Information Technology (IT) Users in Tertiary Education Institutions in Bulawayo, Zimbabwe: Case of Security Awareness

Bongani Ngwenya
https://orcid.org/0000-0002-6852-1449
University of KwaZulu-Natal
ngwenyab@ukzn.ac.za

Theuns Pelser
https://orcid.org/0000-0001-5935-0185
University of KwaZulu-Natal
pelser@ukzn.ac.za

Abstract

Information Technology (IT) expansion exposes organisations in developing countries to IT security risks. Zimbabwe's tertiary education institutions (TEIs) are not spared. Every year, cyber-attacks increase and become more sophisticated, resulting in losses of personal and financial data for individuals, organisations and governments. As the world is interconnected, small and big organisations share the same internet platform. Therefore, IT security risks that affect one, affect all. When IT users are unaware of the risks and uninformed of ways to protect their IT systems, they remain vulnerable. Like other organisations in Zimbabwe, TEIs are vulnerable to cyber-attacks. The study that directed this article employed a quantitative methodological approach in the collection of the data and its analysis. A sample of 261 respondents was selected from the population of IT users in TEIs in Bulawayo. The results indicated that IT security awareness of IT users in TEIs in Bulawayo is low. This is evidenced by the low IT drivers' contribution towards building IT users' security awareness, and inadequate implementation and utilisation of IT security awareness tools. The prevailing phenomenon exposes TEIs in Bulawayo to a high risk of cyber-attacks. The results indicated a positive and significant correlation between IT security drivers' contribution and IT security awareness tools utilisation in TEIs in Bulawayo. The implication is that an increase in IT security drivers' contribution and IT security awareness tools utilisation will lead to increased IT security awareness. The study recommends that IT drivers double their contribution towards building IT security awareness through adequate implementation and utilisation of IT security awareness tools. This will safeguard the information that tertiary education institutions generate.

Keywords: IT security awareness; IT users; IT drivers' contribution; IT security awareness tools utilisation; tertiary education institutions (TEIs)

UNISA university of south africa PRESS

Progressio
https://upjournals.co.za/index.php/Progressio
Volume 41 | Number 1 | 2019/20 | #6856 | 21 pages

https://doi.org/10.25159/2663-5895/6856
ISSN 2663-5895 (Online)
© Unisa Press 2021

Introduction

Information Technology (IT) security awareness is growing among organisations. Kendrick (2010) suggests that, as IT has become a business and operations driver in the globalised environment, non-commercial organisations such as education institutions are becoming more vulnerable and susceptible to cyber-attack. Like other organisations, education institutions are running their business and operations within insecure cyberspace. Stewart, Tittel, and Chapple (2008a) suggest that this phenomenon is now a reality, nevertheless, coming with risks, threats and challenges, particularly of IT security nature. These authors emphasise that IT users within organisations are constantly vulnerable and prone to IT security risks. This has raised current and future major concerns among IT-based or IT-intensive business and organisational operations organisations—education institutions included.

Technology is driven by and revolves around the Internet. The United Nations International Telecommunications Union (UNITU May 2014) predicted that internet users would reach nearly three billion by the end of 2014. As millions and millions of users are connected to the Internet at any given time worldwide, the risk of breach of IT security over the Internet has the potential of spreading faster than veld fire and has the potential of affecting large numbers of unprotected users instantly, worldwide (Snedaker 2006). According to the Federal Bureau of Investigation (FBI) of the United States of America (USA), if computer systems are not securely protected and users are not familiar with the measures to take to protect their computer systems and their operations, then organisations risk unprecedented IT security damages costing millions of dollars and even threatening their business success and survival. The FBI made a statement before the USA Senate Judiciary Committee on 12 April 2011 that it is not easy to accurately quantify losses that organisations incur due to cybercrimes. The FBI intimated that over the period 2006 to 2011, the costs of cybercrime to the USA economy increased from millions of dollars to billions of dollars. It is in line with this that the Internet Crime Complaint Centre (IC3), which regulates and deals with self-reported complaints of cybercrime, reported in 2012 that identity theft schemes accounted for up to 9.8% of cybercrimes that were recorded in 2012; and the IC3 reported that consumers lost over US$525 million due to internet swindles.

Gessin (2010), of the Asia Oceania Electronic Marketplace Association (AOEMA), indicated in 2010 that the current trends were that some governments of developing countries were forging partnerships with private sector participants in advancing the development of their IT infrastructure. This marked a positive paradigm shift, particularly in the case of Zimbabwe. The public and the private sector have in recent years installed fibre optic links, which link big and small businesses to each other and to the world at large. However, some of these countries are lagging behind in terms of a legal framework to back the IT infrastructure development. These concerns were echoed by the then Zimbabwe ICT Minister, Mr Nelson Chamisa, on 28 November 2012. What this meant was that at that stage, there were no IT laws yet that addressed

specific IT activities in Zimbabwe. This shortcoming exposes IT users, as they remain vulnerable to cyber-attacks, together with the companies that employ them. Like any other sector in the country's economy, the Zimbabwean tertiary education sector remains exposed and vulnerable. Examples of such IT security activities that are at risk include the transmission of encrypted emails, access to encrypted websites, and identity theft that occurs on social networks and media such as Facebook, Twitter, and many more. In these circumstances, Zimbabwe currently relies on circumstantial laws:

- Zimbabwe Access to Information and Protection of Privacy Act (AIPPA) 2002.
- Zimbabwe Broadcasting Services Act 2003.
- Zimbabwe Criminal Law (Codification and Reform) Act 2008.
- Zimbabwe Federal Information Security Management Act (FISMA) 2002.
- Zimbabwe ICT Policy of Zimbabwe 2005.
- Zimbabwe Interception of Communication Act 2010.
- Zimbabwe Postal and Telecommunications Act 4 of 2000, Chapter 12:05 (as amended), Part X. http://www.potraz.gov.zw/images/potraz/Postal_Act.pdf.

