International Journal of Wireless Communications and Mobile Computing
2021; 9(2): 7-15
http://www.sciencepublishinggroup.com/j/wcmc
doi: 10.11648/j.wcmc.20210902.11
ISSN: 2330-1007 (Print); ISSN: 2330-1015 (Online)

Information Security Mechanisms and ICT Policy in Practice: A Case of the University of Namibia

Paulus Kautwima[*], Valerianus Hashiyana, Titus Haiduwa

Department of Computing, Mathematical and Statistical Sciences, Faculty of Agriculture, Engineering and Natural Sciences, University of Namibia, Windhoek, Namibia

Email address:
pkautwima@unam.com (P. Kautwima), pkautwima@gmail.com (P. Kautwima), vhashiyana@unam.na (V. Hashiyana), vhashiyana@gmail.com (V. Hashiyana), thaiduwa@unam.na (T. Haiduwa)

[*]Corresponding author

To cite this article:
Paulus Kautwima, Valerianus Hashiyana, Titus Haiduwa. Information Security Mechanisms and ICT Policy in Practice: A Case of the University of Namibia. *International Journal of Wireless Communications and Mobile Computing.* Vol. 9, No. 2, 2021, pp. 7-15.
doi: 10.11648/j.wcmc.20210902.11

Received: October 26, 2021; **Accepted**: November 22, 2021; **Published**: December 29, 2021

Abstract: As new technologies emerge in the next generation of wireless communication systems so the continued rise of cyber threats and attacks in higher education institutions. In the wake of COVID-19, however, institutions of higher learning increasingly searched for alternative ways to deliver remote education. Hence, planning for cyber security became a priority and not an option due to the new level of vulnerability posed by human factors as they utilize both licensed and open-source software and wireless devices. Based on this ground, this paper discussed pertinent points on the examined ICT policy and security mechanisms as security practices and strategies implemented by the University of Namibia's Directorate of Information & Communication Technology Services before and post the sudden shift to remote learning. It further proposed alternative strategies to curb vulnerabilities as an element of human action. Key findings show that security breaches do happen mostly due to end-user errors and not always technical issues. A qualitative research method with a random sampling technique guided the study. Virtual interviews and a survey have been used to gather data from security specialists, academics, and administrative staff. Data got analyzed in themes. It has been concluded that both people and technology are essential in information security structure. Increased awareness, training, and improved security practices are the key solutions.

Keywords: Cyber Security, Security Mechanisms, ICT Policy, Information Systems

1. Introduction

Due to the current pandemic, educational institutions around the world had to find new ways of working [1]. To remain competitive and relevant, the University of Namibia (UNAM) embraces the use of digital technologies as its modern approach to education. In response to the pandemic and as part of its transformation, UNAM implemented an e-learning system on a full scale using Moodle LMS. This digital platform and its complementary learning tools are needed to ensure data integrity as far as there are human-computer interactions. Before that, the university had information systems in place to manage its daily operations. It is commonly known that human aspects affect information security and assurance [2]. Information security is when information is in danger due to security threats. Attackers on daily basis are tirelessly trying to penetrate universities' networks, e-mails exchange servers, information system database servers, web servers, end-user devices, and its applications by exploiting vulnerabilities and threats [28]. When security threats materialize it put information in university systems at risk of security breaches such as unauthorized access, sensitive information theft, misuse, and malware infections. In this case, UNAM is not an exception especially during the COVID-19 pandemic where teaching and learning have been fully transitioned online. As security evolves, new security issues arise.

Therefore, this paper pinpoints how the University of Namibia protects its information assets and, above all, its data. Usually, computers and network equipment are physically safeguarded for the following motives: to circumvent theft, harm, unauthorized access, and modification to the university management information systems data, and to avoid interference or denial of services.

According to the Department of Information & Communication Technology Services (DICTS), formerly UNAM Computer Centre which is responsible for setting up security over one million phishing and spam e-mails were detected to have been directed to various UNAM e-mail user accounts. The report further stated that spammers were using zombie computers and techniques such as compromised accounts of UNAM legitimate users to send out endless and impersonating e-mails with links requesting users to upgrade their e-mail account or change their passwords [3]. Shambalula [3] has argued that although UNAM has technological measures in places such as Firewalls running on the gateway, Intrusion Detection System (IDS), and anti-virus to curb possible loopholes within the network, user accounts are still being compromised, resulting from spammers using legitimate user accounts to obtain sensitive information from end-users. Hence, Information Systems are still exposed to attacks even if optimal technological measures are in place. This is perceived as a threat in the UNAM corporate network and e-mails servers. As noted, attacks continue regardless of the existing technical solutions in place hence the university's electronic filing systems are more vulnerable to attacks than before using web services. According to research, databases attacks are prevailing nowadays therefore automated logout systems must be prioritized [18]. Evaluating technological vulnerabilities help protect against targeted attacks [19]. Vulnerability is any flaw or weakness in an information system that can be exploited by hackers or accidentally triggered and result in a security breach or violation of the system's security policy [26]. Tools such as firewall implementations are not always practical enough to analyze and test potential network issues hence vulnerabilities in software and hardware firewalls leave information systems vulnerable [20, 21]. Even though various institutions make use of a high number of technical security controls, they still show a non-proportional number of security breaches [22]. Is postulated that modern encryption and cryptosystems such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are said to be ineffective for a small amount of data encryption due to producing much overhead and increase in complexity [23]. Software vulnerabilities exist due to poor designs and programming errors. Technology-based countermeasures are insufficient [24, 25]. Therefore, does not always guarantee total security [27]. Thus, a lack of understanding of security problems to think that technology alone can solve security problems is a dream since people and technology are inseparable yet users are prone to make mistakes [19, 25].

