SYSTEM END-USER ACTIONS AS A THREAT TO INFORMATION SYSTEM SECURITY

Paulus Kautwima, Titus Haiduwa, Kundai Sai,
Valerianus Hashiyana and Nalina Suresh

Department of Computing, Mathematical and Statistical Sciences,
University of Namibia, Windhoek, Namibia

ABSTRACT

As universities migrate online due to the advent of Covid-19, there is a need for enhanced security in information systems in the institution of higher learning. Many opted to invest in technological approaches to mitigate cybersecurity threats; however, the most common types of cybersecurity breaches happen due to the human factor, well known as end-user error or actions. Thus, this study aimed to identify and explore possible end-user errors in academia and the resulting vulnerabilities and threats that could affect the integrity of the university's information system. The study further presented state-of-the-art human-oriented security threats countermeasures to compliment universities' cybersecurity plans. Countermeasures include well-tailored ICT policies, incident response procedures, and education to protect themselves from security events (disruption, distortion, and exploitation). Adopted is a mixed-method research approach with a qualitative research design to guide the study. An open-ended questionnaire and semi-structured interviews were used as data collection tools. Findings showed that system end-user errors remain the biggest security threat to information systems security in institutions of higher learning. Indeed errors make information systems vulnerable to certain cybersecurity attacks and, when exploited, put legitimate users, institutional network, and its computers at risk of contracting viruses, worms, Trojan, and expose it to spam, phishing, e-mail fraud, and other modern security attacks such as DDoS, session hijacking, replay attack and many more. Understanding that technology has failed to fully protect systems, specific recommendations are provided for the institution of higher education to consider improving employee actions and minimizing security incidents in their eLearning platforms, post Covid-19.

KEYWORDS

Information Systems, Security Threats, End-user errors, Human Factors, DDoS, Virus, Worms, Trojan.

1. INTRODUCTION

The University of Namibia is one of the largest and leading national institutions of higher learning in Namibia. In carrying out this mandate, to provide higher quality education, it embraces technology. The university uses digital means that led to the collection of data and information gathered from its stakeholders, be it staff members, students, or education partners. The amount of data and information collected therein is a very important resource to the university; hence, safeguarding and protecting it against illegal access is crucial [1]. The university's information systems here refers to e-mail systems, integrated tertiary system (Self-Help enabler), staff computers, and corporate network. The university's responsible division, Computer Centre, needs to ensure full implementation of the three information security requirements: confidentiality, integrity, and availability of the information, also known as the CIA triad. The CIA Triad assures users that information is correct, timely, reliable, and free from modifications, destruction, unauthorized access, misuse, and disclosure [2], [3].

Ensuring data protection is not a one-size-fits-all approach. This difficulty could be attributed to the fact that there is a myriad of end-user errors. Human actions can't be hindered. For example is hard to ignore using free public Wi-Fi, clicking on an attractive Add or popup, or losing a device. In addition to technology (AI or IoT) can regulate human thinking. Also, most human errors are overlooked in security policies. Knowing it all, end users pose a potential risk to any organization. End-user errors refer to possible actions by logged-in users. Such errors or acts could occur as a deliberate act, accidentally or as a result of negligence, or simply a mistake without intent to cause harm or malicious purpose by an authorized user of an institution. End users' errors also known as human errors are infinite. It may include but are not limited to using the same credentials on different accounts, not logging out of the system, sharing the password with colleagues, clicking links from an unknown sender, weak password, lack of experience in technology use, and improper training and lack of strong ICT security policy and practices for computer security. System end-user errors lead to vulnerabilities and create room for attackers to penetrate the information system and access sensitive information. Hence, information security governance in education needs attention, and if ignored, consequences of employee actions may lead to catastrophic cybersecurity incidents such as phishing email, social engineering, ransomware attacks, and many more.

Educational institutions will always face security challenges regardless of their financial status reserved for technical controls [4]. Research shows that 52% of users experience viruses and malware infection, although 98% of the users had anti-virus software [4]. This is a clear and lucid manifestation that information security is not all about technology integration. Information security can also be viewed as human-centric since the technological solution cannot fully protect a system one-hundred percent. Neely [4] and Lee [18] agreed that the main loose end of information security is the end-users who interact with the information system. On the other hand, Hadlington [17] argued that users' unintended actions such as incompetence and lack of knowledge towards information security approaches are the weakest component in information security and the main cause of cybersecurity breaches. Safianu et al. [5] further disputed that an institution might have installed the optimum security technologies and defended its physical structures, but it is still completely vulnerable to attacks.