Other instruments that regulate internet security are the Zimbabwe Legal Information Institute (ZIMLII), an organisation that provides legal information; the Post and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ); and Zimbabwe Information and Communication Technology (ICT) Policy Framework (Zimbabwe Government 2005).

While large private sector corporations can afford to employ IT specialists with extensive experience in IT security, the public sector institutions such as state universities and tertiary colleges, with their constrained capital resources base, cannot afford adequate security measures (McAfee 2015). This leaves the tertiary education institutions in Zimbabwe exposed to IT security risks. A wave of IT security breaches in Zimbabwe was reported in 2014, and the report indicated that the breaches affected both small and large companies (Techzim 2013). This IT-reporting website, focusing on Zimbabwean technology news, went further and stated that more than 1 000 websites of the ".co.zw" identifier in Zimbabwe were hacked over the period 2001–2014. The bulk of these was hacked between 2010 and 2014. Several cases of piracy and copyright infringements were also reported and recorded in Zimbabwe over the same period. For example, in the report on the "world piracy scourge" presented by the Business Software Alliance (BSA), Zimbabwe was ranked among the top five countries, with the highest index of software piracy in the world in 2010. As these IT security issues affect all organisations, the tertiary education institutions (hereafter TEIs) in Zimbabwe are exposed and remain vulnerable. According to the Zimbabwe 2013 National Budget Statement, presented by the Minister of Finance, Mr Patrick Chinamasa, the education sector in Zimbabwe employs more than 50% of the country's workforce and accounts for about 30% of the country's fiscal expenditure. This means that any activity that

threatens the private and public economic sectors also poses a threat to TEIs in Zimbabwe.

Statement of the Problem

The embracement of IT usage in organisations, both of public and private nature, renders these organisations increasingly vulnerable to various IT security risks, and TEIs in Zimbabwe are not an exception to this global phenomenon. Operating in such an environment means that TEIs in Zimbabwe are equally exposed to piracy and cyber-attack. The media and literature are awash with statistics on organisational cyber-attacks that are on the increase and are becoming much more sophisticated than ever, resulting in massive losses of information and data for individuals, organisations and governments worldwide. With IT connecting the world, such that organisations, big or small, are now sharing the same internet platforms, this implies that IT security risks affecting one easily affects all. Therefore, if the IT systems users are unaware of security risks involved, and they are not conscious of ways they can protect themselves and their IT systems, they constantly remain vulnerable to cyber-attacks. Organisations, TEIs included, are at risk if they have systems that are unsecured and that can be utilised by cyber-attackers to launch cyber-attacks. The low levels of user security-awareness-building efforts by IT drivers and the low levels of security risk awareness of IT users create a gap that can be exploited by IT systems attackers.

Therefore, the study that motivated this article undertook an investigation into the level of IT security awareness of IT users in TEIs in Bulawayo, Zimbabwe. The study was guided by the objectives to measure the levels of IT security awareness of IT users; to assess the contribution of IT security drivers in building the levels of IT security awareness of IT users; to measure the extent to which IT awareness building tools are being utilised in raising the levels of IT security awareness of IT users; and to identify if there are any correlations existing between IT security drivers' contribution, IT awareness tools utilisation, and IT security awareness levels of IT users in TEIs in Bulawayo, Zimbabwe.

Conceptual Framework

The researchers drew up a conceptual framework (figure 1) to address the study's objectives. The conceptual framework defines the two key variables of the study, namely, IT user security awareness building; and IT user security awareness level, which can be viewed as being "high" or "low" (Tryfonas and Askoxylakis 2013; US DSDS 2013). IT user security awareness building has two indicators or sub-variables, namely, IT security drivers' contribution; and IT security awareness tools utilisation (Conrad, Misenar, and Feldman 2010; US NIST 2014). IT security drivers' contribution is indicated by government and management development and the implementation of IT security strategies and polices, while IT security awareness tools utilisation facilitates IT drivers and IT users' interaction through IT security training, IT security education

and IT security workshops (Security Awareness Programme Special Interest Group PCI DSS 2014).