The overall objective of this study was to (1) examine and discuss existing information security services, mechanisms, and security policies put in place at the University of Namibia and (2) propose further actions to prevent and mitigate end-user risks. Sub-objectives ascertain to (i) stimulate security innovation and creativity in data protection within higher education institutions and (ii) highlight different human elements that can comprise security services and render specific security mechanisms and ICT policy useless in the university context. This study is timely and significant to the body of knowledge as it closes the gap in the literature on the institutions' readiness to fight cybercrimes and during the Covid-19 pandemic. Further, it shares ideas to solve security issues in this fast-changing area of Computing, Wireless, and Mobile Computing.

2. Analysis of Information Security Mechanisms and ICT Policy in Practices at UNAM

The University of Namibia has put in place an ICT policy to guide its resources users. Security policy is considered important for managing the security of information systems [15]. Exploration and analysis of the current state of information security policies in academic institutions illuminate the need to upscale and adopt the latest security solutions [16]. UNAM also applies security services to implement security mechanisms. These security services as asserted in extension 800 (X.800) include authentication, identification, access control, confidentiality, and integrity. Security mechanisms involve specific and none specific (pervasive) mechanisms [11]. In particular, various security mechanisms can be implemented to protect the university's information system from attacks and avoid unauthorized access [4]. Specific security mechanisms used at UNAM include confidentiality, encryptions, identification and authentication, authorization, and access controls.

To ensure information security at the University of Namibia, and the following countermeasures are put in place.

2.1. ICT Policy

The ICT policy serves as a guideline for user actions towards security compliance among the UNAM community while using its network (internet), e-mail systems, computers, and other ITS services such as Finance iEnabler, Personnel iEnabler, Lecturer iEnabler, and UNAM Portal.

2.2. Software Patches and Regular Updates of System Software and Its Applications

There are vulnerabilities in many open source applications. General software patches, upgrade and updates of operating systems and their applications are very much critical to surviving security breaches. Keeping all software up-to-date introduces new features and fixes software bugs and security flaws. Consequently, security fixes via software update protect users against the most common security exploits by black hat hackers. In 2014, attacks increased dramatically, and 60 percent of recorded attacks exploited application weaknesses. Amongst those recorded attacks, 40% of the attacks emanate from shortcomings for which a patch had been issued and 20 percent from the misconfigured application [8]. As part of the patching process, the patch issuer administers a disclosure that details the very nature of the vulnerability that the patch is about to correct. If the network administrator does not patch quickly enough, it gives cybercriminals the time to exploit that vulnerability and infect systems before the patch is installed [8]. This makes it extraordinarily significant to keep all software updated to prevent security incidents. In the case of anti-virus and spyware applications, the program is only as good as the last update [9]. Frequent software updates, particularly those that safeguard against malware, is indispensable as it helps record the names of the up-to-date and leading threats [9]. It was discovered that UNAM updates software frequently, and it is done automatically.

2.3. Malware Protection

Protection against malware is also instrumental in protecting corporate information. This is accomplished through the installation and configuration of anti-malware programs to automatically scan computers and connected devices such as external hard drives, smartphones, and USB devices. Educational institutions should have mechanisms that protect the IS from malware. The common mechanism to protect the university network from malware is anti-virus software. Anti-virus software is an application that safeguards a computer from malicious software called a computer virus. It is recommended that all computers inside the university network should have an anti-virus installed to minimize the chances of attacks and security threats on the network [5]. Therefore, this study found out that the University of Namibia has recommended anti-malware be installed in all computers stationed in laboratories and offices. Even though these newer technologies are being gradually adopted, the user name and password authentication method remain the most widely used procedure for protecting information [10].

Implementing a strong password policy is not all about formulating and enforcing the policy, but it also entails educating system end-users on how to treat and protect the passwords. Educational institutions should train employees on password protection dos and don’ts, such as not writing down the password or using the same password for both work and social media because these are things that users do. The level of protection offered by passwords is directly related to their complexity [4]. A strong password is defined as a series of more than ten characters, at least one change of case, a number in the middle, and a non-alphanumeric character such as hash (#) or ampersand (&) that does not appear at the end of the password [9]. At UNAM, the application of a strong password policy is embraced. The technical team continuously encourages by introducing measures such as the expiration of a password after a month, a password with non-alphanumeric, and no repetition of a password.