According to the UNAM Computer Centre Report of 2019, over one million spam e-mails have been detected directed to various user accounts. The report further stated that spammers were using advanced techniques by using compromised accounts of legitimate UNAM users to send out impersonating e-mails with links to upgrade e-mail accounts or change their passwords. In addition, although UNAM has technological measures in places like firewalls, Intrusion Detection Systems, and anti-virus to curb loopholes in the network, user accounts are still being compromised, resulting in spammers using legitimate UNAM user account to obtain sensitive information from end-users. These security events happen because current efforts to advance information security and address cyber-security had been mainly focusing on software and hardware, with little or no efforts directed at addressing the users' aspect of information systems [5].

The overall purpose of this study was to (1) identify system end-user errors as part of end-user actions that could lead to information security threats and vulnerabilities and (2) present state-of-the-art human-oriented countermeasures and intellectual ideas on how to deal with human errors to protect the universities' information systems. This research is solicited to contribute to the body of knowledge by presenting original results and disseminating new ideas and significant advances on responding to cybersecurity attacks arising from end-user actions.

2. RELATED WORK

There are many different studies carried on information system security and end-user errors. Researchers have slightly different argumentation, interpretation, and perspectives in their literature reviews. For instance, a study by Pill [6] asserted that information stored in databases is susceptible to a multitude of attacks. However, it is possible to alleviate risks by addressing the most critical threats. Silver [7] also conducted a study on evaluating technological vulnerabilities and found that to protect against targeted attacks, institutions could configure a scanner to check web applications for vulnerabilities such as SQL injection, cross-site scripting, and forceful browsing. The study recommended the use of a web application firewall to protect against vulnerabilities. Lamar [8] argued that database attacks are prevailing nowadays because of the vulnerabilities in Operating Systems. The study also outlines that database rootkits and services associated with the databases could create a loophole for illegal access, leading to a Denial of Service (DoS) attack. Kamara et al. [10] suggested a taxonomy to comprehend firewall vulnerabilities in the framework of firewall implementations as it is not always practical to analyse and test each firewall for all potential issues. Hence, the study scrutinized firewall features and cross-referenced each firewall operation with the causes and effects of faults in that operation, evaluating twenty recognized flaws with prevailing firewalls.

The work by Kassiri & Shahidinijad [11] examined vulnerabilities in software and hardware firewalls and discovered four common vulnerabilities in firewalls. (1) Insider attacks, (2) network traffic, (3) tunnelling, and (4) internet threats. Another study by Soomro et al. [12] established that cryptosystems are even more vulnerable to attack when handling little amounts of data. Soomro et al. [12] recommended a technique to reduce the inefficiency in the algorithm by introducing XOR operation in the major steps of the symmetric algorithm to alleviate communication overhead in transmitting small amounts of data. According to Kaspersky Lab [13] report on software vulnerabilities, it was found that software vulnerabilities exist because of improper process, poor design, and programming errors. Despite the sophisticated design of modern encryption and cryptosystems, they still exhibit the same flaws that the first systems contained many years ago. According to Hadlington [17], a lack of understanding of security problems makes people think that technology alone could solve security problems. Furthermore, Kizza [9] proffered that technology-focused security alone was insufficient as users were being targeted when the technological attacks failed. Safianu et al. [5] narrated that even though many institutions used an extraordinary number of technical security controls, the non-proportional number of security breaches still prevails.

In summary, all literature stated explores the vulnerability studies in software and hardware aspects of information assets, ignoring end-user actions as a potential threat to information security. For this reason, this study investigated the matter intending to close the gap in knowledge on the topic under discussion. Researchers assume there is a great need to address this problem of end-user error-induced vulnerabilities, which many computer security researchers had overlooked.

3. METHODOLOGY

3.1. Research Methods and Designs

A research methodology refers to systematically designing a study to guarantee valid and reliable outcomes that address the research aims and objectives [25]. There are many inquiry or investigation methods in existence: qualitative, quantitative, and mixed-method. This study applied a mixed research methodology that combines qualitative and quantitative approaches to

research. The qualitative research approach has been used to analyse reviewed thoughts as expressed in literature, interpretation, and synthesis of information in secondary and tertiary sources such as related textbooks, reports, and articles. The qualitative study unearths the original thoughts and security perceptions of respondents in words during semi-structured interviews [23], while the quantitative aspect of the (close-ended questionnaire) illuminates the various practices and attitudes regarding cybersecurity. Such approaches and designs allowed the researcher to present theoretical and practical aspects of system security.