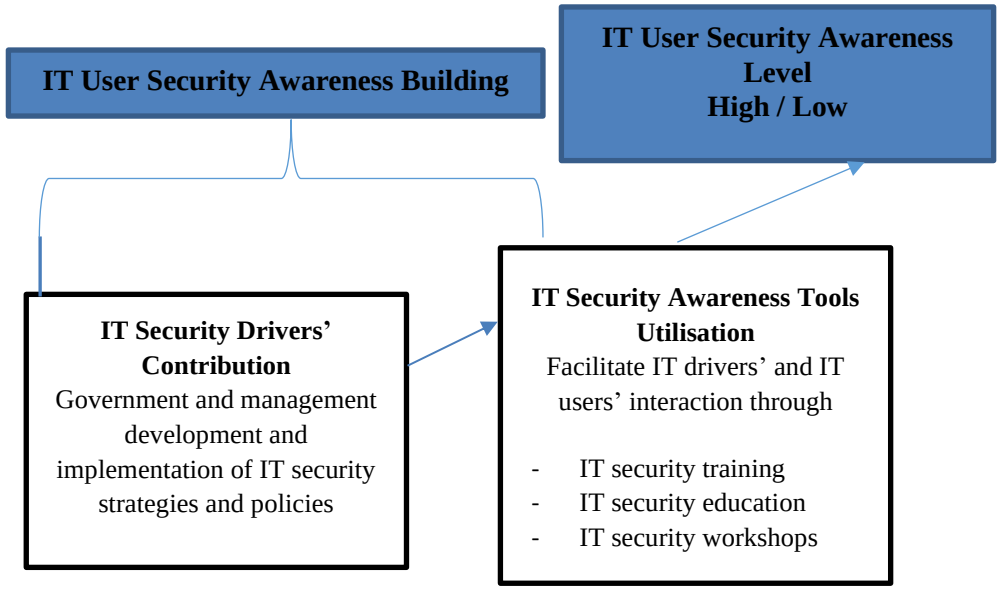

Figure 1: IT user security awareness building and level

Theoretical Framework and Literature Review

In this section, the researchers review related literature on IT security awareness, IT security drivers' contribution in building the levels of security awareness, and IT awareness building tools utilisation among various IT users in organisations. The section also covers literature on management and IT security strategy development and implementation in organisations.

Theoretical Framework

The following section outlines the theoretical framework of the study.

IT User Security Awareness Level

IT security awareness levels among IT users in organisations, including education institutions, can be categorised as high or low. This phenomenon describes the perceptions of IT users towards their security risk appreciation or risky IT operations (Tryfonas and Askoxylakis 2013). With this in mind, Contos et al. (2007) suggest that IT converges the physical world and the logical world; the world that TEIs also find themselves entangled in—and as a result rendering it critical to promote the transference of human physical knowledge and their awareness of security risks in order to fit into this new logical world of IT. Furthermore, Contos et al. (2007) reiterate that as the need

for IT increases in today's tertiary education environment, so do the IT security risks in the environment.

According to Lisa Lindholm of the United States of America (USA) Department of State Diplomatic and Computer Security Awareness Team (US DSDS 2013), users of IT organisational systems require information so as to understand the risks they face in the IT environment. The department further states that the importance of creating awareness among IT users and providing them with vital information cannot be over-emphasised. IT users need to be enabled to become conscious and aware of the possibility of cyber-attacks and security risks they are exposed to in the IT operational environment of TEIs. The department extends the issue of contention by proposing that IT users in TEIs need to have the knowledge required to protect the tertiary institutions' information systems, as this is critical for the effectiveness of any organisation and the fulfilment of its mission, vision and achievement of objectives.

IT Security Awareness Building

The Security Awareness Programme Special Interest Group, Peripheral Component Interface (PCI) Data Security Standards Council (PCI DSS 2014) indicates that the risks affecting organisations' information security systems are not necessarily a sign of weakness in the organisations' technological control environment, rather it is the IT users' ability or lack of ability to act when faced with situations that demand application of IT security awareness. The special interest group goes further to suggest that employees and other organisational staff that are not aware of security risks pose a threat of security risk incidents such as unintentional disclosure of secret organisational information during social engineering attacks by failure to report observed unusual activities and failure to follow proper operational procedures. As a result, there is a need for organisations to have security awareness programmes put in place to ensure that employees remain aware of the importance of securing sensitive organisational information and also that they are aware of the role they are supposed to play to ensure that organisational information and assets are secured and safe. In further support, PCI DSS (2014) reiterates that employees' awareness, understanding of organisational and individual liability and consequences of mishandling sensitive organisational information are critical to organisations' success, and this should be achieved through IT security awareness building exercises and practices. TEIs are also found wanting in this regard.

Furthermore, the PCI DSS (2014) suggests an outline that shows a successful security awareness programme in organisations that hinges on assembling security awareness teams. The support group intimates that these teams can be role-based security awareness teams. There is a need to ensure that the metrics are in place, that there are also available appropriate training materials and adequate content provided. Communication and interaction on security awareness issues within TEIs and other organisations need to be maintained and encouraged all the time. Above all, security

awareness training checklists could help and become handy for organisations when they develop, monitor and/or maintain their security awareness training programmes.

IT Security Drivers' Contribution

Most of the governments in developed countries such as the United States of America (USA) have enacted laws dealing with the safe guiding and defining of acceptable user policies for the Internet and other related technologies. For example, Stewart et al. (2008a) state that the IT-related Federal legislations gazetted by the United States of America (USA) government include the following:

- The Computer Fraud and Abuse Act (CFAA) of 1984.
- Computer Security Act (CSA) of 1987.
- National Information Infrastructure Protection Act (NIIPA) of 1996.
- Government Information Security Reform Act (GISRA) of 2000.
- The Federal Information Security Management Act (FISMA) of 2002.

Stewart et al. (2008a) borrow from the FISMA of 2002, particularly the section stating that the USA government plays a critical role in creating legal frameworks that ensure the promotion of compliance and security risk awareness. Secondly, governments need to take leadership and initiatives to enforce these specifications across all governmental structures. Such government commitment should be evidenced in government institutions such as TEIs and other government organisations. The belief is that if governments lead by example in the application of IT security awareness programmes, the private sector and industry (including the public) will follow suit.