2.4. Physical and Network Access Control

The university is also serious about avoiding physical loss or theft of corporate devices. Physical security mechanism to protect computer resources from theft and damage is done in the basic form of locks on doors of computer laboratories and offices [04]. Another ideal strategy towards implementing enhanced physical security is to record all IT equipment's serial numbers for identification purposes and minimize access to computer laboratories and equipment, for instance, servers and switches [12].

The institution could also secure the computers physically by using cable ties to tie all cables together and lock them. This protects the computer from physical theft because a computer cannot be easily taken away as opposed to when cables are not secured with cable ties. All laptops should have locks to secure them on the desk when users are leaving them unattended. Areas with sensitive equipment such as routers, servers, and switches should have access points for employee identification and could embrace safeguarding entrances and exits. The backup storage area should be protected as part of the Disaster Recovery Plan. Information such as the network infrastructure model, indicating the network set up and the devices that protect it should be kept confidential because information of that nature in the hands of an attacker is equivalent to a route map to the front door. This study discovered that the University of Namibia has physical security in place, such as security officers at the entrance of the computer labs, cable ties, and locks for computers' physical security. In addition, network traffics to intranet resources is controlled by implementing an access control list on its local firewall as an added layer of protection.

2.5. Cyber Security Training and Awareness

In UNAM emails, an email warning banner is appended at end of each email received. It acts as a warning message to end-users to be aware of scams or phishing coming through external incoming emails. The main goal of phishing awareness and training among university employees on cyber security attacks have become a priority of the computer center team since ignoring this exercise has the potential to cause security problems that may affect the University Information System badly as employees interact with IS every day to carry out the university day to day operations. On this note, it is a sensible idea for an educational institution to adopt employee security awareness and training to mitigate the chances of attacks on the university network [12]. However, statistically, employee training and security awareness are the lowest on the list of top priorities of the information security budget at 16 and 13 percent, respectively. The existing UNAM policy regarding information security was analyzed to determine what is missing or lacking in the current information security.

2.6. Identification and Authenticating of Users

Access to the data center is controlled by biometric technologies, a verification system that requires the user’s fingerprint. To get access to labs, registered students and staff members are identified by presenting what they have such as staff or student cards. There are also access restrictions, whereby registered user's details are the synchronized school domain and used to and authenticate users prompting for a service. In this case, they are required to present what they know, such as their username and passwords for secure login.

2.7. Secure Remote Access

The remote access technology has advanced corporate productivity, provided online information, facilitated a flexible work schedule, and improved business communication [12]. Both public and private networks provide a channel through which the information can be accessed. Educational institutions have workers who are not fixed at one university campus and need access to the university intranet from a remote site, such as home, hotel, or guesthouse [4]. To maximize the confidentiality, integrity, and availability of data when working remotely. A Virtual private network (VPN) is used to securely connect remote users to the university's network. VPN technology is the method that an educational institution should adopt to secure the communication channels between the distant employee and the university network. VPNs allow users to authenticate data from end to end and prevent unauthorized access to the university intranet [9]. In addition, user traffic is channeled through a secure proxy server as an intermediary to authenticate and safely connect authorized users. Self-managed remote access points are also encouraged from users outside UNAM jurisdiction.

2.8. Hardware Security

Handling of computers that provides service to other computers such as servers is a critical issue nowadays. Controlling what a server can permit and what a server can do is very crucial to information system security. Limiting access to the server is a brilliant idea, just to tighten security. At UNAM server rooms and labs are equipped with security camera recording services that can be viewed and monitored in real-time. Some network ports that are not necessary for operations could be blocked to ensure limited access to the server. Servers can control personal computer (PC) operations and inhibit users without administrative privileges from downloading unauthorized programs. This is a common mechanism used by institutions to mitigate vulnerability to viruses that attach themselves to programs [12]. For this study, the mechanism of locking down servers was investigated in UNAM.

It has been determined that severs and lab computers with Linux and Windows systems were given vulnerability protection utilizing a firewall to prevent access from hostile IP addresses. A firewall can be software or hardware that aids to filter out available attackers and malware that attempt to invade the devices over the Internet. Firewalls are the institution's first line of security and need to be installed regardless of the magnitude of the institution [6]. As most institutions expose their networks to Internet traffic, firewalls are becoming a requirement [7]. Intruders in everyday life are undoubtedly probing institutions with a constant Internet connection. Firewalls defend the university network from unauthorized access by filtering out packets from untrusted networks; it is imperative to take cognizance that firewalls cannot safeguard against attacks that pass via authentic communication routes. It is recommended for the university to have hardware and software firewalls installed so that the software firewall could serve as an alternative to back to the hardware firewall. However, it can only operate on the machine on which it is installed hence the software firewall needs to be installed on all devices or network entry points to provide maximum protection [6]. It has been learned that UNAM firewalls are well-configured firewalls; however, the results also revealed that the firewall could inadvertently block access to some useful sites.

