareness programs that respondents are exposed to are not likely to improve or influence their security behaviours their security behaviours as they do not address their specific needs and environment they operate in.

4.8 Information security behaviours of employees
The study also sought to find out how employees conduct themselves on a day today basis with regards to information security and subsequently cyber security. The respondents were asked if they were aware of any information security policy in their various firms and the responses where in the positive. 73% of the total 254 respondents admitted that they were aware of the information security policy while 27% of the respondents said that they were not aware of such a policy. The reason why some said that there were not aware of the policy could be because they were either new in the organisation or the policy might not have been shared with them when they joined the organisation through an error of omission. By making the policy available and known to employees the organisations are setting themselves in the right direction so that there is a guideline on how employees should conduct themselves or operate to ensure information security. The researchers also found out that despite the majority of the respondents having admitted that they were aware of the security policy of the firms, 68% said they do not refer to the policy at all and 25% said they referred to the policy frequently while 11% said they only refer to the policy when asked to. This therefore means that the majority of employees do not know what the security policy talks to and hence they do not know the security procedures that the organisations expert them to follow. This revelation also means that the security policy is not serving its purpose as a high number of employees did not bother to refer to it or study its contents. This also puts the organisations at a risk of being attacked by hackers as employees do not know the standard operating procedures to follow when a breach is imminent. Responses are shown in the figure below;

Figure 4.7 How frequent do you refer to the security policy



Source: Researchers' data

Since an IT security policy is a model of the organisation's culture in which rules and procedures are driven from its employees' approach to their information and work, an effective IT security policy is a unique document for each organization, cultivated from its people's perspectives on risk tolerance, how they see and value their information, and the resulting availability that they maintain of that information. The above chart shows that the majority of employees do not bother to refer or visit the security policy and as a result leaves the organisation vulnerable since the employees will not behave in accordance to the policy in ensuring that the organisation is safe from potential attacks. This means that the responses shown above leave the firms understudy at high risk as there is no common culture amongst employees on how to behave security wise although this is available in the policy. Employees clearly do not find a reason to refer or familiarise themselves with the policy at their disposal thus they are ignorant to information meant to keep the organisation and themselves safe which is at their disposal.

4.8.1 Password management

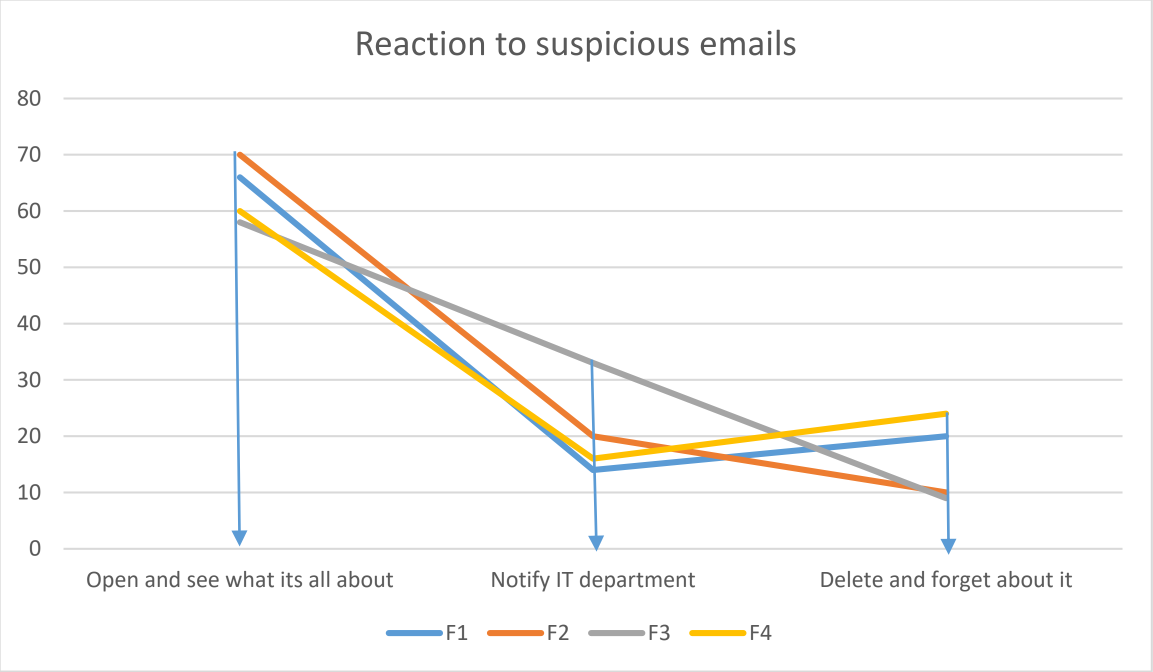
64% of the 254 respondents stated that they changed their passwords only when prompted by the system and this is a major security concern noted by the researcher. The responses from the respondents showed that their security behaviour is consistent with what the firms prefer as it should be at the top of their minds to ensure that they regularly change their passwords but they wait for the system to prompt them to. Relying on the system can be an issue as it may take too long to get the prompt and at times because of the nature of technology where it’s a possibility to go for months without seeing the prompt. This has to be a personal responsibility to ensure that both the individual and the organisation are safe from attack. Only 25% of the respondents said that they regularly change their passwords and this group can be attributed to be the respondents who said they refer to the security policy regularly in the above analysis. The researchers also wanted to find out if employees shared their passwords with anyone at any point. 73% of the 245 respondents said that they do share their passwords in some instances and 27% said they do not. Some said that they share their passwords with the IT personnel, family members and work mates. The respondents explained that in some instances there is need to share login details as there may be limited user licenses for a specific application.

