SYSTEM END-USER ACTIONS AS ATHREAT TO INFORMATION SYSTEM SECURITY

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

School of Computing, University of Namibia, Windhoek, Namibia

ABSTRACT

Information system security is of paramount importance to every institution that deals with digital information. Nowadays, efforts to address cybersecurity issues are mostly software or hardware-oriented. However, the most common types of cybersecurity breaches happen as a result of unintentional human errors also known as end user actions. Thus, this study aimed to identify the end-user errors and the resulting vulnerabilities that could affect the system security requirements, the CIA triad of information assets. The study further presents state-of-the-art countermeasures and intellectual ideas on how entities can protect themselves from advent events. Adopted is a mixed-method research approach to inform the study. A closed-ended questionnaire and semi-structured interviews were used as data collection tools. The findings of this study revealed that system end user errors remain the biggest threat to information systems security. Indeed errors make information systems vulnerable to certain cybersecurity attacks and when exploited puts legitimate users at risk.

KEYWORDS

Information security, Information Systems, End-user errors.

1. INTRODUCTION

1.1. Background

The University of Namibia (UNAM) collect different type of data and information 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 protectingit and securing the University information systems is crucial [1]. The university's information systems here refers to email systems, integrated tertiary system (Self Help enabler), staff computers and corporate network (internet). In carrying out this mandate, however, the university's responsible division, Computer Centre, need to ensure full implementation of the three information security requirement: confidentiality, integrity and availability of the information, also known as the CIA triad. The CIA Triad assure users that information is correct, timely, reliable, and free from modifications, destruction, unauthorized access, misuse and disclosure [2], [3].

Ensuring data protection, however, has no one way to fix. This difficulty could be attributed to the fact that there is a myriad of end user actions and mostly human errors are overlooked. End-user (human) errors refer to possible actions by logged in users. Such errors or acts could occurs as a deliberate act, accidentally or a result of negligence or simply a mistake without intent to cause harm or malicious purpose by an authorised user of an institution. Human errors are infinite may include but not limited to using the same credentials on different accounts, not logging out

David C. Wyld et al. (Eds): SOFEA, CTCM, BIBC, SIPR, NCWC, CSEN, EDTECH - 2021
pp. 125-135, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111611

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 get access to sensitive information.

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 but it also entails user-centric since technological cannot protect a system one-hundred percent. Neely [4] and Global Security Survey [20] agreed that that the main loose end of information security is the end-users who interact with the information system. On the other hand, Hadlington [19]arguedthat user'sundeliberate 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 [5] further disputed that an institution might have installed the optimum security technologies in existence and defend its physical structures but it is still completely vulnerable to attacks.

1.2. Problem

According to the UNAM Computer Centre Report of 2019, over one million spam emails have been detected directed to various user accounts. The report further stated that spammers were using advanced technics by using compromised accounts of legitimate UNAM users to send out impersonating emails with links to upgrade email account or to change their password. In addition, although UNAM has technological measures in place like firewalls, Intrusion Detection System and antivirus 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. Thesesecurity 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].

1.3. Objectives

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.
2. Present state-of-the-art countermeasures and intellectual ideas on how to deal with human errors to protect the universities'information systems.

1.4. Significance

This research is solicited to contribute to the body of knowledge by presenting original results and disseminate new ideas and significant advances on how to respond to cybersecurity attacksarising from end-user actions.

2. LITERATURE REVIEW

2.1. Related Work

There are a number of 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 [9] 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 [10], 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 [11] 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 which may lead to a Denial of Service (DoS) attack. Kamara [12] 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 scrutinised firewall features and cross-referenced each firewall operation with the causes and effects of faults in that operation, evaluating twenty recognised flaws with prevailing firewalls.

The work by Kashefi [13] examined vulnerabilities in software and hardware firewalls and discovered that there are four common vulnerabilities in firewalls. (1) Insider attacks, (2) network traffic, (3) tunnelling, and (4) internet threats. Another study bySoomro [14] established that cryptosystems are even more vulnerable to attack when they are handling little amounts of data. Soomro [14] 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 [15] 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 [19], a lack of understanding of security problems makes people think that technology alone could solve security problems. Furthermore, Kizza [12] proffered that technology-focused security alone was insufficient as users were being targeted when the technological attacks did not succeed. Safianu [20] narrated that even though many institutions made use of an extraordinary number of technical security controls, the non-proportional number of security breaches still prevail.