According to the FISMA (2002), organisations need to provide security awareness training to the users of organisational information systems. The purpose of such training is to equip the IT systems users with the necessary knowledge on how to protect organisations' information systems and sensitive information and data from potential external and internal cyber threats. The foundation of this policy anchors on the government's disposition towards IT security awareness philosophy, which emphasises that the levels of IT security consciousness and awareness among IT users determine the magnitude of "the window of vulnerability of the organisation" (US National Institute of Standards and Technology US NIST 2014).

Pursuant to the IT security awareness philosophy and adherence to legislation, the American government has, for example, established boards responsible for administering and overseeing the delivery of IT security awareness, particularly in Federal or government institutions such as state universities and other tertiary institutions and departments. These established boards include the Office of Personnel Management (OPM) and the NIST, which are empowered by the Computer Security Act of 1987 to monitor issues of computer security awareness and training that are based on functional organisational roles. The guidelines were produced in the form of a NIST

Special Publication 800–16 titled, "Information Technology Security Training Requirements (Role and Performance-based Model)."

IT Security Awareness Tools

Conrad et al. (2010) see IT security awareness as a prerequisite and driver for deliberate security awareness training by organisations. The authors further suggest that the objectives of instilling a sense of security awareness are to inspire behavioural change, raise security awareness attention, and make it an organisational strategic issue. Furthermore, Conrad et al. (2010) reiterate that security awareness underlies a common base and foundation for security awareness understanding among organisations or even national entities. In support of raising national security awareness and consciousness, the Department of Homeland Security (DHS) in the United States of America, for example, marked the beginning of the national cyber security awareness month of 2 October 2014, in an effort to enhance public understanding of basic cyber-security awareness practices in America, and the potential role that every individual could play to keep cyberspace free of attacks. The DHS views cyber security awareness as critical to countries' economic survival and acknowledges it as being an integral part of the United States of America's collective national IT security awareness concerns, as both essential services provision and delivery's critical infrastructure technologically relies on cyber networks and systems.

IT security awareness is not entirely realised through classroom-type of expeditions but also through conducive work environments (Conrad et al. 2010). According to Conrad et al. (2010), IT data owners and custodians should avoid assuming that IT users will always know what they are supposed to do or assume they are already doing the right thing. Instead, they should be made aware of safe user behaviour through IT security awareness activities and tools. Workshops, campaigns, presentations, memos, as well as traditional instructor-led training courses and education, are several ways and tools that can be used to create IT security awareness (Stewart et al. 2008a). Security awareness focuses on key and critical issues relating to IT security that every employee in the organisation needs to understand and comprehend (Conrad et al. 2010). The authors further point out that adequate IT security awareness levels of IT users can be enhanced through deliberate IT security awareness advocacy and promotion on a regular basis.

Literature Review

IT Risk Management through Preventive Strategies

Top management in companies must realise and accept the truth about IT security risks. Their companies are continuously becoming more exposed to IT risks and threats. Therefore, sustainable business success depends on their ability to introduce mitigating and preventive strategies, Stewart et al. (2008a) explain. The authors continue that IT is a specialised field and that business IT specialists and professionals are becoming a basic requirement for organisations. They add that when organisational leaders of big

or small companies sit down to strategise, they should identify the risks and value that IT has on their organisation. In line with this, they advise that organisational policies should include IT security on the agenda. Managers in organisations should stop viewing IT security issues as a security person's problem, but rather they should view it as a major risk with the potential to cause problems for everyone in the organisation. Organisational policies, baselines and standards need to be discussed, documented and supplied to all departments. Finally, Stewart et al. (2008a) command management to lead in the motivation towards security.

Of interest is that Cunningham, Manzuik, and Dykstra (2007) make an assessment of small businesses in the USA and conclude that the small businesses which are most likely to avoid, delay or short-cut business continuity planning and disaster recovery planning in IT security issues, are giving excuses that they cannot afford to avoid, limit or transfer risk and therefore, they accept risk by default; thereby committing a serious mistake. According to Cunningham et al. (2007), this is a limited view of security and should not be the default position taken by IT drivers of small organisations when faced with IT risks.

Human Resources Management and IT Governance

In support, Kendrick (2010) introduces a concept of human resources management and IT governance. Kendrick suggests that it is generally recognised in the information security context that the majority of IT security incidents (up to about 70%) arise from human error. Noting this, Kendrick points out that it is thus the responsibility of the management and employed specialists (including the board or partners) to ensure that personnel are trained to understand their responsibilities. The streamlining of the recruitment, selection and induction security training process helps to reduce most IT security risks. This is a key principle of corporate governance, which begins with the board or leadership's responsibility to establish clearly defined lines of accountability and responsibility throughout the organisation. Kendrick (2010) suggests that the board or leadership committee should enact suitable policies and procedures to be observed during business operational activities. IT operational activities that need to be clarified in the business policy include, for example, the use of e-mail, the handling of confidential data, rules about employees engaging in social networking sites, as well as security procedures to follow during the recruitment and dismissal of IT system drivers and users.

IT Risk Acceptance

This article contends that risk acceptance should be evaluated along with the other options to determine the implications, appropriate actions and costs of various mitigation strategies. IT risk acceptance is the least expensive option in the near-term and the most expensive option in the long-term, supposing that the risk event occurs. One cheap way of reducing IT risk is to start educating IT users, Cunningham et al. (2007) advise. In conclusion, they suggest that business continuity and disaster recovery

planning are extremely important for companies of all sizes, even small companies as they try to mitigate risk. Regardless of the size of the company, the impacts of an IT disaster are not just limited to the corporate entity itself, but it may impact the lives of all the employees and suppliers, as well as have a ripple effect on the rest of the community.