An example of sage pastel was used where respondents advised that the available licenses are not enough for everyone in the accounts office and as a result they have to share the login details. Other respondents said that they share their passwords with their co-workers in the event that they are away from their work station and there is information needed from that specific work station. The respondents admitted that they share in most instances both ERP passwords as well as windows passwords within their confines. This kind of security behaviour is very risky to both the individual and the organisation. By sharing your password one can cause damage or harm using your credentials and as a result you may be disciplined or dismissed from the organisations because of someone actions.

4.8.2 Social Engineering

The researchers also wanted to understand if employees understood the concept of social engineering and whether or not they could tell if this is being tried on them. Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Responses of how employees react to suspicious email are shown below;

Figure 4.6 How employees react to suspicious emails



Source: Researcher's data

From the chat above, the researcher noted a similar trend amongst the four firms. They all have a high percentage of their employees admitting that when they receive a suspicious email they open and see what it is about with F1 having 66%, F2 70%, F3 58% and F4 20% of respondents stating that they open the suspicious emails. This means that employees are not trained are how to handle suspicious email as clicking on it is a high security risk. Since standard IT security practice requires that all suspicious emails be reported to the IT personnel in the organisation or forwarded to the Suspicious Email Reporting Services (SERS), the respondents on the contrary to not exercise such caution but however open and see what the email is all about therefore putting the organisation as the risk of a cyber-attack. This sort of behaviour means that the respondents have not been exposed to awareness programs which deal with ways in which they should react to such emails.

4.8 Cyber security risk assessment

It was the researcher's goal to find out the factors that influence adoption of cyber security tools. The researcher through the interviews asked the respondents on whether or not the firms have conducted any cyber risk assessment audit as well as network vulnerability tests. Of the four firms only F2 conducted a cyber-risk assessment audit within the 3 years under review. On asked what motived this audit to happen, the researcher was informed that a breach once occurred in 2018. The firm had to invest in the audit so that all areas that need security were attended too. The respondent admitted to the researcher that although the audit was done and recommendations given on ways to tighten system and network security, nothing much was done in terms of implementation of the recommendations mainly because of budgetary constraints. From the information gathered, F2 seem to be the better firm of the four, but conducting a network security audit once in three years is not sufficient. The reason being technology is dynamic and needs constant improvement.

The majority of the firms F1, F3 and F4 confirmed that within the three years under review, no security audit had been carried out. To assess their weakness, they all gave similar sentiments that they depended on the standard IT audit. This showed the researcher that these firms are under high risk as basic IT audit does not tackle fundamental security concerns. Cyber security assessment is a significant factor affecting organisations on the form of security tools that should be implemented. The vulnerable sections of IT systems and networks are identified through cyber security audits, and appropriate recommendations are made for addressing the vulnerabilities. Therefore, the security audit brings the less guarded aspects and probable means to the attention of the companies by which hackers are probable to investigate when launching an attack.