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 urgently 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 had been overlooked by many computer security researchers.

3. METHODOLOGY

3.1. Research Design Methodology

The study applied a mixed research methodology with an experimental research design. Such an approach allowed the researcher to present theoretical and practical aspects of system security.In principle, the qualitative research approach has been used through analysis of reviewed thoughts as expressed in literature,interpretation and synthesis of information in secondary and tertiary sources such as related textbooks, reports and scholarly articles. The qualitative data involve theoriginal outcome of the questionnaire and semi-structured interviews.

An experimental study usingPenetration 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 on employees to find out if theyfollow security standards and policies as stipulated in the UNAM ICT policy. The phony phish system has been used to send phishing emails and that outcome has been used to measure the accuracy and validate the result of research. Figure 1 shows the architectures and design of the phony system.

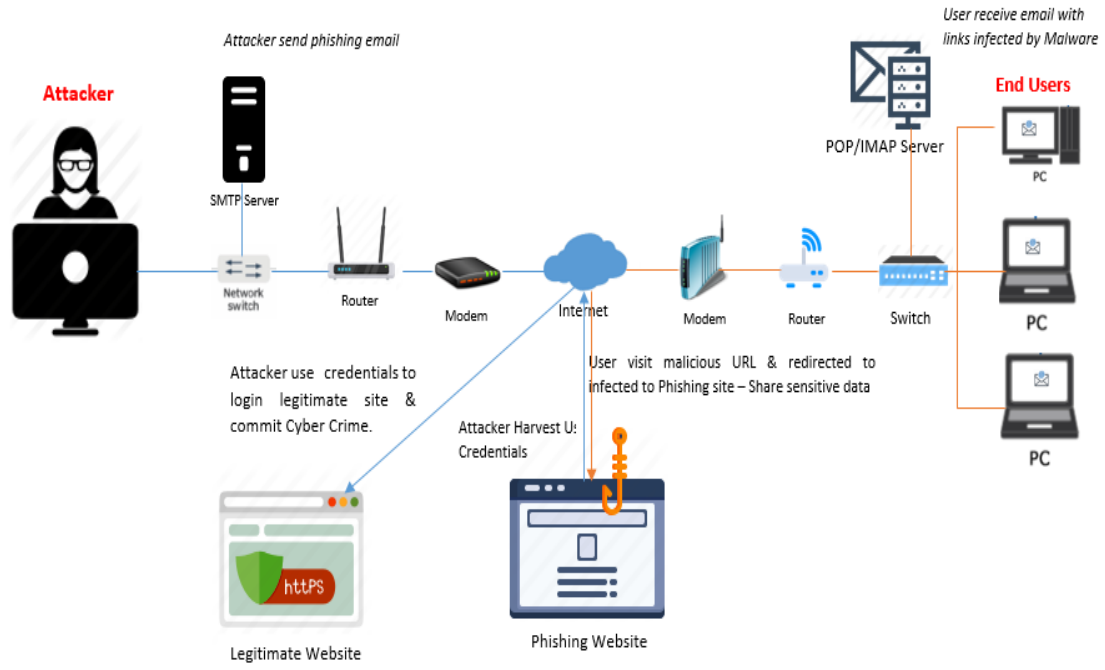
Attacker send phishing email
User receive email with links infected by Malware
Attacker
End Users
POP/IMAP Server
PC
SMTP Server
Network switch
Router
Modem
Internet
Modem
Router
Switch
PC
Attacker use credentials to login legitimate site & commit Cyber Crime.
User visit malicious URL & redirected to infected to Phishing site – Share sensitive data
Attacker Harvest U: Credentials
PC
httPS
Legitimate Website
Phishing Website

Figure 1. Phony Phish System Architecture and Design

As illustrated above, an attacker sends solicit emails to UNAM staff members and requested them to the respondent by visiting a phishing web page and download an application for removing malware. The email was formulated as follows:

Dear UNAM Network User,

Your computer has been infected with a virus and to remove the virus downloads and installs 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,

IT Technician, UNAM Computer Centre

3.2. Data Collection

The data collection for the study consisted of a survey using an online questionnaire. The questionnaire consisted of open-ended questions. Also, a semi-structured interview was organised to collect the expert's primary data.