Stewart et al. (2008b) maintain the focus on risk and encourage the advancement of risk management skills in managers and IT security drivers as a policy. The authors also encourage the creation of acceptable organisational policies. They define an acceptable "use policy" as a commonly produced document that exists as part of the overall security documentation infrastructure. The acceptable "use policy" is specifically designed to assign security roles within the organisation, as well as to ensure that responsibilities are tied to those roles. Stewart et al. (2008b) suggest that this policy should define a level of acceptable performance and expectation of behaviour and activity. Failure to comply with the policy by the IT system users, or any other stakeholder in the organisation, should be linked to clearly stated implications such as job action warnings, penalties, or even termination of contracts. They link the functions of creating, implementing, monitoring and enforcing policies to the top managers, who should be seen as the first line of organisational internal IT security drivers.

IT Risk Exposure

Stewart et al. (2008b) continue to advocate for risk management and go on to say that security is aimed at preventing loss or controlling disclosure of data while sustaining authorised access. The possibility that something unwanted could happen and lead to the damage, destruction, or disclosure of data is known as risk. Managing risk is, therefore, an element of sustaining a secured environment. Stewart et al. (2008b) view risk management as a detailed process of identifying factors that could damage or disclose data. They evaluate those factors in light of data value and countermeasure cost and implement cost-effective solutions for mitigating or reducing risk. The authors conclude by linking the awareness of IT system users as one factor related to the level of risk exposure in IT security. The more IT system users are aware, the better they are at reducing their IT security risk costs. Another factor raised by Stewart et al. (2008b) is that managers should introduce incentives as a way to motivate safe and risk averse operations as far as IT security risks are involved. This could help employees to become more IT security conscious and be motivated in working according to the stipulated IT standards of the organisation.

Kendrick (2010) proposes that management and the specialised staff recruited by the company must work collaboratively in order to achieve IT security and meet the required levels of organisational IT security awareness and consciousness. He goes on to state that this is possible if, initially, management agrees that IT security poses risks to the organisation and thus requires it to be managed. This should be followed by a skills audit to identify if the critical specialised skills are present for the effective managing of cyber risks in the management team. A variety of specialist areas, such as

risk management, information security, legal and regulatory knowledge, personnel management and administrative functions, must be covered. Other skills may also be required, depending upon the size of the organisation, the way it employs the Internet and the level of employee awareness. The actual management process of cyber risk was explained by Kendrick (2010) using the Cyber Risk Management Framework. Kendrick states that a Cyber Risk Management Framework should be integrated into the organisation's overall management framework to avoid the risk of resistance or lack of commitment by other organisational members who may be against its agenda.

Research Methodology

Research Design

The authors employed a descriptive quantitative research design in this case study of TEIs in Bulawayo. The case study approach allowed the researchers to focus on what is required in the tertiary education sector regarding issues of IT security awareness. Tertiary institutions, by their nature, depend on IT and internet technologies for their operations on a daily basis. Making use of the descriptive quantitative research design allowed the researchers to statistically explore the data collected for the purposes of the study in the process of deducing answers and satisfying the research objectives. The researchers' ability to focus and concentrate on a specific case study group made it easier for them to collect reliable data in the process. It is, however, critical and important to note that the results of the study may not be generalisable to other areas outside the case study.

Population and Sample

At the time of conducting the study, Bulawayo housed a total of 7 tertiary institutions. The institutions included four universities, one polytechnic and two teachers' training colleges. IT and internet technologies are intensively used in these organisations. IT users in these organisations range from staff to students, and their population numbers vary significantly. The three colleges had populations ranging from 500 to 4 500 combined student enrolment and staff, while the four universities had their population ranging from 4 501 to 8 500 (see table 1 below). Students and faculty or teaching staff of these institutions were classified as IT systems users, while the rest of the staff were classified as IT drivers. Each college had at least one IT security driver, while universities had at least two IT drivers who managed the IT systems and IT policies. The researchers used a random sampling technique to arrive at the target sample of 250 IT systems users (comprising students and faculty or teaching staff); and a purposive sampling technique to select all the IT drivers from the three colleges and the four universities. Therefore, 261 respondents were selected for the purposes of the study.

Research Instrument

The main research instrument used in this study was an online questionnaire, which collected the demographic characteristics and profiles of the respondents and the

quantitative data from the respondents. The questionnaire was designed to collect data from the IT users, which were used to assess the users' level of IT security awareness, and to examine the extent to which IT security drivers contributed to building IT security awareness among the IT users. The instrument also measured the extent to which the IT awareness tools were employed in raising the IT security awareness of IT users in TEIs in Bulawayo. The researchers drafted the instrument and its constructs that were derived and informed by the research objectives and conceptual framework. The questionnaire was constructed in the form of a Likert scale that was used to standardise the respondents' responses. The Likert scale was scaled on a 5-perspective measurement, ranging from very high (5); high (4); medium (3); low (2) and very low (1).

Data Collection Procedure

The researchers used the online questionnaire for data collection. This method proved convenient as all the targeted respondents had access to a computer and internet and were computer literate. The respondents' ability to complete the online questionnaire was evidence enough to support that they were IT users and that they had adequate online access. The online questionnaire facilitated instant and wide coverage of data collection across the selected respondents. Furthermore, instant and automatic collection of completed questionnaires was facilitated by an online web collection interface that was provided by an online surveys service provider. More so, the online system provided the required support for easy management of the collected data and provided convenience to both the researchers and the respondents. The instrument covered all the areas of interest and measured all the relevant variables or constructs that were conceptualised for the purposes of this study.

