International Journal of Information Processing and Communication (IJIPC) Vol. 7 No. 2 [December, 2019], pp. 83-99

Online: ISSN 2645-2960; Print ISSN: 2141-3959

A Qualitative Case Study of Cybercrime Types on Ahmadu Bello University's Network

[1]Bukhari Badamasi, [2]Shitu Musa and [3]Aminu Musa Umar

[1]Department of Library and Information Science, Ahmadu Bello University, Zaria, Nigeria
[2,3]Kashim Ibrahim Library, Ahmadu Bello University, Zaria, Nigeria

Email: bbadamasi@abu.edu.ng; mshitu21@gmail.com and aminumusaumar@gmail.com

Abstract

Cybercrime denotes criminal acts that are being committed through the use of computers, mobile devices and the Internet. In the recent time, there is high prevalence of cybercrimes in various organisations both public and private such as banking sectors, security organisation, insurance companies as well as higher institution of learning (universities). Universities have become one of the victims of cybercrime globally where many universities have in one way or the other suffered network breaches and data loss because of the failure of security protocols. This study investigates the causes and types of cybercrimes experienced in Ahmadu Bello University's Network, in order to provide necessary measure to prevent further occurrence. The study adopted qualitative case study research design, using interview as an instrument for data collection. The population of the study consists of 123 staff of the Institute of Computing, Information and Communication technology (ICICT) where 15 staffs were sampled using purposive sampling technique. While the data collected was analyzed thematically. The findings of the study indicated that social engineering, denial of service attacks, website defacement were among the types of cybercrimes occurring on the university network. It is therefore recommended that use of firewall, antivirus, mikrotik servers, and demilitarized zone among others. This when put in place will go a long way in curbing the menace of cybercrimes in universities in Nigeria and beyond.

Keywords: *Advanced Persistent Threat, Computer Information System Company, Computerized Information System*

1. Introduction

The advancement in Information and Communication Technology (ICT) and the Internet has brought a lot of transformation in every sphere of our everyday life. The Internet as described by Zittrain (2006), is a global computer network that provides a variety of communication facilities using standard communication protocols. The Internet has become a very effective tool for all forms of business transactions in every organization. Its usage now spans the globe as organizations around the world are increasingly depending on it for the facilitation of their business transactions. The use of Internet in today's businesses makes it possible to obtain information, exploit new ideas and even facilitate business alliances across the globe using different form of technologies. The technologies are now being rapidly integrated into various departments of universities. However, the rapid integration of technology also comes with its own challenges. One of the challenges being faced by universities is the perpetuation of

Online: ISSN 2645-2960; Print ISSN: 2141-3959

cybercrime activities by cybercriminals. Halder and Jaishankar (2011) described cybercrime as offences that are committed against individuals, property, or government, with the motive to cause physical or mental harm or even cause reputational damage, either directly or indirectly, using modern technologies that comes with the Internet and telecommunication devices. According to Kenya – based IT and business advisory firm Serianu, "cybercrimes cost African economies $3.5 billion in 2017. In that year, annual losses to cybercrimes were estimated for Nigeria at $649 million, and Kenya at $210 million. Likewise, according to the South African Banking Risk Information Centre (SABRIC) South Africa loses $157 million annually to cyberattacks" (Kshetri, 2019 p. 1). According to Omodunbi, Odiase, Olaniyan and Esan (2016) the alarming growth of the internet and its wide acceptance has led to increase in security threats. In Nigeria today, several internet assisted crimes known as cybercrimes are committed daily in various forms such as fraudulent electronic mails, pornography, identity theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy and phishing.

Cybercrime has become a major concern for every organisation nowadays; however, more recently there has been a high increase in the number of cyber attacks on institutions of higher learning Also, about seventy percent (70%) of Universities in UK became victims to phishing attacks. In the same vein, The University of Manchester reported an email phishing scam targeting international students where many students received a fake invoice via email requesting mandatory payment for services for their arrival in Manchester (Strawbridge, 2019). According to a news report by NBCNews (2013), a student at the University of Nebraska, United States, hacked into the University's database and compromised the records of about 650,000 current and old students. Another security breach occurred at the University of Pittsburg (PTT) in 2013, where hackers compromised PTT's server and obtained private information of students and staff. The hackers then threatened to release the information publicly unless the university apologised for the lack of security on the server (NBCNews, 2013). Recently, according to Strawbridge (2019) Lancaster University experienced a sophisticated cyber attack where data from undergraduate applicants for 2019 and 2020 was retrieved and student record systems were also breached in the attack. Looking at the traction of cybercrimes in academic institutions, Ahmadu Bello University, Zaria is not an exception. Therefore, this study is aimed at investigating the causes and types of cybercrimes experience in the Ahmadu Bello University Network. The main objective of this paper is to identify the causes and the different types of cybercrime and how they are perpetuated on Ahmadu Bello University, Network.