4.9 Measures put in place to secure data, systems, computers and networks

It was the researcher's objective to have an understanding of the measures that the firms have put in place to secure their data, systems, computers and networks. The four firms through the IT managers interviewed gave varying lists of the measures they have put in place to secure their organisations from cyber-attack. Below is table showing security measures that organisations should employ versus what the firms have.

5.0Conclusions and Recommendations

5.1 Conclusions

The results of the study demonstrated that the firms under study where ill prepared in terms of cyber security. The study also revealed a low level of cyber security awareness and subsequently how employee security behaviours are not influenced by these awareness programs. A comprehensive discussion on the conclusions reached from the research are detailed below.

5.1.1 Attitude/perceptions of employees towards cyber security

The researchers concluded that employees think cyber security is important and a significant number of respondents demonstrated that they knew what cyber security was. The was a negative attitude towards cyber security as most of them indicated that they did not think cyber security added any value to themselves and the organisations that they are working for. This therefore means that employees are vulnerable and remain the weakest point in the security architecture of the firms they represent. Attitude toward safekeeping of information or data is very essential and insider threat is one of employee's behaviour that shows the strength or weakness of cyber-security in an organization. Insider threat could be malicious or an unintentional threat to an organization and businesses which comes from employees, former employees, or contractors who have inside information about the mode of operation and how data is being handled hence employees, ex-staff, security and IT staff can be an insider threat to an organization.

5.1.2 Level of preparedness of organisations in response to cybercrime/attack.

The researcher also concluded that the firms understudy where ill prepared on cyber security as they lacked the adequate security tools to protect their networks and information systems. It was apparent to the researcher that should there be a cyber-attack, none of the firms which were studied would survive the attack. It is concluded that there has not been adequate investment of resources on cyber security yet this is how organisations lose millions every year. IT is now the cornerstone of how every modern business operates and with that comes the unassailable fact that proper levels of IT security are not negotiable. This therefore means that if you are not taking proper steps to ensure the security of your business' IT systems, you are placing your business, yourself, your employees, and your customers/clients at great risk. This is the case with the firms which where understudy as they demonstrated that they were much ill prepared on the aspect of cyber security.

5.1.3 Eeffectiveness of cyber security awareness programs in combating cybercrime

The researcher can also conclude that the cyber security awareness programs are effective to a lesser extent in improving the security behaviours of employees. The researcher concludes that there is minimal or lack thereof of cyber security awareness programs in firms as three out of four firms studied had not done any awareness programs within the last three years. The only firm that has had these awareness programs has been proven to be in effective by the respondents as they cite issues of repetition of the programs and that they do not seem to address their needs as there is as standard template for the whole group regardless of the country they operate in. Employees therefore attend these sessions to tick the box instead of actually being educated so that their security behaviours improve and as a result protect both the organisation and themselves.

5.1.4 Factors that influence adoption of cyber security tools

It is also a conclusion that the researcher draws from the study that there are a number of factors which affect the adoption of cyber security tools in audit firms. The researcher noted that budgetary constraints are major factor that lead to inadequate tools being deployed to cyber security. The respondents testified that some of their recommendations fail to materialise as the cyber security aspect of the business is less prioritised and hence leaving it exposed and vulnerable. The other reason that affects the adoption of cyber security tools is the level of education and skill set of the IT personnel. The researcher noted that there were no IT personnel from the firms who had a professional qualification on cyber security. The only personnel who had a professional qualification had CISA (Certified Information Systems Auditor) which only looks at policy and compliance issues as compared to professional cyber security skilled people who focus on the technical aspects of cyber security. The conclusion is therefore that there are no suitably qualified personnel to recommend to the firms the best tools that they have to adopt in order to secure the business from potential cyber-attacks.

5.1.5 Measures which organisations have put in place to secure their data, computers and networks.

The researcher also concluded that the firms under study have put ineffective measures to mitigate the risk of cyber-attacks. It was noted that the firms use basic IT security measures in trying to protect themselves against cyber risk. The researcher noticed that no investments where being done to ensure that the firms employ the most appropriate measures to protect the organisation. A firewall device is a basic cyber security device that organisations must use to protect their networks but the study revealed that only one firm had a firewall in place. This shows the poor state of preparedness at the firms.