Data Analysis

The collected data were analysed using the Statistical Package for the Social Sciences (SPSS) version 25. In the process of data analysis, the demographic profile and characteristics of the respondents were analysed in terms of gender, age and the size of the TEI, as measured by the student enrolment and staff complement at the time of conducting the study (as shown in table 1 below). Descriptive statistics were used to measure the IT users' level of IT security awareness, IT security drivers' contribution and involvement in building IT security awareness and IT utilisation tools, while inferential statistics were applied to measure the correlation between awareness tools utilisation and IT user awareness levels.

Table 1: Frequency table showing the gender, age distribution of respondents and size of institution

Gender		Frequency	%	Valid %	Cumulative %
Valid	Male	35	48.6	49.3	49.3
	Female	36	50.0	50.7	100.0
	Total	71	98.6	100.0	
Missing	**System**	1	1.4		
Total		72	100.0		
Age					
Valid					
	16–24	11	15.3	15.5	15.5
	25–34	45	62.5	63.4	78.9
	35–44	10	13.9	14.1	93
	Over 45	5	6.9	7.0	100
	Total	71	98.6	100.0	
Missing	**System**	1	1.4		
Total		72	100.0		
Size by student enrolment and staff compliment					
Valid					
	500–4500	3	42.9	42.9	42.9
	4501–8500	4	57.1	57.1	57.1
	Total	7	100.0	100.0	100.0
Missing	**System**	0	0		
Total		7	100.0		

The statistical analysis of the demographics indicated a balanced response ratio attained in the study, with 49.3% representing male respondents and 50.7% representing female respondents. As indicated in the table above, the majority of the respondents (63.4%) had ages between 25 and 34 years, and 15.5% of the respondents had ages between 16 and 24 years. The four universities with a population ranging between 4 501 and 8 500 contributed the bulk of the respondents' sample, constituting 57.1% of the total respondents. While the three colleges, with a population ranging between 500 and 4 500, constituted 42.9% of the total respondents.

Results and Discussion

Table 2: IT users' level of IT security awareness

Descriptive Statistics					
	N	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**
I write the difficult passwords down for future reference	51	-2	2	-.07	1.439
I suspect that my computer at work is infected by viruses	51	-2	2	.08	1.627
I suspect that other users' computers at work are infected by viruses	51	-2	2	-.28	1.321
Overall average on awareness of safe computing practices	53	-1.67	1.67	-.0881	.95217
Spam and unsolicited emails provide me with valuable information	51	-2	2	.17	1.382
I open email attachments from unsolicited emails and spam	51	-2	2	-.92	1.207
Overall average on knowledge of vital security policies and standards	51	-2.00	2.00	-.3750	.99447
I just sign or agree to the IT policies and terms of agreement on websites, I do not read them	51	-2	2	-.61	1.295
I use the same password for social networks and work systems	51	-2.0	2.0	-.942	1.2744
I use the company email address to register on social networks	51	-2.00	2.00	-.8077	1.50865
Overall average on general application of acceptable IT security principles	51	-2.00	1.33	-.7908	.97744
Overall average on total IT user awareness	51	-1.75	1.25	-.4289	.67558
Valid N (listwise)	51				

The results show that the level of IT security awareness of IT users in TEIs in Bulawayo was found to be generally low, as indicated by the attained overall mean score of -0.4289 and standard deviation of 0.67558. The overall statistical result is a build-up of the average awareness of safe computing practices mean of -0.0881 and a standard deviation of 0.95217; the average knowledge of vital security policies and standard mean of -0.3750 and standard deviation of 0.99447; and the average general application of acceptable IT security principles mean of -0.7908 and standard deviation of 0.97744. However, the implication of these results is that the IT users in TEIs in Bulawayo showed a reasonably strong disposition towards a willingness to follow taught and training standards, and to a certain extent, observed due care diligence in the application of generally acceptable IT policies as reinforced by the average mean score -0.7908 and SD 0.97744, with respect to the general application of acceptable IT security principles.

This implies that IT users rarely break the rules when it comes to managing email addresses and the mixing of business and social site passwords.

Table 3: IT drivers' contribution and involvement in building user IT security awareness.

Descriptive Statistics					
	N	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**
The IT people at my work place emphasise IT security awareness as part of company policy	51	-2.00	2.00	-1.3962	1.06228
IT Systems managers at work monitor IT users' activities on the computer systems as part of their IT security control	51	-2.00	2.00	.7500	1.39853
IT personnel at my workplace perform a routine monthly check-up on user computers	51	-2.00	2.00	.4231	1.45987
IT personnel at work perform monthly general IT security discussions and presentations with IT users	51	-2.00	2.00	.3462	1.42643
Overall average IT drivers' contribution at workplace level (internal)	51	-2.00	2.00	.0735	.99284
The government of my country emphasise IT Security Awareness as part of a national security policy	51	-2.00	2.00	-.0385	1.34254
My country's government enacts IT security laws and Acts at parliament	51	-2.00	2.00	.1538	1.19451
State media writes and talks about IT security in my country	51	-2.00	2.00	.1538	1.09158
Overall average IT drivers' contribution at government level (external)	51	-1.67	2.00	.0897	.91968
Overall average IT drivers' contribution towards IT user security awareness	51	-1.43	1.86	.0812	.86956
Valid N (listwise)	51				