2.9. Intrusion Detection and Prevention

Intrusion Detection System (IDS) also used as anomaly-defense systems which detect network intrusion, threats (i.e. data breach, misuse of information systems or manipulation of information and corruption of data), and attacks (i.e. unauthorized access, identity theft, denial of service, and man in the middle attack) in the institution systems and also to help to trace information about the attacker afterward. The audit trails and logs file logs information regarding attacks for specific IS [4]. Usually, an intrusion detection device is network equipment located on a reflected network switch port and reviews network traffic between switches to identify any possible presence of wicked bit patterns. It uses statistical anomaly or pattern matching detection. These systems can also be host-based. It is a virtuous idea to use intrusion detection systems along with access control because access controls alone cannot fully control unauthorized access to the institution network [13].

2.10. Encryption

To encrypt content in transit via the Unam website, the institution has a secure certificate that uses communication such as protocols Secure Sockets Layer (SSL) and Transport Layer Security (TLS). On its website, UNAM uses web application security such as cryptographic security protocols such as HTTPS protocol that leverages the services of SSL or TLS SSL Certificate and ensures confidentiality to web traffic and data integrity by authenticating communicating agents (client and server) [17]. It also uses vulnerability scanners such as Acutenix to check its website for possible vulnerabilities in configurations and attacks such as site scripting, SQL injections, etc.

2.11. Account Management

In accord with the university security policies, staff computers that are connected to the domain are configured to automatically log out users and lock the device after a period of inactivity. Also, emails systems block users on a maximum of three incorrect login attempts. This enhances email access security at the university.

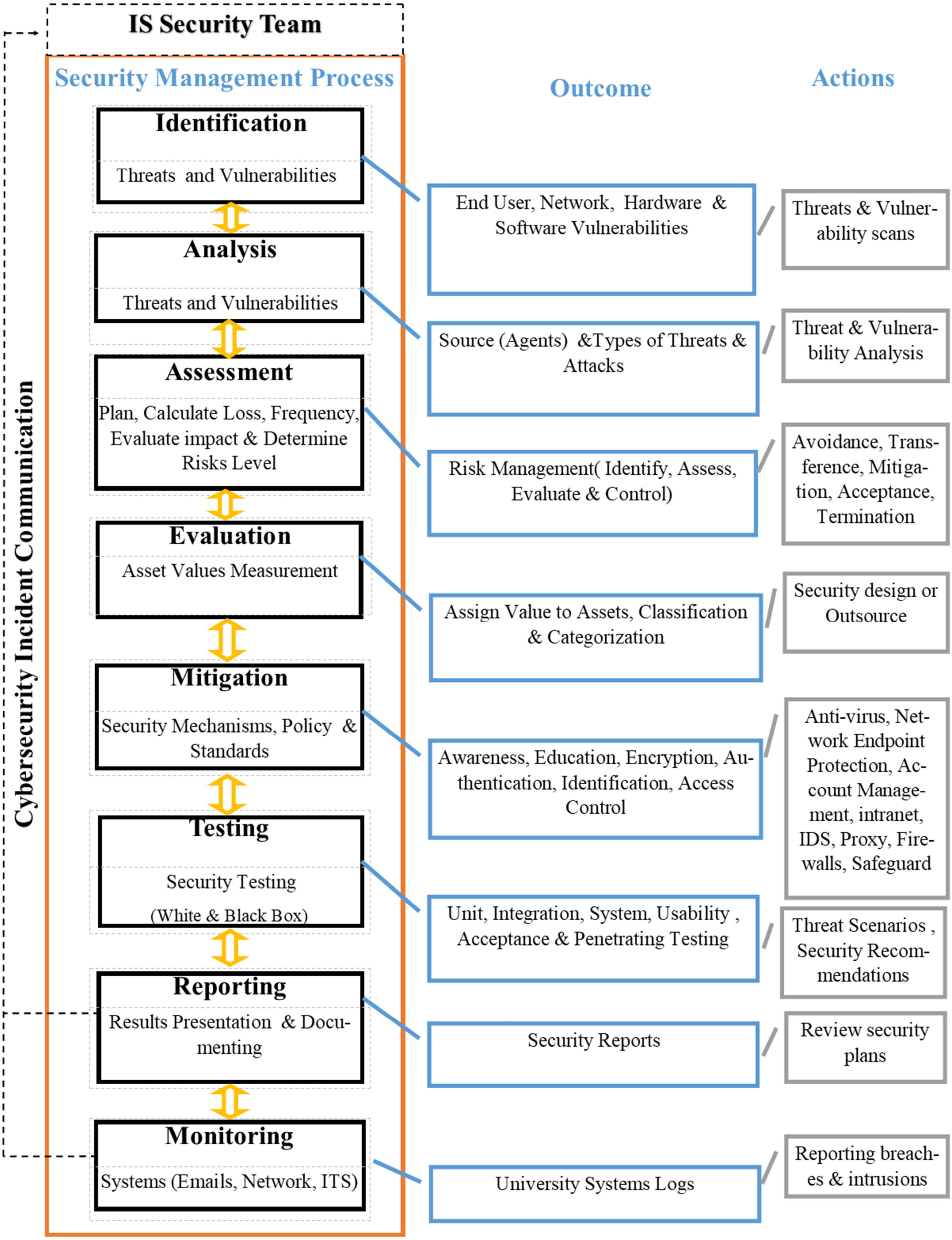
IS Security Team
Security Management Process
Outcome
Actions
Cybersecurity Incident Communication
Identification
Threats and Vulnerabilities
Analysis
Threats and Vulnerabilities
Assessment
Plan, Calculate Loss, Frequency, Evaluate impact & Determine Risks Level
Evaluation
Asset Values Measurement
Mitigation
Security Mechanisms, Policy & Standards
Testing
Security Testing
(White & Black Box)
Reporting
Results Presentation & Documenting
Monitoring
Systems (Emails, Network, ITS)
End User, Network, Hardware & Software Vulnerabilities
Source (Agents) &Types of Threats & Attacks
Risk Management(Identify, Assess, Evaluate & Control)
Assign Value to Assets, Classification & Categorization
Awareness, Education, Encryption, Authentication, Identification, Access Control
Unit, Integration, System, Usability , Acceptance & Penetrating Testing
Security Reports
University Systems Logs
Threats & Vulnerability scans
Threat & Vulnerability Analysis
Avoidance, Transference, Mitigation, Acceptance, Termination
Security design or Outsource
Anti-virus, Network Endpoint Protection, Account Management, intranet, IDS, Proxy, Firewalls, Safeguard
Threat Scenarios , Security Recommendations
Review security plans
Reporting breaches & intrusions