2. Literature Review

2.1 The Concept of Cybercrime

Cybercrime is a form of criminal activity that involves the use of a virtual medium such as the Internet. It also involves illegal access to computer data via the Internet (Goldsmith and Wu, 2006). It is one of the prevalent, challenging and intricate problem in cyberspace (Poonia *et al.*, 2013). For example, Millet (2015) reported an instance in Poland where hackers targeted airline travelers and successfully grounded around 1,400 passengers. Similarly, the United Kingdom (UK) security intelligence's database was reported to have been hacked into, and this resulted in compromising the confidentiality of e-mails and personnel information of security personnel (Shimomura and Markoff, 1995). United Nations Office of Drugs and Crime (2013), stated that private sector enterprises in Europe reported serious cybercrime threats while performing online transactions. In the same study, it was further indicated that 16% of cybercrimes were due to intrusion, phishing or e-mail spamming. Some of these problems could threaten nation's security, universities' infrastructure or individual's computer systems, and even communication devices in organizations. As Akogwu, (2012) pointed out that such crimes may threaten nation's security and financial wellbeing.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

2.2 Types of Cybercrimes and Factors Contributing to Its Increase

In recent years computer crime and how to tackle it has become a great issue of concern. Nowadays in Nigeria, cybercrime has become one of the means for pilfering money and business espionage. According to Check Point, (a global network cyber security vendor), as of 2016, Nigeria occupied 16th position in cyber-attacks vulnerability countries in Africa (Ewepu, 2016). Nigerians both at home and abroad are known to be rampant perpetuators of cybercrimes (Omodunbi, Odiase, Olaniyan, and Esan, 2016).

Unsurprisingly, the increasing use of the Internet creates new opportunities for cybercriminals. The cyberspace being virtual, that is, where transaction could be made without physical contact, has created new phenomena that are notably distinct from the (mere) existence of computer systems, but also provide opportunities for crime and criminals. Persons may, for example, commit crimes on the Internet that they would not otherwise committed in physical space due to their status and position. As supported by Jaishankar (2011) who stressed that, identity flexibility, dissociative anonymity and lack of deterrence may serve as contributing factors and may provide opportunities for criminal behaviour in cyberspace.

Looking at the types of cybercrimes mostly experienced in organisations and organizational institutions, Ribadu (2007) stated that the prominent forms of cyber crime in Nigeria are cloning of websites, false representations, internet purchase and other ecommerce kinds of fraud. Olugbodi (2010), states that the most prevalent forms of cyber crime are website cloning, financial fraud, identity theft, credit card theft, cyber theft, cyber harassment, fraudulent electronic mails, cyber laundering and virus/ worms/ Trojans. Cybercrime at universities is a challenging area for information technology (IT) professionals (Carolina, 2014). Students' passwords, credit card details, grades as well as alumni information can be obtained by hackers (Carolina, 2014).

Several scholars have expressed their views concerning causes of cybercrimes for instance, Nadiah (2014) observed that, like many crimes committed physically where money is a major motivator, likewise cybercrimes. According to Amit and Schoemaker (2012), the high level of unemployment , urbanization and massive movement of people from rural settlement to cities are contributing that leads to the increase of cybercrime-related activities. To buttress this further, Ionescu (2012), lamented that, cybercrimes are associated with high rate of unemployment, harsh economic conditions, and poor educational system. Levy and Lemeshow (2013), indicated that, the factors contributing to the increase in cybercrime includes: economic factor (get rich quick syndrome), urbanisation, difficulty in tracing cybercriminals, loose laws in some countries (e.g. Nigeria) and negligence of some IT staff. Kahoka (2015), observed that the negligence of some IT staff in organisations also contributes to the increase in cybercriminal-related activities. The negligence may be in form of revealing passwords that is meant to be confidential to friends, using sensitive data in a public place and even storing data without protecting it. Cybercriminals can take advantage of such negligence and use it to obtain, manipulate and forge information. The negligence is very closely connected with human conduct (Kahoka, 2015). In another related study, The perception of low risk and very high financial reward is also prompting many cybercriminals to engage in phishing, identity theft and fraudulent money request attacks (Castell, 2013).