The overall results that are a mean score of 0.0812 and a standard deviation of 0.86956 indicate that the general IT drivers' contribution towards the building of IT users' security awareness in TEIs in Bulawayo was perceived to be low. This implies that there is a lack of interaction taking place between the IT security drivers and the IT users in TEIs in Bulawayo with respect to IT security awareness building. Contributing to the overall perception of low IT security driver contribution to IT user security awareness are both the internal IT security drivers and external IT security drivers. These were rated with low perceptions, that is, average internal IT security drivers' contribution at work place mean score of 0.0735; corresponding standard deviation of 0.99284; average external IT drivers' contribution at government level mean score of 0.0897; and

corresponding standard deviation of 0.91968 respectively. The implication of these results is that there is no interaction seen between IT users, government policy makers and state media with regard to IT security awareness building in TEIs in Bulawayo in terms of government IT tools such as IT laws, IT policies and legislation. There is a lack of publicity and promotion through the media of IT security at a national level, as evidenced by the mean score of 0.1538 and corresponding standard deviation of 1.09158.

Table 4: IT awareness tools utilisation

Descriptive Statistics					
	N	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**
New staff undergo induction training on IT security at the company I work for	51	-2.00	2.00	.1923	1.04859
IT users at work are provided with "on-the-job" or "off-the-job" IT security awareness programmes and workshops	51	-2.00	2.00	.1176	1.51851
The IT policy at my workplace is reviewed within every 6 months	51	-2.00	2.00	-.1765	1.46569
I receive IT policy change updates and reminders at work	51	-2.00	2.00	-.6863	1.28826
I receive IT security awareness emails at work	51	-2.00	2.00	-.2353	1.55677
I attend IT security courses and education as my own initiative	51	-2.00	2.00	-.2157	1.43267
Overall average on IT awareness tools utilisation	51	-1.83	2.00	-.1667	1.02144
Valid N (listwise)	51				

The results show that, largely, IT security awareness tools are not being fully implemented and utilised in the raising of IT user security awareness in TEIs in Bulawayo, as indicated by the overall mean score of. -0.1667 and the corresponding standard deviation of 1.02144. These results imply that it is not clear whether there are any standing policies in place to define and govern the usage of IT security awareness tools in TEIs in Bulawayo. The results also indicate that, largely, IT users are not taking personal initiative to search more about issues of IT security and learn other ways in which they can protect themselves from cyber-attacks. A mean score of -0.2157 is evidence of this, with a corresponding standard deviation of 1.43267 indicating that largely IT users remain complacent and indifferent; that is, they assume an aloof position that is divorced of self-drive and initiative directed towards searching and acquiring IT security awareness knowledge.

Table 5: Correlation between awareness tools utilisation and IT user awareness levels

		IT User Security Awareness	IT Awareness Tools Utilisation	IT Drivers Contribution
IT User awareness	Pearson correlation	1	.274	.182
	Sig. (2-tailed)		.614	.572
	N	51	49	50
IT awareness tools utilisation	Pearson correlation	.274	1	.760**
	Sig. (2-tailed)	.614		.000
	N	49	51	50
IT drivers' contribution	Pearson correlation	.182	.760**	1
	Sig. (2-tailed)	.572	.000	
	N	50	50	51

**. Correlation is significant at the 0.01 level (2-tailed)

Inferentially the results show that there is a positive and significant correlation between IT security drivers' contribution and IT security awareness tools utilisation in TEIs in Bulawayo. The results reflected that at a confidence level of 95%, existed; and a significant and positive correlation of r = 0.760 between IT security drivers' contribution and utilisation of IT awareness tools. This implies that with an increase in IT security awareness tools utilisation comes increased IT security drivers' contribution towards IT users' security awareness building. Similarly, a decrease in IT security awareness tools utilisation leads to a decreased IT security drivers' contribution towards IT users' security awareness building. The results also indicate that there is a positive but weak correlation between IT security drivers' contribution and IT users' security awareness of r = .182; and a positive but weak correlation between IT awareness utilisation tools and IT user security awareness of r = .274 respectively. These positive but weak correlations corroborate the descriptive statistical results that indicated low levels of association among this study's variables.

Conclusion

The objectives of this study were to measure the levels of IT security awareness of IT users in TEIs in Bulawayo, to assess the contribution of IT drivers in building the levels of IT security awareness of IT users; to measure the extent to which IT awareness building tools are being utilised in raising the levels of IT security awareness of IT users; and to identify if there were any correlations existing between IT security drivers' contribution, IT awareness tools utilisation and IT security awareness levels of IT users in TEIs in Bulawayo. The conclusions drawn from the results of the study are that the level of IT security awareness of IT users in TEIs in Bulawayo is generally low because of inadequate awareness of safe computing practices and knowledge of vital security policies and standards. Challenges in the general application of acceptable IT security principles are also a cause for concern. However, despite the identified pitfalls, the IT

users demonstrated a strong will to stick to and apply the personally acquired generally accepted IT principles and policies. There is a concern as well that the IT security drivers' contribution towards the building of IT users 'security awareness in TEIs in Bulawayo is not enough. Lack of clear government policies and legislation governing issues of IT security was also raised as posing a serious challenge affecting the tertiary education sector. Whatever there could be in the form of documentation is not adequately promoted and publicised through state media as well as the available IT security awareness tools that are inadequately utilised. Advantage could be taken of the established positive and significant correlation that exists between the IT security drivers' contribution towards IT security awareness building and the IT security awareness tools utilisation, as increased IT security awareness tools utilisation is most likely to enhance the IT security drivers' contribution towards building IT security awareness among the IT users in these tertiary institutions.