The researchers further noted that there is an information gap between the IT professionals and the partners of the firms who make the decisions on whether or not the business should invest in cyber security. The researcher concluded that the partners have less appreciation on issues of cyber security as it was discovered during the research that they do not think issues of cyber security should be of high priority as far as budgets are concerned. This therefore means that the partners lack information, exposure or knowledge on how cyber breaches can cost their business millions.

5.2 Recommendations

5.2.1 To firms

Firms should make it a habit to conduct cyber security awareness programs so that employees appreciate the subject area and get an understanding of what a potential breach can cost the organisation. This will help employees conduct themselves in a safe manner when conducting the organisation's business and for individual safety purposes as well. Most organizations commit to one yearly security awareness training programs at the very least, but many are shifting to the overkill of monthly training. However, that the awareness training should not be too frequent as they will be effective because employees are inevitably going to feel like it's too much too often. With this argument in mind and what respondents of one firm attested to that they feel the awareness programs are becoming to redundant, the researcher recommends that the firms conduct cyber security awareness programs at least once per quarter so that are not overwhelmed and subsequently develop a negative attitude towards the programs.

The researchers recommend that firms prioritise the aspect of cyber security in their organisations as this can cause serious financial damage and a threat to the security of the firms' data. There is need to educate the decision makers so that they fully understand the subject area and as a result know the importance and need to invest highly on cyber security tools. It was discovered throughout the research that the partners who are the decision makers had little or no knowledge of what really cyber security is all about and why there is need to invest resources on that aspect of the business.

It is further recommended that the firms adopt a professional standard or framework that they can benchmark their processes with. It was discovered through the study that the firms do not have any framework that they use and this is against best international practise. International frameworks like ISO and COBIT can help organisations align their processes to international standards. The researcher acknowledges the costs associated with adopting these frameworks therefore it is his recommendation that instead of the organisations certifying with the frame work they can instead just align their processes to the framework using as a guideline. Those who however have the financial capacity can go a step further and actually get certified as compliant with the framework. This route would be costly as there will be external compliance audits that will have to take place to ensure that all guidelines are being followed, all recommended tools are implemented and this will be at the firms cost.

Another recommendation to the firms is that they should invest in cyber security specialists. It was discovered through the research that the firms understudy where lacking in the requisite skill set needed to comprehensively address cyber security issues. Most of the IT personnel only had undergraduate degrees with no specialised professional qualifications on cyber security. Without the necessary skill set it is difficult for firms to have the best and appropriate security measures. It is therefore recommended that the firms invest in the training of their current IT personnel or hire the people with the special skill that is needed so that the best recommendations and technical knowhow are achieved.

5.2.2 To government

The government should make it mandatory for organisations to submit cyber security audit reports annually and impose a penalty for those you do not. This will help organisations to adequately prepare for potential cybercrime and subsequently avoid loss of millions of dollars to hackers. It is important to take note that when organisations with in a country loss money treasury bleeds as well.

References

Adamson, J. et al. 2004. 'Questerviews': using questionnaires in qualitative interviews as a method of integrating qualitative and quantitative health services research. [online] Available from http://www.ncbi.nlm.nih.gov/pubmed/15272971 . (Accessed 2016 March 10)

Alam, Md. Shah. (2015). Cyber Crime: A new challenge for law enforcers. [Online]. Available from http://www.prp.org.bd/cybercrime_files/Cybercrime%20--%20Bangladesh%20Perspective.ppt. (Accessed 2020 April 27)

Aloul, F. (2012). The Need for Effective Information Security Awareness. Journal of Advances in Information Technology. Available from https://www.researchgate.net/publication/257980212_The_Need_for_Effective_Information_Security_Awareness. (Accessed 2020 May 1)

Anderson. C. 2010. Presentng and Evaluating Qualitative Research. [online] Available from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2987281/ . (Accessed 2016 March 10)

Armencheva,et al. 2019. Cyber Globalization as an in/Stability Factor. [Online] Available from https://ssrn.com/abstract=3332357. (Accessed 2020 May 5)