3.3. Population and Sampling

The survey targeted the entire University of Namibia staff members who frequently use information systems. A significant number of staffs have participated. This includes ten (10) IT professionals at Computer Centre Division and 300 other staffs members such as academics and administrative staffs.

4. Results and Discussions

This section presents different types of end user errors discovered.

4.1. Following links via mail from unknown senders

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 vulnerable attacks comparing to those organisations that lack technical and computer security [16]. Phishing and social engineering are some of the most effective routes to stealing confidential information from organisations.

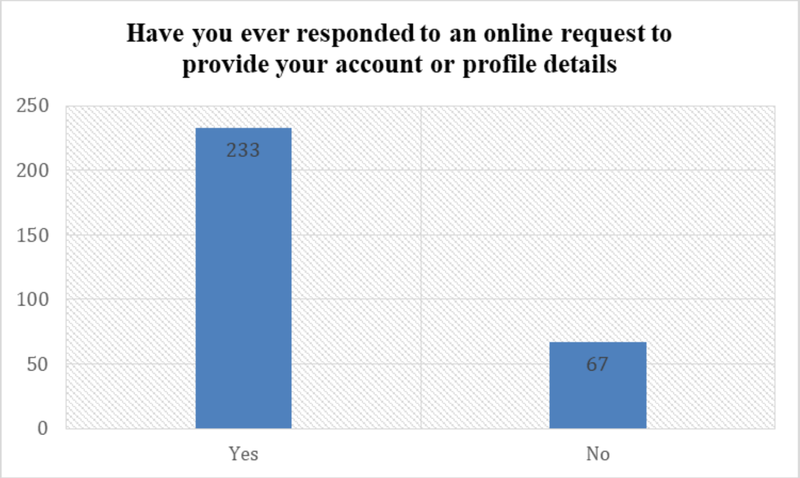

Figure 2. Response to an online request

The questionnaire results showed that 233 participants (77.7%) followed 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 staffs 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 unauthorized users. Hence, educational institutions and individuals must adopt a combination of both technology solutions and user awareness to help protect sensitive information. The findings above corroborate with the findings of Van-Zedlhoff [16], who noted that clicking on links from unconfirmed sources can lead to security breaches.

4.2. Lack of strong password and inappropriate use of password

A password rule is very important. The complexity of passwords is one of the recommended measures in the information security industry. Preferably, a password should be difficult to guess which also implies 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]. Studies revealedthat 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 3 months or more.

Results of this study indicated that 72.3 % of the participants use up to 7 characters as their password 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 do write their password down when it is difficult to remember. Indulging in these practices such as the use of a weak password, writing down and sharing of 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 risks of 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. The findings above conform to the findings of 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.

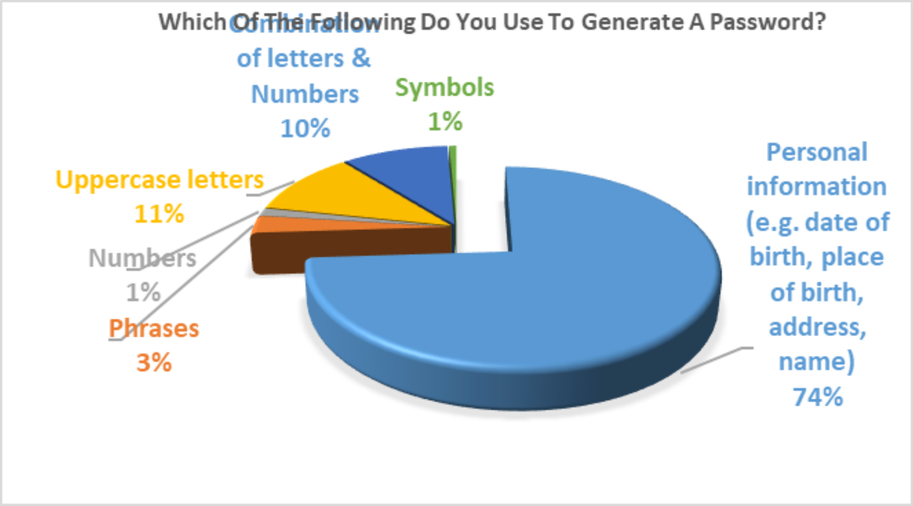

Figure 3. Generation of a password

4.3. Reckless Handling of Computers

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 [17]. In many instances, people do 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 threaten the viability of the university in protecting its information.