Recommendations

Based on the results of the study, the following recommendations are proffered. There is a need for the government (through policy makers) to come up with clear national policies and legislation that govern the use of IT and issues of IT security awareness. There is a need for deliberate and mandatory policies to be put in place to facilitate the building of IT security awareness, not only in government organisations and in institutions such as TEIs, but in private sector organisations as well.

There is a need for TEIs' management and the institutions' IT personnel to exert more effort and contribution towards IT users' security awareness through consistent interaction between IT security drivers and IT users. The study thus encourages internal IT security drivers to devise IT security awareness building strategies that holistically involve the application of both technical and administrative IT security controls. That is, focusing on both technical controls and administrative controls will strengthen effective teamwork and interactive action between IT security drivers and IT users—thus ensuring sustainable IT security awareness growth. Interaction needs to be put in place between IT users and IT security drivers' policies and procedural manuals on IT security policy information, IT security knowledge and other relevant IT security awareness building efforts. The management of TEIs would need to ensure that the developed policies and procedures cascade down to reach the IT users, who are supposedly the main beneficiaries of these initiatives.

IT users need to positively change their attitudes and learn to take the initiative to read and research wide in order to improve their own IT security awareness levels. IT security awareness and knowledge are of a cumulative nature. IT users need to make a consented effort to research widely and develop their own levels of awareness of personal safety computing practices so that they can protect themselves and others.

Recommendation for Further Future Studies

A single study cannot be exhaustive of any phenomenon under consideration and cannot answer all the questions arising in the field of the study. Bearing this in mind, the study recommends further future research to examine what nature of statistical relationships may exist between IT drivers' contribution and IT users' security awareness levels, as well as between IT security awareness tools utilisation and the levels of IT security awareness of IT users. What moderating factor, if any, influences the relationship between IT drivers' contribution and the levels of IT security awareness of IT users in other organisations. A potential further future study could be conducted on a wider population that includes TEIs in other regions of the country, and this could include private institutions as well.

References

Conrad, E., S. Misenar, and J. Feldman. 2010. *CISSP Study Guide*. Burlington: Elsevier.

Contos, B. T., W. P. Crowell, C. DeRodeff, D. Dunkel, E. Cole, and R. McKenna. 2007. *Physical and Logical Security Convergence*. Burlington: Syngress Publishing. https://doi.org/10.1016/B978-159749122-8.50007-7.

Cunningham, B., S. Manzuik, and T. Dykstra. 2007. *The Best Damn IT Security Management Book Period*. Burlington: Syngress Publishing.

Gessin, Jan. 2010. Asia Oceania Electronic Marketplace Association (AOEMA). 2010.

Kendrick, R. 2010. *Cyber Risks for Business Professionals. A Management Guide*. UK: Cambridgeshire.

McAfee. 2015. Live Safe Internet Security 2015 review.

PCI – see Security Awareness. 2014.

Security Awareness Programme Special Interest Group PCI Security Standards Council. 2014. *Information Supplement: Best Practices for Implementing a Security Awareness Programme*, Version 1.0. Security Standards Council.

Snedaker, S. 2006. *IT Security Project Management*. Canada: Syngress Publishing.

Stewart, M. J., E. D. Tittel, and M. Chapple. 2008a. *Certified Information Systems Security Professional Study Guide*, 4th edition. London, San Francisco: Sybex. http://index-of.co.uk/Hacking-Coleccion/CISSP%20-%20Certified%20Information%20Systems%20Security%20Professional%20Study%20Guide,%204th%20Ed.pdf.

Stewart, M. J., E. D. Tittel, and M. Chapple. 2008b. *Network Security, Firewalls and VPNs*. Indiana: Wiley Publishing.

Technology Zimbabwe (Techzim). 2013. http://www.techzim.co.zw/2013/01/why-zimbabwean-websites-increasingly-getting-hacked/ United Nations Department of Economic and Social Affairs http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html.

Tryfonas, T., and I. Askoxylakis. 2013. *Human Aspects of Information Security, Privacy, and Trust*. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-319-07620-1.

United Nations International Telecommunications Union (UNITU). May 2014.

US Department of State Diplomatic and Computer Security Awareness Team (US DSDS). 2013. Accessed August 29, 2019. http://www.dsds.gov/.

US National Institute of Standards and Technology (US NIST). 2014. Accessed September 12, 2019. http://www.nist.gov/.

Zimbabwe Government. 2005. Zimbabwe Information and Communication Technology (ICT) Policy Framework. Harare: Print Flow.

Zimbabwe Legal Information Institute (ZIMLII).

Acts

Zimbabwe

Access to Information and Protection of Privacy Act (AIPPA) 2002.

Broadcasting Services Act 2003.

Criminal Law (Codification and Reform) Act 2008.

Federal Information Security Management Act (FISMA). 2002.

ICT Policy of Zimbabwe 2005.

Interception of Communication Act 2010.

Postal and Telecommunications Act 4 of 2000, Chapter 12:05 (as amended), Part X. http://www.potraz.gov.zw/images/potraz/Postal_Act.pdf.

United States of America

Computer Fraud and Abuse Act (CFAA) of 1984.

Computer Security Act (CSA) of 1987.

Federal Information Security Management Act (FISMA). 2002. Public Law 107–347. National Institute of Standards and Technology. Accessed August 9, 2019. http://www.nist.gov/.

Government Information Security Reform Act (GISRA) of 2000.

National Information Infrastructure Protection Act (NIIPA) of 1996.