Bashay, F. 2018. What is the CIA Triangle and why is it important for Cybersecurity Management? [Onilne] Available from https://www.difenda.com/blog/what-is-the-cia-triangle-and-why-is-it-important-for-cybersecurity-management. (Accessed 2020 May 3)

Bernard, R. 2016. Research Methods in Anthropology: Qualitative and Quantitative Approaches. 4th edition. Roman and Littlefield publishers. New York

Bruijn, H and Janssen M. 2017. Building cybersecurity awareness: The need for evidence-based framing strategies. [Online] Available from

Chad. F. 2016. Behold, the hoverboard of digital reading—or not. [online] Available from http://www.mhpbooks.com/behold-the-hoverboard-of-digital-reading-or-not/ (Accessed 2020 May 19)
Cohen D, & Crabtree B. 2006. Semi-structured Interviews. [online] Available from http://www.qualres.org/HomeSemi-3629.html . (Accessed 2020 May 16)

Cresswell, J.W. 2008. Research design: Qualitative, quantitative, and mixed methods approach. [online] Available from http://gregperreault.com/creswell-j-w-2008-research-design-qualitative-quantitative-and-mixed-methods-approach/ . (Accesed 2020 May 20)

Crewell, J.W. 2009. Research Design: Qualitative, Qualitative and Mixed Methods Approaches. 3rd edition. London. Sage Publication.

Explorable.com (Nov 15, 2009). Research Population. Retrieved May 16, 2020 from Explorable.com: https://explorable.com/research-population

Grustniy, L. 2019. Twich security and privacy settings: Kaspersky daily. [online]. Available from https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. (Accessed 15 April 2020).

Hadlington, L. 2018. Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. International Journal of Cyber Criminology. [Online] Available from http://cybercrimejournal.com/HadlingtonVol12Issue1IJCC2018.pdf. (Accessed 2020 May 6)

Hospelhorn, S. 2012. Events That Changed Cybersecurity Forever. Available from https://www.varonis.com/blog/events-that-changed-cybersecurity/. (Accessed 2020 May 4)

https://reader.elsevier.com/reader/sd/pii/S0740624X17300540?token=C4C378BDEF3F87D66B3EAB45FE2F868AE8E9AB551C68E6C3313208671523E472F8F0A5BEAB40D8140C1CAF938BF20D69. (Accessed 2020 March 17)

Institute of Chartered Accountants of England and Wales, (ICAEW). 2019. Audit insights. Cyber security, taking control of the agenda. [Online]Available from https://www.icaew.com/-/media/corporate/files/technical/audit-and-assurance/audit-insights/audit-insights-cyber-security-taking-control-of-the-agenda.ashx. (Accessed 2020 May 1)
Jay, J. 2017. Organisations' lack of preparedness for cyber threats leading to major crisis.[Online] Available from https://www.teiss.co.uk/organisations-cyber-threats-crisis/. (Accessed 2020 May 4)

Jemal, A. 2014. User preference of cyber security awareness delivery methods, Behaviour and Information Technology. [Online] Available from https://doi.org/10.1080/0144929X.2012.708787. (Accessed 2020 April 24)

Johnson et al (2007). The benefits and challenges of Mixing Methods and Methodologies: Lessons Learnt from Implementing Qualitatively Led Mixed Methods Research Design in Trinidad and Tobago.

Julie M. Haney and Wayne G. 2018. It's Scary...It's Confusing...It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security University of Maryland, Baltimore County. [Online] Available from https://www.usenix.org/conference/soups2018/presentation/haney-perceptions. (Accessed 2020 April 30)

Kabanda, G. 2018. A Cybersecurity Culture Framework and Its Impact on Zimbabwean Organizations. Available from http://www.academia.edu/download/60361766/Gabriel_Paper_AJMECS_Cybersecurity_Culture_Framework20190822-109031-t3ubm9.pdf. (Accessed 2020 May 4)

Khan, et al, 2011. Effectiveness of information security awareness methods based on psychological theories. Center of Excellence in Information Assurance, King Saud University, Saudi Arabia

Khan, F. 2019. Understanding the impact of technology in audit and finance. [Online] Available from https://www.icaew.com/technical/technology.