Figure 1. *Information Systems Security Management Preliminary Conceptual Framework.*

3. Perspectives on Challenges of Security in Universities and Possible Solutions to Human Errors

3.1. Perspectives

Ensuring data protection in institutions of higher learning proved to be a challenge. This difficulty could be attributed to the fact that there is a higher number of users within universities. Hence a myriad of end-user actions happen. Many are easily tricked through social engineering and phishing. It has also been noted that human errors are infinite, and it is nearly impossible to know the causes of human mistakes. Also, people's behavior towards security controls differs. Ignorance, negligence, lack of information security literacy, competency, security awareness, and best practices top the list. In the exception of human errors, it must also be stated that many applications or system software are not designed with security in mind. Security principles are simply afterthought mechanisms; hence users use them without understanding the underlying weaknesses or security vulnerabilities due to design problems in source code; thus, end-users become victims due to their actions and eventually attacks against systems. Errors usually occur due to software failures at the sender or receiver side and buffer overflow rather than errors in the network [10]. This positions human security as the major challenge and concern in general. It also shows a shocking gap between perceived priority and the level of users' security preparedness. Hence leading to this investigation.

3.2. Proposed Solutions

3.2.1. Employee Education and Training

Since most data protection approaches such as encryption are more technical. Universities need to put human factors at the center and implement end-user security assessment strategies to measure and evaluate the level of adherence to rules stipulated in the enacted ICT policy. Also, universities should ensure continuous education on specific mechanisms to control and protect their privacy and data, security skills training of users, security awareness campaigns, controlled access, account monitoring, worker background screening, system audit logs, continuous vulnerability assessment, secure system configuration, malware and network controls [8]. Further, researchers proposed a preliminary conceptual framework for managing information system security in Institutions of Higher Education (IHE) to ensure human error inclusion in system defenses. The components of a preliminary framework aim to guide in managing security incidences in a university information system.

3.2.2. Proposed Preliminary Conceptual Framework

Figure 1 presents an Information Systems Security Management Preliminary Conceptual Framework. This conceptual framework can be considered valuable in any institution of higher education as it illustrates system variables and their relationship in ensuring information security requirements. It contains processes and steps needed to effectively manage vulnerabilities, threats, and risks associated with human actions in university information systems. The proposed conceptual framework further highlights the expected outcomes of the processes as well as specific actions needed thereof. Its primary aim is to bridge the divide between information security technical countermeasures and soft countermeasures for human errors. This gap can be closed by analyzing end-user errors for possible causing security breaches and by studying conflicting attitudes of employees on security in the organization. Study results demonstrated that the divide could be bridged by effective communication, awareness, training, and education.

4. Materials and Methods

This study adopted a qualitative approach with an exploratory research design to find, collect, analyze and interpret information. In particular, this research approach has been applied by studying and analyzing textual information conveyed in scholarly work such as books, journals, and pre-reviewed conference articles.