Online: ISSN 2645-2960; Print ISSN: 2141-3959

3. Theoretical Framework

Routine Activity Theory (RAT) was adopted for this study. The theory indicates that Crime occurs when there is an intersection in time and space of a an attractive target, motivated offender, and a lack of capable guardianship (Felson & Cohen, 1979). For the purpose of this study attractive target connotes the study area (Ahmadu Bello University) and motivated offender (the intentional or unintentional cybercrimes). It is assumed that offenders (cybercriminals) on the Internet may commit a crime by luring their victims into their snare. RAT posits that in order for a cybercrime to take place there is the need to have an offender with criminal inclinations and the ability to carry out the crime. Lastly, a capable guardian: this can be any security mechanisms that could intervene and prevent cybercrime from occurring. Based on the aforementioned theoretical construct, the current weakness or strength of security protocols will have direct bearing on the prevention of the different type of cybercrimes on the University network. However, even with the presence of the capable guardian in the form of the systems administrator and the security protocols, Ahmadu Bello University still experiences cybercrimes. In a university, web and database servers can equally be affected if security protocols are not properly implemented and well managed. Therefore, it is in the interest of the University to improve its security protocols to regain the confidence of its end users. This section stands on the premise that the more effective the guardian, the more difficult it becomes for cybercriminals to infiltrate a Network. Conversely, guardians' weaknesses are vulnerabilities that can be exploited.

4. Methodology

In this study, a qualitative research method was employed, which allows the researcher to collect data through semi-structure interview, and document analysis. An exploratory research design was used in this study in order to provide the needed insight and to understand the types of cybercrime experienced at Ahmadu Bello University. The study site is Ahmadu Bello University, Zaria; it is one of the largest academic institutions in sub-Sahara Africa, situated in the city of Zaria. Currently, the university covers a land of 7,000 hectares and has 2 campuses, 16 faculties, 99 departments and 16 research institute. The University has a data center hosting about 150 different servers and several databases that contains different confidential information of both students and staff.

For consistency, coordination and reliability, the researcher considered (in this study) the staff of the six different units under the Institute of Computing and Information Communication Technology at Ahmadu Bello University as the target population. These units and their population are i. Information Technology Academy (ITA) 14, Management Information System (MIS) 19, Computing and Academic Support Services (CASS) 35, Research and Development (R&D), 10, Software Development Unit (SDU) 22 and Network Infrastructure and Security (NIS) 23. The overall population of this study is one hundred and twenty three (123).

4.1 Sample

At the time of the study, the total population of is 123 staff members of the ICICT Directorate. Therefore, a total of 15 participants were purposely selected as sample of the study, this is base on their expertise. The selected participants from the different units were experts in areas of network management, vulnerability assessments, penetration testing, IT management and cyber threat analysis. The data collected was analysed thematically in which the researcher identify, and interpret patterns from the data collected.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

4.2 Instrument for Data Collection and Analysis Procedure

The instruments used for data collection were semi-structured interview and documentary sources. These sources (interviews and case files) are forms of qualitative research instrument that are often employed to obtain participants' perceptions, ideas and attitudes towards a particular phenomenon under study (Stuart & Headlam, 2008). Interviews, which could be conducted on a one-on-one basis, are generally used to support and extend an investigator's knowledge on the thoughts and attitudes of the phenomena under study (Woods, 2011).

The process of data analysis involves the collecting, synthesizing, reporting the exact views of the participants on the phenomenon under investigation. In this study, thematic Analysis was used to analyze data, because it enabled the researcher to identify, analyze and interpret patterns from the data collected from the participants.

5. Results and Discussion

In order to ascertain the types of cybercrimes and their corresponding effects on Ahmadu Bello University's Network, the study provides summary of the findings as presented in Table 1.

Table 1: Types of Cybercrimes and their corresponding effects on Ahmadu Bello University's Network

Type	Findings based on participants responses	Effects
Social Engineering Attacks	The common types of social engineering attack affecting Ahmadu Bello University Network are phishing attack, shoulder surfing, and password sniffing. Cybercriminals have at some point used social engineering techniques to enhance Advanced Persistent Threat (APT) attacks in order to cause damage to the university network and steal valuable data or reach a particular target. Most cybercriminals employ social engineering technique at the initial stage of an attack, and they use the information obtained through this means to create an opening for executing more sophisticated forms of cybercrimes. Cybercriminals use social engineering to attack university students, staff and network.	The effect off social engineering on university network is identity theft. Identity theft also known as identity fraud is one of the major effects of cybercrime. It involves the cybercriminals obtaining key pieces of personally identifiable information of their victims, such as Social Security Number (SSN) or credit card number in order to impersonate them.
Denial-of-Service (DoS) Attacks	Cybercriminal adopt DoS attacks mainly so as to make the university network resources unavailable to staff and students.	One of the effect of DoS is through the disruption of Internet access or through the illegal utilization of Internet resources. DoS also affect the entire activities and services on the university network.
Malware	Malware (known as malicious software) is any program or file that is harmful to a computer and/or computer network. Malware includes computer viruses, ransomware, worms, Trojan	Led to the close-down of thee-mail server for many months, with lecturers not able to read their mails. The effect of malware leads to damages to organizational information systems,