Further, the study applied exploratory and experimental research designs. According to [22], a research design refers to the overall strategy or a framework the researcher chooses to integrate different study components coherently and logically for this study. The exploratory design has been adopted by using researchers' ideas and thoughts on the subject matter. It explored theories to inform the topic under discussion. The experimental study design applied Penetration Testing as a hacking method was undertaken. This form of attack constitutes social engineering, phishing, and penetration attempts. The experiment (attack) using a phony phish system has been directed to employees to determine if they follow security standards and policies as stipulated in the ICT policy. The phony phish system has been used to send phishing e-mails, and that outcome has been used to measure the accuracy and validate the result of the research. Figure 1 shows the architecture and design of the phone system. In addition, the study used UNAM as a single case study to do an empirical inquiry about security. This allowed researchers to capture the typical everyday life security experiences faced by staff members at the university. Below is an illustration of the Phony Phish System Architecture.

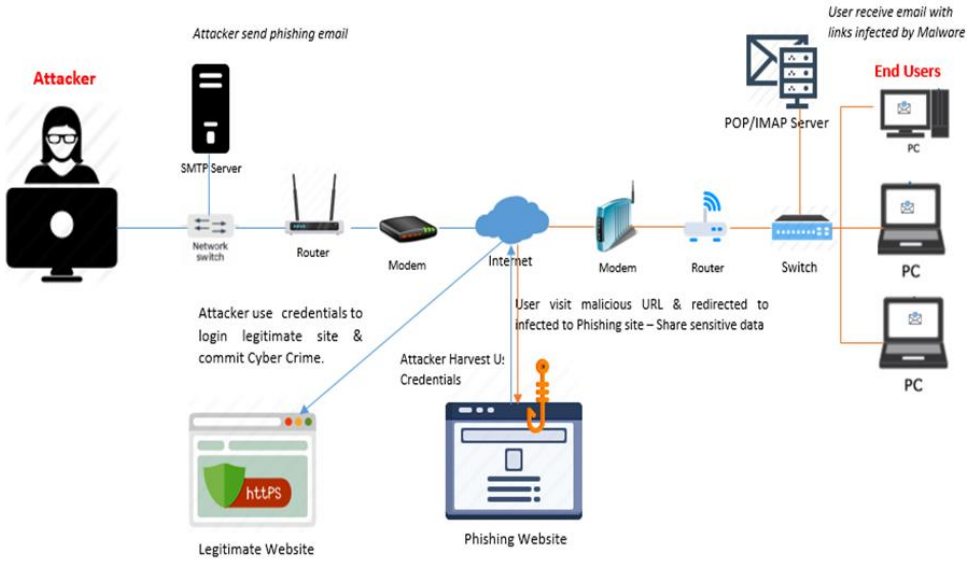

Figure 1. Phony Phish System Architecture and Design

As illustrated above, an attacker sends solicited e-mails to UNAM staff members and requests them to the respondent by visiting a phishing web page and downloading an application for removing malware. The purpose of this was to test staff members on how they react to spam and phishing e-mails. It was also important to know whether employees are aware of Web 2.0 security. The results of the penetrating testing have been astounding. After questioning whether they have seen a similar e-mail as given below, it was found that over half of employees (52%) were aware of it and understood the risks posed by opening questionable e-mails. A well was crafted phishing e-mail was as follows:

> "Dear Sir/Madam,
>
> Your computer has been infected with a virus, and to remove the virus, download and install the tool from this link herein https://leancoding.co/70TIYR with the institution's authorized PC cleaner to eliminate the virus from your computer. Have a nice day.
> Kind Regards,
> Computer Centre"

3.2. Population and Sampling

[21] Defined population "as a total group of individuals from which the sample might be drawn" (p. 1). In this context, the survey targeted the entire University of Namibia staff members (N= 2500) who frequently use its information systems. Sampling is a process of drawing a sample from a specified group using several sampling methods such as simple random sampling, systematic sampling, stratified sampling, clustered sampling, convenience sampling, quota sampling, judgment, or (purposive) sampling, and snowball sampling [20]. Specifically, this study applied a simple random sampling for employee surveys and purposive sampling to select the ten (10) security specialists from Computer Centre Division. The use of purposive sampling was based on the fact that it involves selecting participants for a specific purpose. In this case, the ten security specialists were believed to be in the best position and have the knowledge and skills to answer interview questions. A significant number of 300 staff have participated, and researchers found the results sufficient to represent the total population.