Data collection tools include online interviews and a survey. The interviews were done with security professionals from the University of Namibia's Computer Centre, while a survey was administered to UNAM’s wide community. A simple random sampling technique has been applied to select individuals to participate in the interview. This strategy gave an equal chance for everyone to participate in the study. An e-mail with a humble request to participate in a survey was sent out to the UNAM community. The survey had open needed questions accompanied by an informant consent that explained the purpose of the research.

Before the study began, an ethical clearance certificate was requested and obtained from the university ethical clearance committee. The study ensured confidentiality, unanimity, and integrity. The qualitative data has been analyzed, interpreted, and presented in the form of direct quotes in section 3.

5. Results and Discussions

Qualitative data analysis has been done to interpret and understand data arising from transcripts, observations, interviews, and the survey. Researchers surveyed and interviewed specialists from Computer Centre on cyber security in the university. An online survey has been, however, addressed to UNAM Community to ensure inclusiveness. Results of the interview from participants in this study are presented below in the form of citations:

Participant 1 was quoted saying, "UNAM has a firewall installed, and this saves the university from attacks by blocking traffic from untrusted sources and protects information from being disclosed to intruders". This was further supported by Participant 2, who stated, "The university network has a firewall installed which filter out network traffic from unverified or suspicious sites or sources, UNAM firewall can even block useful sites, and hence the installed firewall does not allow any traffic from untrusted sites.

This issue was further strengthened by Participant 5, who said that "UNAM has properly configured firewall which filters out network traffic from suspicious sources. Firewalls had been the first line of defense in UNAM network security for over 25 years."

In terms of the frequency of reconfiguration, participant 4 indicated, "Our university firewall is usually reconfigured once a year" This issue was further strengthened by participant 8, who said, "Reconfigurations UNAM firewall is ad-hoc basis". These findings testify that firewalls are the institution's first line of security and need to be installed regardless of the size and magnitude of an institution also, further validate the earlier findings that most institutions expose their networks to internet traffic, firewalls are becoming a requirement for every institution [6, 7].

Updating software is an essential part of keeping a computer secure, and keeping all software up-to-date will protect a user or institution against the most common security exploits. If the software is not up to date, this could lead to unauthorized access to computer systems, which may result in the vulnerability of sensitive information such as student marks, salary details of employees. The participants in the study indicated that their computers have recent software which is updated regularly.

Participant 7 was quoted saying "UNAM computers have an up-to-date software and are updated three or more times a year; this is securing UNAM computers from malicious software infections". This was further supported by Participant 9, who stated that "Software update automatically depending on their requirements and this could safeguard computers from malware."

These findings concur with Wash et al. (2014), who indicated that updating software is essential for keeping a computer secure. Keeping all software up to date could protect a system user against the most common security exploits. If the software is not up to date, it gives a hacker carte blanche to exploit any identified vulnerability and infect the system [26]. Hence it is extraordinarily imperative to keep all software updated to prevent security incidents.

Protection against malware attempts to identify, prevent and eliminate computer viruses and other malicious software. Ten participants, representing 100% of the research sample, indicated that they had anti-virus software installed and the anti-virus updates automatically as new updates occur. One of the respondent's words is as follows.

Participant 10 said, "The University has anti-virus software installed which updates automatically as new updates occur". On this issue participant, 9 had this to confirm that "UNAM has Kaspersky anti-virus installed from preventing computers from malware". Having anti-malware installed provides an assortment of security protection and monitoring of spams, viruses, and spyware.

Implementing a strong password policy is important as it includes developing and enforcing the policy and educating employees about how they should be protecting their passwords. Enforcing password rules is an effective step in sustaining information security [8]. Informants representing 50% of the research sample confirmed that are aware of email password policy such as non-repetition of password characters, password expiration, and prohibition of username as a password. Regarding the password length, 1 of the respondents indicated that they had six or more character password length while 9 IT professionals indicated that their password ranged between 7 or more characters in length. Ten respondents indicated that their passwords consisted of numbers, upper and lowercase, symbols, and special characters concerning the characters that constitute a password. The verbatim quotes below are extracted from the MS excel sheet where participant's data is exported after a survey. They claimed as follows:

Participant 1 further revealed that "UNAM has a password in place such as non-repetition of a password, which implies that a user cannot reuse the same password after it expires, the system always prompt for a never used password". This issue was further strengthened by participant 3, who indicated that "Our university has a password which expires after one month, which means we have password expiration as an additional measure to our password policy" Participant 4 had this to say on the issue "UNAM system prohibits the use of the username as a password and the password length is six or more characters, all these are measures in the password policy."

These findings show that implementing a strong password policy educates employees about how they should be protecting their passwords. A strong password should have more than eight characters, at least one change of case, a number that is not at the end, and a non-alphanumeric character such as & or * that are also not at the end of the password.

Physical security measures can be as simple as putting locks on doors and adopting a disaster recovery plan [6]. When a question was presented to the IT professionals to investigate if they had implemented security measures to protect their computer assets, ten IT professionals said that they had implemented physical security measures to protect their computer assets. Laptops are locked to desks, and physical access is highly restricted to staff. The citations below from the participants endorse these claims: "UNAM has physical security measures in place as our computers have locks and cable ties as a physical security measure to protect computers from theft as a threat to information" (Participant 7). This was further supported by participant 5, who said that "UNAM has disaster recovery plan, which means we can back up our data even if computers in the university are destroyed by disasters such as fire or theft."