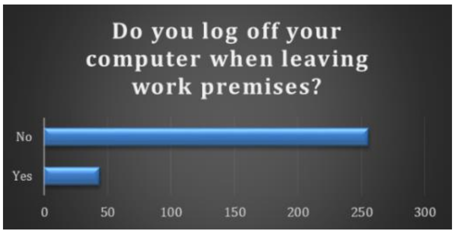

Figure 4. Logging off a computer when leaving work premises

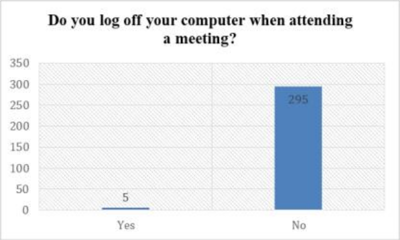

Figure 5. Logging off a computer when attending a meeting

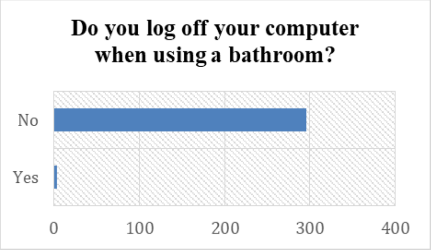

Figure 6. Logging off a computer when using a bathroom

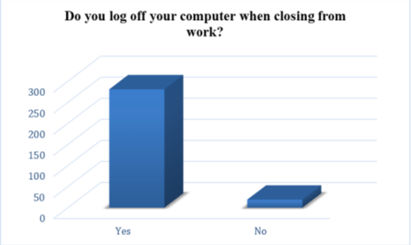

Figure 7. Logging off a computer when closing from work

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 computer even when their workplace. It has been noted also 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 computer even when using a bathroom. Out of the total, 281 UNAM employees do log off their computers when closing from work and 19 of the participants indicated that they do not log off their computer when closing from work. These findings concur with the earlier findings by Evans [18] who indicated that computers that are left idle and unattended may pose a threat to information. Hence, employees should not leave their computers unattended this could put information at risk of being exposed and altered.

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 piece of information available to search for their victims, the most popular source for such a search being the internet and social networks. The study discovered that email is one of the routes attackers use to access a network.When users use the institution network to send and receive emails they are putting the network and information in jeopardy. 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 [23] who indicated that the lack of consistency in privacy settings gives attackers room to operate and phish information to attack the network[19, 21].

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

Lack of strong passwords to social media accounts such as Facebook and Twitter could be an entry point for hackers. Also, unauthorised applications used by users in the university network could compromise the security of the university networks. The institution and worker's personal information could be in jeopardy when unofficial applications are used on the institution network [23]. The unauthorised applications are mostly downloaded from malicious websites. This applicant can come along with viruses, Trojan Horses or worms. The study found out that malicious programs could be spread over the university network when files are downloaded from unknown and untrusted web sites. This could cause a serious security breach. These findings concur with the findings of the study conducted by Gyunka & Christiana [23] which indicated that unauthorised applications used by users in corporate networks could compromise the security of these networks.

4.6. Distant employee security

As institution’s operations become more and more dispersed and transition online, mobile workers increase the potential threat for data [19]. Employees tend to move unfinished work to their devices and take it along at home so that they could work on it later. This is quite risky because often personal computers and devices are less secured compared to corporate ones. The study has shown that improper handling of data, such as moving files from an office device to a home computer that does not have proper IT security measures attracts information theft. Hadlington [19] 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 of the security measures in an institution into a useless process and could put information at risk of theft and other threats.