3.3. Data Collection Methods

The data collection for the study consisted of document analysis and direct observation, an online survey, and interviews. Observations were made when visiting staff study areas in the library. Content analysis involves the use of journal articles and books that discuss information security in colleges and universities. The online questionnaire or survey consisted of both open-ended and close-ended questions. Surveys are timely and cost-effective [24]. It is also freedom of expression. In addition, the researchers used a semi-structured interview to collect the experts' perspectives. Ten security specialists participated in the virtual interview, and about 300 other staff members, such as academics and administrative staff, responded to the survey.

3.4. Data Analysis

Data analysis is the process used by researchers to turn large sets of data into a more coherent story and interpret it to derive insights. Data analysis can also be defined as the process of identifying common patterns within the responses and critically analysing them to achieve research aims and objectives. Data analysis enables the examination of the collected information and assists in the preparation of the conclusions. For this study, data entry on a survey and interview was analysed using software packages such as Microsoft excel. This made use of graphical representations of data that were easier to understand. Below each chart of the figure is a caption and interpretation of the data. Findings in qualitative data have been presented in direct quotes followed by a short discussion about a specific theme or concept. Duplicate data were sorted and summarised, so they didn't get dismissed.

4. FINDINGS

Researchers noted that security could be compromised from within the organization. This section, therefore, presents different types of end-user errors discovered during this investigation. Discussions are made below each excerpt, chart, or graph concerning the dangers of irresponsible and uninformed employees within the university. Below are the human factors identified.

4.1. Clicking suspicious links and attachments sent via mail from unknown senders

Taking a closer look at these findings, institutions that use secure communication network protocols such as IP Security, Secure Socket Layer (SSL), Transport Layer Security (TLS), HTTPS, Secure Shell (SSH) and guide employees to follow security procedures and policy tend to have secure hardware and software, hence not vulnerable to attacks compared to those organizations that lack technical and computer security [16]. Phishing and social engineering are among the most effective routes to stealing confidential information from uninformed employees in organisations.

Figure 2. Response to an online request

The questionnaire results showed that 233 participants (77.7%) did have careless actions by following a link that requested them requested to change their credentials by providing their UNAM account details such as UNAM E-mail address and password) and only 67 (22.3%) of the UNAM staff followed a link that requested them to download updates. It was also discovered that the majority (65%) of the respondents hardly check if the link where they enter their login details starts with 'HTTPS'. This tendency of system users can give a hacker a way to steal sensitive information. Moreover, by attacking the right people, attackers can gain access to unauthorised users. Hence, educational institutions and individuals must adopt a combination of technology solutions and user awareness to help protect sensitive information. The findings above corroborate the findings of van Zadelhoff [14], who noted that clicking on links from unconfirmed sources can lead to security breaches. Such irresponsible manners put all security strategies at risk.

After all, an open-ended question was posed to staff members about their thoughts of the university's security strategies. One of the participants was quoted saying: "*In recent days, we experienced increased targeted attacks on e-mails and devices. Therefore fellows need to be aware of malware such as viruses, worms, and Trojans.*" In a similar response to an open needed question of how they perceive the security status of the university, one said: "*staff members are*

our first defence mechanism; however, they can also be the weakest link in a technical system. Humans are so prone to security breaches". In light of this, employees need to mitigate the risks by protecting their systems first as a defined mechanism for institutions since most of their corporate laptops are connected to the university's network domain. "*We all need be vigilant and responsible because if a security incident happens, it affects us all*", another respondent alerted. Contrarily, one said, "*I have no idea, but I do believe they have security plans in place to avoid data breaches. In my experience, they lock e-mails on failed attempts to login*".

4.2. Lack of strong password and inappropriate use of password

A password rule is very important as it is part of human factors. Inappropriate use of passwords and employee behaviour does affect efforts in protecting data and information systems. The complexity of passwords is one of the recommended measures in the information security industry. Preferably, a password should be difficult to guess, implying that it should not be a phrase or word or a number that can be easily remembered, such as ID, birth date, or telephone number [4].