These findings concur with the fact that physical security measures could be simple as putting locks on doors and adopting a disaster recovery plan. Sensitive areas should have an access point for identifying workers and could include safeguarding entrances and exits [4]. The remote access technology has advanced institutions output, catered for online information, simplified, flexible work schedule, and enhanced business communication. Hence both public and private networks provide means for accessing organizational information. All the participants (100%) indicated that they have remote users, and they connect to remote users securely using virtual private network (VPN) communication which can never be intercepted. The citations below from the participants validate these claims:

"We have remote users, and we connect to remote users securely using VPN communication which can never be intercepted" (participant 1). This was further supported by participant 2, who indicated that "UNAM connects to its remote employees securely with the help of VPN, which contain encrypted data in its channel making it difficult for information to be compromised"**.** These findings support the fact that VPN technology had been the tool to secure communication between mobile employees who need to remotely access the institution's network [4]. VPN channels are secure as it contains encrypted data. On this note, it is concluded that UNAM connects securely to remote users.

Management of servers is very important in today's world of information security. Limiting what a server can do and what it can allow is an effective way to protect this vital network component. Security personnel who participated indicated that they had secured server rooms, as server rooms are locked and had biometric authentication. Participant 7 claimed: "Our server rooms have locks to prevent unauthorized access or entry" (Participant 8). This issue was further validated by participant 9, who was quoted saying "Our server rooms are always locked have authentication as a security to avoid unauthorized entry". Indeed, limiting exposure to servers is always a good idea [12]. Scanning open ports and blocking ports that are not needed for operation also limits servers' exposure and reduces attacks.

Intrusion Detection Systems are crucial in network security because they detect network attacks in progress and assist in post-attack forensics. At the same time, audit trails and logs serve a similar function for individual systems [14]. When the questions were presented to the respondents to investigate if the institution had a properly configured intrusion detection system, the majority of the participants said that they had an intrusion detection system that sends alerts to the admin in case of paranoid or suspicious activity. The citations below from the participants substantiate these claims:

Regarding the configuration frequency, participant 9 said, "Our IDS is configured once every year". This was further confirmed by participant number 10 narrated that, "We have an intrusion detection system which sends alerts to the administrator in case of suspicious activity". This demonstrates that is a good idea to use IDS along with access control because access control alone may not be sufficient.

When asked about how they perceive cyber security at UNAM, survey respondents indicated the following: "My Junk mail is full of spam e-mails claiming to come from IT support"(Participant 10). "As far as I know, e-Mail Spam and Phishing are something common in UNAM e-mail systems" (Participant 13). "It is difficult to distinguish between legitimate e-mails and malicious e-mails." (Participant 11). "I received many e-mails asking for personal information and some with links and pop-up windows that redirect users to fake websites" (Participant 15). "Cyber security awareness among staff and students is needed" (Participant 17). "Cyber threats and attacks are common today. I feel at risk every day" (Participant 19).

Most survey respondents indicated they had been exposed to cyber security incidents before, many of which were delivered via e-mails. Although information security policies and procedures are in place, not everyone agrees to them. The insight also tells us that everyone is responsible and the computer center needs to keep upgrading its security strategies and tools.

6. Conclusion and Recommendations

COVID-19 disrupted teaching and learning worldwide, therefore, leading to the blended mode of studies that constitute the use of both faces to face and online classes using distributed systems and ubiquitous portable computing devices, wired and wireless connectivity (internet), and web 2.0 technologies, thus bringing security concerns in universities efforts to wirelessly communicate and interact with students. Therefore, the study concluded that using technology in teaching and learning in higher education can be both rewarding and challenging. However, technology alone is inadequate to safeguard the university's information system from possible attacks. Despite the fact, the University of Namibia implemented all the recommended best practices in security assurance it continues to face security challenges. In modern times, it is recommended that users' education and training on basic information security shall not be ignored. Continuous training and awareness on how to protect systems from cyber-attacks is a necessity and not an option in academia. Hence, the study concluded that information breaches happen not only because of technical issues or lack of tech-know but because of users' attitudes and actions toward security. The study further recommended the implementation of the conceptual framework as proposed in section 2.

Acknowledgements

The authors would like to thank everyone who participated in this study, particularly respondents and IJWCMC reviewers.

References

[1] Jahankhani, H., Kendzierskyj, S., Akhgar, B: Information Security Technologies for Controlling Pandemics (2021) DOI: https://doi.org/10.1007/978-3-030-72120-6

[2] Furnell, S, Clarke, N.: Human Aspects of Information Security and Assurance. 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, July 7–9 (2021).

[3] Shambalula, M.: Be Cyber Savvy. UNAM Computer Centre. (2019).