Kim, L. 2017. Cybersecurity awareness, Nursing Management. Available from https://journals.lww.com/nursingmanagement/fulltext/2017/04000/Straight_talk__Nurse_manager_role_stress.6.aspx. (Accessed 2020 May 5)
Madondo, T. 2017. Exploring Cybersecurity threats in Zimbabwe: Policy brief No 8. Harare. Parliament of Zimbabwe.

Majome, M. T. 2017. Everyday aspects of cybercrime. [online]. Available on http://www.newsdayzimbabwe.co.zw. (Accessed on 11 April 2020).

Martin, J. 2014. Cybersecurity Awareness is about both 'knowing' and 'doing'. [Online]. Available from https://securityintelligence.com/cybersecurity-awareness-is-about-both-knowing-and-doing/. (Accessed 2020 April 28)

Mehio, R. 2019. Fighting hackers: The development of cyber security in Saudi Arabia. [online]. Available on https://stepfeed.com/fighting-hackers-the-development-of-cybersecurity-in-saudi-arabia-8579. (Accessed 3 April 2020).

Michael. K. 2012. Cybersecurity: A Pre-history, Intelligence and National. Available from https://www.tandfonline.com/doi/abs/10.1080/02684527.2012.708530. (Accessed 2020 May 4)

Muller, L. 2015. Norwegian Institute for International Affairs (NUPI). [Online] Available from www.jstor.org/stable/resrep07959. (Accessed 2020 March 31)

Muller, Lilly Pijnenburg. Cyber Security Capacity Building in Developing Countries. Norwegian Institute for International Affairs (NUPI), 2015, www.jstor.org/stable/resrep07959. (Accessed 31 March 2020).

Mwila, K and Lubobya, C. 2019. An Assessment of Cyber Attacks Preparedness Strategy for Public and Private Sectors in Zambia. [Online] Available from https://kingston.co.zm/an-assessment-of-cyber-attacks-preparedness-strategy-for-public-and-private-sectors-in-zambia/ (Accessed 2020 April 24)
Nabi, M. et al. 2014. Cyber security in the globalized world: challenges for Bangladesh. [Online] Available from https://www.researchgate.net/publication/319069519_CYBER_SECURITY_IN_THE_GLOBALIZED_WORLD_CHALLENGES_FOR_BANGLADESH. (Accessed 2020 April 24)
Nurse, J et al. 2019. Standardisation of cyber risk impact assessment for the Internet of Things (IoT). [online]. Available on http://dx.doi.org/10.1007/s42452-019-1931-0. (Accessed 29 March 2020)

Patil, H and Lush, J. 2018. The Why, What and How of Cybersecurity for Accountants. https://cpatrendlines.com/2018/11/28/the-why-what-and-how-of-cybersecurity-for-accountants/. (Accessed 2020 May 4)

Pickard, A.J.2007. Research Methods in Information. London. Facet Publishing
Politzer, M. 2020. Top cyber threats targeting accounting firms. [online]. Available on https://www.journalofaccountancy.com/newsletters/2020/mar/top-cyberthreats-accounting-firms.html. (Accessed on 15 April 2020).

Pribanic, E. 2018. Role of Cybersecurity in an Organizations. [online]. Available on https://www.techfunnel.com/information-technology/role-cyber-security-organization/. (Accessed on 30 March 2020).

PWC. 2018. The Global state of Information security survey 2018. [online]. Available on https://www.pwc.ru/en/publications/global-information-security-survey-2018.html. (Accessed 11 April 2020).

Reserve Bank of Zimbabwe. (2015). Cybercrime in Zimbabwe and Globally. [online]. Available on www.rbz.co.zw/assets/cybercrime-globally-and-in-zimbabwe.pdf. (Accessed on 27 March 2020).

Singer and Friedman. 2014. Cyberspace is the realm of computer networks. New York. Oxford University.

Taherdoost, Hamed. (2016). Validity and Reliability of the Research Instrument; How to Test the Validation of a Questionnaire/Survey in a Research. International Journal of Academic Research in Management. 5. 28-36. 10.2139/ssrn.3205040.

Vohra, V. 2014. Using the Multiple Case Study Design to Decipher Contextual Leadership Behaviors in Indian Organizations. [online] Available from www.ejbrm.com/issue/download.html?idArticle=334 . (Accessed 2020 May 13)