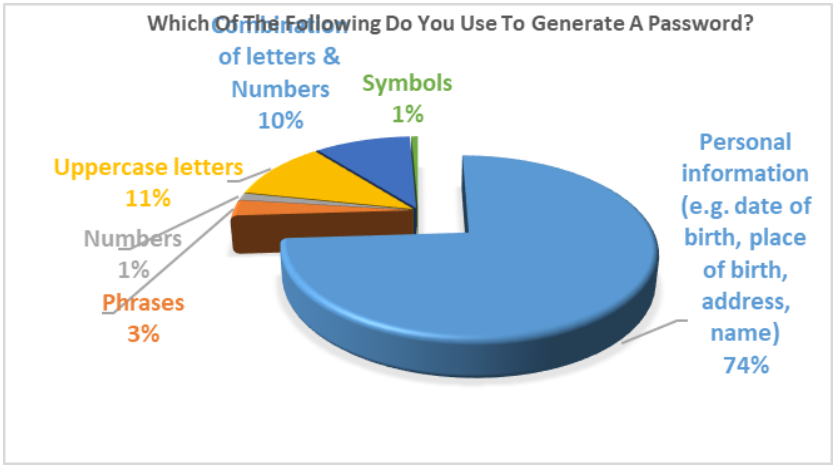

Figure 3. Generation of a password

Results of this study indicated that password use varies considerably. This outcome could be due to several factors such as the level or lack of education on security, awareness, and a pledge to adherence to the organisation's ICT policy. About 72.3 % of the participants used up to 7 characters as their password creation, and 8.3 % mostly set their passwords short. Furthermore, 74 % of the participants indicated that they use personal information such as name, date of birth, place of birth, address, etc., to generate their password, while 11 % use only upper letters. Moreover, 83.3 % of participants indicated that they write their passwords down when it is difficult to remember. The study also revealed that 55.3 % of the participants change their passwords only when the system requires them to do so, and 44 % indicated that they change their password after three months or more. Indulging in these practices, such as using a weak password, writing down and sharing passwords with others, and reusing the same password on different systems, are some of the bad practices that could compromise user accounts and put systems at risk attacks. Like a PIN, passwords must be a secret known to only users to protect data from access from unauthorised individuals. If the password is compromised, the security of the system is at stake. Neely[4], who noted that using a weak password, writing down and sharing passwords with others, and reusing the same password on different systems are some of the bad practices that have the potential to put information at risk. Therefore, users must create strong passwords and log out properly on any system they are interacting with.

4.3. Reckless Handling of Cooperate Computers

Employee carelessness can lead to hardware theft and, eventually, access to data stored on it. It is normal for people to lose devices as we have no control of human behaviour and thinking such as the desire to steal. The study tells us that over half (74%) of the passwords of their devices contain personal information. The chart also shows that only 1% of employees set their passwords to numbers such as "123456". About 3% use phrases such as "password". Few (11) use upper case and lower case or combine phrases and numbers such as "! 12345678@nam." In this case, if a device is stolen and their credential are guessable, information is of value to an attacker may be exploited and be used to launch phasing, harassment-related attacks or other attacks such as DDoS. Therefore, threats and vulnerabilities can be avoided if employees respect to log out or lock their devices whenever they leave their desks.

Moreover, a session timeout could limit the risk to unattended computers [15]. In many instances, people leave their computers idle when leaving the work premises or unattended when attending meetings. Also, some do not log off their computers when visiting the bathroom. These actions, such as misconduct of computer-related equipment, could jeopardise data security. Insiders' attacks are mostly associated with employees leaving their PCs unattended yet with active sessions running hence threatening the viability of the university in protecting its information.

Figure 4. Logging off a computer when leaving work premises

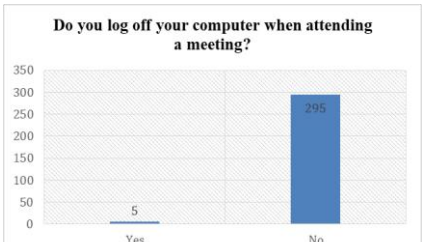

Figure 5. Logging off a computer when attending a meeting

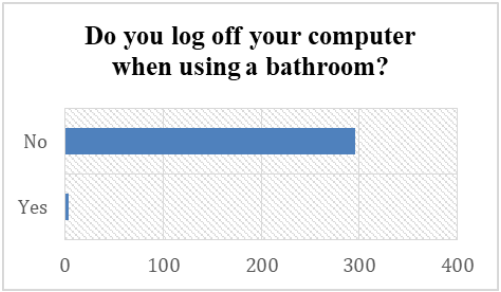

Figure 6. Logging off a computer when using a bathroom

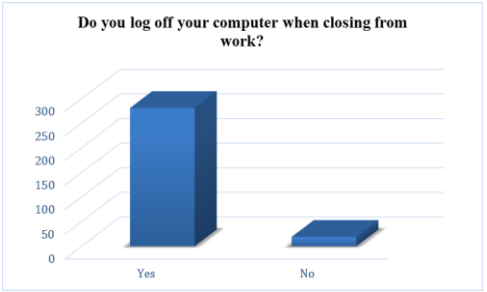

Figure 7. Logging off a computer when closing from work

Figure 4-7 shows the results of UNAM employees who participated in the study. About 256 do not log off their computers when leaving work premises, and only 44 of the participants indicated that they log off their computers even when at their workplace. It has also been noted that around 295 UNAM employees hardly or do not log off their computers when attending a meeting. However, 5 of the participants indicated that they log off their computer even when attending a meeting. Similarly, 296 UNAM employees do not log off their computers when visiting a bathroom, and only 4 of the participants indicated that they log off their computers even when