[4] Sai, K., Manjeese, C., Mawere, J., Denture, T., Prosper, T.: An Overview of Information Systems Security Measures in Zimbabwean Small and Medium-size Enterprises. Research Inventory: International Journal of Engineering and Science, 6 (2), 21-26 (2016).

[5] Alkandary, Y. H., Alhallaq, F. M.: Computer Security. International Journal of Advanced Research in Computer and Communication Engineering, 5 (1), 1-6 (2016).

[6] Microsoft Safety Security Center. (2014) https://www.microsoft.com/security/pc-security/firewalls-whatis.aspx, last accessed 2020/12/20.

[7] Laudon, K. C., & Laudon, J. P.: Management Information Systems: Managing the Digital Firm (14th Ed.). Essex: Pearson Education Limited (2014).

[8] Paul Lin, P.: System Security Threats and Controls. The CPA Journal, pp. 58-66 (2006).

[9] Namaya, A., Mirza, A: Understanding Awareness of Cyber Security Threats among IT Employees. International Journal of Civil Engineering and Technology, 33-35. (2018).

[10] Helkala, K., Bakas, T. H.: Extended results of Norwegian password security survey. Information Management & Computer Security, 22 (4), 346 – 357 (2014).

[11] Stallings, W.: *Network Security Essentials*: Applications and Standards. 4th Edition. Pearson Education, ISBN 13: 978-0-13- (2), 21-26, (2016).

[12] Sun, J., Ahluwalia, P. & Koong, K. S.: The more secure the better? A study of information security readiness. Industrial Management & Data Systems, 111 (4), pp. 570-5 (2011).

[13] CSB. Cyber Security Breaches Survey. UK: Social Research Institute. (2018).

[14] Sai, K. O., Gumbo, R., Mzikamwi, T., & Ruvinga, C.: Classification of Point of Sale information Security Threats: Case of SMEs in Zimbabwe. Research Inventory: International Journal of Engineering and Science, 5 (9), 33-36 (2015).

[15] Weidman, J., Grossklags, J.: What's In Your Policy? An Analysis of the Current State of Information Security Policies in Academic Institutions, (2018). Research Papers. 23. https://aisel.aisnet.org/ecis2018_rp/23

[16] Karyda, M. Kiountouzis, E. Kokolakis, S.: Information systems security policies: a contextual perspective, Computers & Security, Volume 24, Issue 3, pp. 246-260, (2005) https://doi.org/10.1016/j.cose.2004.08.011.

[17] Eric, C., Seth, M., Joshua, F.: Chapter 3 - Domain 3: Security engineering, Eleventh Hour CISSP® (Third Edition), Syngress, pp. 47-93, (2017). https://doi.org/10.1016/B978-0-12-811248-9 00003-6.

[18] Hadlington, L.: The human factor in cybersecurity: Exploring the accidental insider. In Psychological and Behavioral Examinations in Cyber Security, 46–63 (2018).

[19] Kamara, S., Fahmy, S., Schultz, E., Kerschbaum, F., Frantzen, M.: Analysis of vulnerabilities in internet firewalls. (2018) https://www.cs.purdue.edu/homes/fahmy/papers/firewall-analysis.pdf

[20] Kashefi, I., Kassiri, M., & Shahidinijad, A.: 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), pp. 585-591. (2013).

[21] Shannon, S.: The human factor of cybersecurity. (2019).

[22] Soomro, A. W., Nizamudin, A., Iqbal, U., Noorul, A.: A secured symmetric key cryptographic algorithm for the small amount of data. 3rd International Conference on Computer and Emerging Technologies. (2013).

[23] Lee, H.: The human factor in cybersecurity: Exploring the accidental insider. UK: IGI Global. (2018).

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

[25] Kaspersky Lab.: Software Vulnerabilities. (2013) http://www.securelist.com/en/threats/vulnerabilities?chapter=35

[26] Lambert, S.: What is the purpose of a Threat and Risk Assessment (TRA)? (2014). https://www.modernanalyst.com/Careers/InterviewQuestions/tabid/128/ID/3011/What-is-the-purpose-of-a-Threat-and-Risk-Assessment-TRA.aspx

[27] Alavi, R., Islam, S., Mouratidis, H: A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations. (2014). In: Tryfonas T., Askoxylakis I. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2014. Lecture Notes in Computer Science, vol 8533. Springer, Chamhttps://doi.org/10.1007/978-3-319-07620-1_26

[28] Mbowe, J. E., Zlotnikova, I., Msanjila, S. S., Oreku, G. S.: A Conceptual Framework for Threat Assessment Based on Organization's Information Security Policy. Journal of Information Security, 5, 166-177. (2014). http://dx.doi.org/10.4236/jis.2014.54016

Biography

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, e-government, and educational technologies.

Valerianus Hashiyana is currently a Senior Lecturer at the 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

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's Degree in Engineering with a specialization in Software Engineering from Wuhan University.