4.7. Threats from within the institution (inside attackers)

When workers are discontented with their jobs, peeved with their boss, or sentimental for any reason, they can become insider threats who can purposely damage or leak data [19].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 expose information deliberately to hurt the institution because of some reason as stated above. Hadlington [19] indicated that sometimes the problem is not that users ignore security threat 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 attack from disgruntled employees.

5. CONCLUSION AND RECOMMENDATION

Cyber-attacks increasingly became more and more sophisticated as systems get dispersed and distributed over the internet and its root causes are system end-user errors. Hence, this study aimed to identify human errors and recommend possible countermeasures. It was concluded thatentities need to address human actions and not only technologies. Even though the technology is indispensable in the information security structure, relying on technology alone is insufficient to safeguard the university's information system from data breaches. End-users need to be incorporated into an information security model to make the security framework complete. 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 terms of security. System end-users can be the weakest or the strongest aspect in the security framework and therefore should alleviate the deficiencies in the prevailing security technology. For that reason, the study concluded that there is a need for the university to integrate IT technological solutions, however, technology alone is not a complete solution to mitigate cyber-security risks and attacks, rather, consider both software, hardware and human actions to achieve an effective information security management system in the university setting. It is recommended that for the end-user errors in information security to be managed meritoriously, the university must encourage and raise the security awareness of possible security incidents or attacks, risks, threats, vulnerabilities, and data protection requirements. It must also strengthen its ICT policy to serve as a guideline. In addition, the division in charge needs to use security best practices.

ACKNOWLEDGEMENTS

The researcher would like to express unlimited appreciations to the Computer Centre and the entire School of Computing, University of Namibia, for granting permission and making resources available for the research to be carried out.

REFERENCES

[1] N. Uushona. "University Of Namibia ICT Policy". 2016. Available: http://unamintranet.unam.na/documents/ict-policy.pdf.(2016) (accessed July 22, 2019).

[2] J. M. Kizza. "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. "Information System Security Threats and Vulnerabilities". 2016. Available: https://www.researchgate.net/publication/304066003_information_system_security_threats_and_vulnerabilities_evaluating_the_human_factor_in_data_protection (accessed August 31, 2019).

[6] B. M. Bowen, R. Devarajan & S. Stolfo. "Measuring the Human Factor of Cyber Security", 2011. Available: http://www.cs.columbia.edu/~bmbowen/papers/metrics_hst.pdf.

[7] CSB. Cyber Security Breaches Survey. UK: Social Research Institute, 2018. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/cyber_security_breaches_survey_2018_-_main_report.pdf

[8] L. Hadlington. "The Human Factor in Cybersecurity: Exploring the Accidental Insider". *Psychological and Behavioral Examinations in Cyber Security*, 46–63, 2018.

[9] M. Pill. "Top Ten Database Attacks", 2016. Available: https://www.bcs.org/content-hub/top-ten-database-attacks/ (accessed May 18 2020).

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

[11] 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).

[12] 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).

[13] I.M. Kassiri, & A. Shahidinijad. “A survey of on 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

[14] 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.

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

[16] V. Zadelhoff. *The Biggest Cybersecurity Threats Are Inside Your Company.* Harvard Business Review, 2016.

[17] P. Kearney. Security: The Human Factor. 2010. Cambridge Shire: It Governance Publishing.

[18] 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.

[19] 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.

[20] H. Lee. “The Human Factor in Cybersecurity: Exploring the Accidental Insider”. UK: IGI Global, 2018.

[21] Kamara, S., Fahmy, S., Schultz, E., Kerschbaum, F. & Frantzen, M. “Analysis of Vulnerabilities in Internet Firewalls”. 2010. Available: https://www.cs.purdue.edu/homes/fahmy/papers/firewall-analysis.pdf (accessed July 31, 2019).

[22] B. A. Gyunka, & A. O. Christiana. “Analysis of Human Factors in Cyber Security: A Case Study of

[23] S. Bureau. “Human-Centred Cybersecurity: A New Approach to Securing Networks”. *Research at Rit*, 2017-2018, 2018.

AUTHORS

Paulus Kautwima is currently a Lecturer in the School of Computing, Department of Computer Science, University of Namibia. His area of research are 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 PhD 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

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

Nalina Suresh is currently a Senior Lecturer in the School of Computing, Department of Information technology University of Namibia. Her area of research are 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