using a bathroom. Out of the total, 281 UNAM employees log off their computers when closing from work, and 19 of the participants indicated that they do not log off their computers when closing from work. These findings concur with the earlier findings by Evans et al. [16], who indicated that computers that are left idle and unattended might pose a threat to information. Hence, employees should not leave their computers unattended this could put sensitive or confidential information at risk of being leaked, exposed, or altered. Theft of devices accounts for 50% of security incidents; thus, undermining human error can cause major issues. For instance, if the system gets hacked, it may damage the integrity of the ITS system, which manages student information.

4.4. Connecting to networks outside the institutional infrastructure

The lack of consistency in privacy settings gives attackers room to operate. End users are strict on security on one network but are inconsiderate on what information they post online. System administrators need to be careful as hackers can gather and use any available information to search for their victims, the most popular source for such a search being the internet and social networks. The study discovered that e-mail is one of the routes attackers use to access a network. When users use the institution network to send and receive e-mails, they jeopardise the network and information. As employees connect to both the private (corporate) and public (internet) networks, their computers become less secure as they can run malicious applications. It was further discovered that some UNAM staffs are irresponsible when using the institution's computers. They often leave their computers unattended and without the proper password. All these behaviours make data and information vulnerable to attacks. These findings substantiate the findings of Gyunka & Christiana [19], who indicated that the lack of consistency in privacy settings gives attackers room to operate and phish information to attack the network[17, 21].In this regard, the use of a Virtual Private Network(VPN) is highly recommended.

4.5. Deficiency of well-formulated personal security guides and unlawful application usage

Mobile devices and application usage behaviour of individual user affects security. For example, a lack of strong passwords to social media accounts such as Facebook and Twitter could be an entry point for hackers. Also, the culture of unauthorised applications used by users in the university network could compromise the security of the university networks as a carrier of infections. The institution and worker's personal information could be jeopardised when unofficial applications are used on the institution network [19]. The unauthorised applications are mostly downloaded from malicious websites. This applicant can come along with viruses, Trojan Horses, or worms. The study found that malicious programs could be spread over the university network when files are downloaded from unknown and untrusted websites. This could cause a serious security breach. These findings concur with the findings of the study conducted by Gyunka & Christiana [19], which indicated that unauthorised applications used by users in corporate networks could compromise the security of these networks.

4.6. Distant employee security

As institutions' operations become more and more dispersed and transition online, mobile workers increase the potential threat for data [17]. Employees tend to move unfinished work to their devices and take it along at home to work on it later. This habit is quite risky because personal computers and devices are often less secure than corporate ones. The study has shown that improper data handling, such as moving files from an office device to a home computer that does not have proper IT security measures, attracts information theft. Hadlington [17] also

indicated that one of the hazardous behaviours of exposing information to attacks is sending them home with an employee. This tendency can turn all security measures in an institution into a useless process and could put information at risk of sophisticated distributed denial of attacks (DDoS) and threats of cyber-espionage, cybercrime, and spam bots [26].

4.7. Threats from within the institution (inside attackers)

Among the employees, some might be discontented with their jobs, peeved with their boss, or sentimental for any reason. These employees may become attack vectors or insider threats who purposely damage or leak data [17].The study established that when employees are unhappy with their jobs, angry with their boss, or sentimental for any reason, they could become insider threats who can purposely damage or leak information. Therefore, users could deliberately expose information to hurt the institution for some reason, as stated above. Hadlington [17] indicated that sometimes the problem is not that users ignore security threats, but the users are the threats themselves; they have the potential to deliberately expose information. Hence is crucial to come up with hiring and termination procedures to avoid attacks from disgruntled employees. In this study, no worker has reportedly been involved in any malicious actions as yet. However, institutions are warned of possible staff who may, for unknown reasons, work against their employers.

5. DISCUSSIONS

5.1. Mitigating Security threats by employee dilemma in universities

Although security mechanisms are put in place within the corporate network, more needs to be done in addition to software and hardware-oriented security practices such as intrusion detection and prevention systems, configuring of proxy servers, firewalls to whitelisting specific or blacklisting of certain software., installing updates and keeping the anti-malware program on, e-mail security (junk e-mail filtering), web security (certificates) and network security (security protocols). Since the connection between humans and technology (security systems) is inseparable, there must also be human-centred cybersecurity approaches at all aspects of security solutions [27, 28, 29]. These employee-focused security measures include two-factor authentication mechanisms to ensure only authorized parties can perform certain actions, user identifications, compulsory education and training of personnel, strict ICT policies to accountability and none repudiation, continuous monitoring and assessments of system's security, employee engagement utilizing lectures and webinars to disseminate knowledge and raise awareness among employees on the significance of user to act on managing personal passwords properly and ignoring fraud-related e-mails, revocation of access in several failed attempts and do computer forensics.

6. CONCLUSIONS

The study aimed to identify human aspects that lead to cybersecurity threats within the institution of higher education and recommend human-centred countermeasures. Findings showed a gap between cybersecurity technological and human factor-oriented solutions at the university. Cyber-attacks have increasingly become more and more sophisticated as systems get dispersed and distributed over the network. The root cause of cybersecurity is end-user errors. For example, reckless or uninformed staff as wires communication becomes ambiguous, so the increase in human errors is due to newly deployed systems. Even though technology is indispensable in the information security structure, it has shortcomings. Hence, technology alone is insufficient to safeguard the university's information system from data breaches. It is not a sensible idea to think

that the role of people is to run the applications only, but people must be considered in all aspects of security solutions. System end-users can be the weakest or strongest aspect in the security framework and, therefore, ongoing training, awareness, frequent review of security policy and security measures should alleviate the prevailing security technology deficiencies. For that reason, there is a need for the university to integrate both technological and human-oriented. Combining software, hardware, and human-centric actions can help achieve an effective information security management system in the university setting. It was recommended that for the end-user errors in information security to be managed meritoriously, the university must encourage and raise awareness of possible security incidents such as vulnerabilities, threats, attacks, and risks. It must also strengthen and enforce its ICT policy to serve as a unique guideline to deter threats from within. In addition, the university security team needs to benchmark its security practices to prevent employee-related threats and stay resilient. Security plans must be in place for any possible worst cases and easy recovery.

ACKNOWLEDGMENTS

The authors would like to express their unlimited gratitude and appreciation to everyone who made this research study possible.

REFERENCES

[1] N.Uushona. "University Of Namibia ICT Policy". 2016. Available: http://unamintranet.unam.na/documents/ict-policy.pdf. (2016)

[2] J. M. Pizza. "Guide to Computer Network Security". (4th Ed.). Chattanooga: Springer International Publishing Ag. 2017.

[3] W. Stallings. Network Security Essentials: Applications and Standards. 4th Ed. 2011. ISBN-10:013608059. Prentice-Hall.

[4] L. Neely. "Threat Landscape Survey: Users on the Front Line". 2017. California: Sans Institute. Available: https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910

[5] O. Safianu, F. Twum & J. B. Hayfron-Acquah. "Information System Security Threats and Vulnerabilities". International Journal of Computer Applications 143(5), 8-14, 2016. Available: https://www.ijcaonline.org/archives/volume143/number5/25071-2016910160

[6] M. Pill. "Top Ten Database Attacks", 2016. Available: https://www.bcs.org/content-hub/top-ten-database-attacks.

[7] P. Silver. Vulnerability Assessment with Application Security. Washington DC: F5 Networks, Inc., 2013.

[8] A. Lamar. Types of Threats to Database Security. 2012. Available: http://ir.knust.edu.gh/bitstream/123456789/10083/1/omar%20safianu.pdf, (accessed June 2020).

[9] Kizza, J. M. (2017). Guide to Computer Network Security (4th Ed.). Chattanooga: Springer International Publishing AG.

[10] S. Kamara, Fahmy, E. Schultz, F. Kerschbaum, & M. Frantzen. "Analysis of vulnerabilities in internet firewalls". 2010. Available: https://www.cs.purdue.edu/homes/fahmy/papers/firewall-analysis.pdf (accessed July 31, 2019).

[11] I.M. Kassiri, & A. Shahidinijad. "A survey of security issues in the firewall: a new approach for classifying firewall vulnerabilities". International Journal of Engineering Research and Applications (IJERA), 3(2), 585-591, 2013

[12] A. W. Soomro, A. Nizamudin, U. Iqbal, & A. Noorul. "Secured Symmetric Key Cryptographic Algorithm For Small Amount of Data". 3rd International Conference on Computer and Emerging Technologies (ICCET), 2013.

[13] Kaspersky Lab. "Software Vulnerabilities", 2013. Available: http://www.securelist.com/en/threats/vulnerabilities?chapter=35.

[14] Marc van Zadelhoff. The Biggest Cybersecurity Threats Are Inside Your Company. Harvard Business Review, 2016.

[15] P. Kearney. Security: The Human Factor. 2010. Cambridge Shire: IT Governance Publishing.

[16] M. Evans, L. A Maglaras, Y. He, & H. Janicke. Human Behavior as an Aspect of Cybersecurity Assurance. Security and Communication Networks, 9(17), 4667-4679, 2016.
[17] L. Hadlington. "Human Factors in Cybersecurity: Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours". (Vol. 3). London: Heliyon, 2017.
[18] H. Lee. "The Human Factor in Cybersecurity: Exploring the Accidental Insider". UK: IGI Global, 2018.
[19] B. A. Gyunka, & A. O. Christiana. "Analysis of Human Factors in Cyber Security: A Case Study of
[20] J. W. Creswell. Research Design (4th ed., Vol. 4).2014. SAGE Publications. https://www.amazon.com/Research-Design-Qualitative-Quantitative-Approch
[21] B. Davis. What is the target population in research methods? 2021. from https://www.mvorganizing.org/what-is-target-population-in-research-methods/
[22] K. S. Muhammad. Basic Guidelines for Research. Research design, 1(1), 111–169. 2016. from https://www.researchgate.net/publication/325847047_research_design
[23] C. Tilley. Qualitative research: What is it and why should you use it.2019. https://www.onepoll.com/qualitative-research-what-is-it-and-why-should-you-use-it/#:%7E:text=In%20short%2C%20in%20comparison%20to,new%20concepts%2C%20theories%20and%20products.
[24] S. Shantikumar. Methods of sampling from a population. 2018. https://www.healthknowledge.org.uk/public-health-textbook/research-methods/1a-epidemiology/methods-of-sampling-population
[25] M. Saunders, P. Lewis, & A. Thornhill. Research Methods for Business Students. 2012. New York: Pearsons Education Limited.
[26] A. Liaropoulos. A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia. Journal of Information Warfare. Vol. 14, pp. 15-24, 2015. Peregrine Technical Solutions. From https://www.jstor.org/stable/26487503
[27] K, Renaud & S, Flowerday. Human-centred Cyber security. Journal of Information Security and Applications. 2017. 34. 10.1016/j.jisa.2017.05.007.
[28] M, Grobler, R, Gaire & S, Nepal. User, Usage, and Usability: Redefining Human Centric Cyber Security. 2021. Front. Big Data 4:583723. DOI: 10.3389/fdata.2021.583723.
[29] C, Barbara. How to Adopt a Human-Centric Approach to Security. 2018. from https://www.csoonline.com/article/3245741/how-to-adopt-a-human-centric-approach-to-security.html

AUTHORS

Paulus Kautwima is currently a Lecturer in the School of Computing, Department of Computer Science, University of Namibia. His area of research is Networking and Security, Online Child Protection, eLearning, IOT, Cloud Computing and Security, AI, Robotics, egovernment, and educational technologies.
Tel:+264814131922, pkautwima@unam.com; pkautwima@gmail.com

Kundai Sai is currently a Ph.D. candidate at University of KwaZulu-Natal, SA. He holds a BSC Degree in Physics and Computer Science from Great Zimbabwe University, a Master of Science Degree in Information Systems Management from Midlands State University.
Tel: +264814515699, ksai@unam.na

Titus Haiduwa is currently a Lecturer in the Department of Information Technology, School of Computing, University of Namibia. He currently holds a Diploma and a Bachelors' Degree in Information Technology from Namibia University of Science & Technology, as well as a Master Degree in Engineering with specialization in Software Engineering from Wuhan University.
Tel: +264812001246, thaiduwa@unam.na

Nalina Suresh is currently a Senior Lecturer in the School of Computing, Department of Information technology University of Namibia. Her area of research is Networking and Security, Computational Theory and modelling, Automation, IOT, Cloud Computing and Security, AI, Robotics, ML, DSP, educational technologies.
Tel: +264812229533, nsuresh@unam.com; nalina.kss@gmail.com

Valerianus Hashiyana is currently a Senior Lecturer at School of Computing and Head of Department: Computer Science, University of Namibia. His area of research are Cybersecurity, Networking, IOT, e-health, Next generation computing.
Tel: +264812830277, vhashiyana@unam.na ; vhashiyana@gmail.com