Online: ISSN 2645-2960; Print ISSN: 2141-3959

	horses and spyware. These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission.	and loss of trust by Internet users.
Pharming Attacks	A participant opined that pharming is common crime during Admission period at Ahmadu Bello University. Targets are directed to webpages controlled by the cybercriminals and are asked to pay money to be given admission into the University.	The victim's computer displays an error message and recommends that the user shut off their firewall and antivirus software. Without the firewall the victim's computer becomes vulnerable. Intellectual property, alumni databases and even a database of car parking permits containing details of vehicle owners would present great values to cybercriminals, where such information if accessed by criminals can be used to impersonate victims.
Website Defacement Attacks	Website defacement is an attack that changes the visual appearance of the site or a webpage. These are typically the work of cybercriminals, who break into a web server and replace the hosted website with one of their own. A participant explained that the new content on the website attracts the attention of the victims with the intention to motivate and lure victim into supplying the necessary information that could be used against them.	The effect of website defacement is wasted financial sources, time, and effort spent by IT personnel in trying to fix problems rather than focusing on the core competencies of the university. Another effect is reputational damage is in the of where student records are compromised by a security breach, the university's reputation can seriously be damaged. Students whose personal information are intercepted or accessed by cybercriminals may not trust the university's information management structure and system anymore, hence tarnishing the University's public image.

6.2 Phishing attacks: Majority of the participants identified phishing attacks to be one of the most common types of cybercrime affecting the University. According to Kaspersky (2013), phishing is a malicious attack that involves the creation of false website by a cybercriminal before proceeding to using various social engineering techniques to attract targets to the website. Popper (2013) further explained that, it is when a malicious party sends a fraudulent email disguised to look like a legitimate email, often purporting to be from a trusted source. The message in such email is meant to trick the recipient into sharing personal or financial information or clicking on a link that installs malware on the user's device (Rouse, 2010). A phishing attack can be seen as a success once a target clicks on the fake link that redirects the target to the false website (Symantec Corporation, 2014). An investigation by Junxiao and Sara (2012) pin pointed the fact that most educational institutions' information systems and some social media websites are the most targeted by phishing campaigns.

A study by Chen *et al.* (2011) reported that 89% of cybercrime offences in universities are committed through phishing attacks. Similarly, respondents in this study also identified phishing as a prevalent cybercrime affecting Ahmadu Bello University. It was explained by one of the respondents that educational institutions are targeted by cybercriminals because of the valuable information maintained by

Online: ISSN 2645-2960; Print ISSN: 2141-3959

the institutions. This is similar to a study by Pratt et al. (2010) where they reported that phishing attack is on the rise and it is increasingly affecting many organisations and educational institutions alike. Some of the information targeted at educational institutions includes intellectual property and databases that contain the information of employees and students that can be used for identity theft and fraud.

6.3 Shoulder Surfing: Shoulder surfing was identified by participants as a type of social engineering technique that is affecting the university network. Shoulder surfing involves the use of less technology. According to Wiedenbeck et al. (2006) and Gao et al. (2010), shoulder surfing refers to a direct observation, such as looking over a person's shoulder in order to obtain confidential information. Wiedenbeck et al. (2006) further stated that, shoulder surfing is done for no reason other than to get useful information from unsuspecting victims. In their study, Kumar et al. (2007) stated that shoulder surfing can also be described as the practice of spying on the user of a cash-dispensing machine (i.e. ATM) or other electronic device in order to obtain sensitive information such as personal identification number, password. Inexpensive, miniature closed-circuit television cameras can be concealed in ceilings, walls or fixtures to observe data entry. Shoulder surfing is an effective way of getting information in crowded places because it is relatively easy to stand next to someone and watch as they fill out a form online, or enter a PIN number at an ATM machine, or use a calling card at a public pay phone (Kumar et al., 2007).

Participants stated that there had been reports from students that when they were doing their online registration, people stood by their side in what they (i.e. the students) believe were an attempt to observe/spy carefully over their shoulder so as to get valuable information. Tari et al. (2006) in their study stated that, shoulder surfing can be done at a distance using other vision-enhancing devices such as binocular, miniature closed circuit camera. If the cybercriminal carrying out shoulder surfing was successful, sensitive information such as user name and password of students will be obtained, and which can be used by cybercriminals for furtherance of their attack.

6.4 Password Sniffing: Responses from the interviews shows that password sniffing is a form of social engineering. One of the respondents explained that password sniffing is a technique used to gain knowledge of passwords. It involves monitoring traffic on a network to pull out sensitive information such as users' password. A respondent remarked that this crime is usually perpetrated by users with the technical know-how skills of managing network traffic. Lee et al. (2009), similarly, explained that password sniffing is a software application that scans and records passwords that are used or broadcasted on a computer or network interface. A study by Abbas et al. (2006) reported that cybercriminals also use password sniffing software to scan incoming and outgoing network traffic and records any instance of a data packet that contains a password.

6.5 Denial-of-Service (DoS) Attacks

Apart from social engineering attacks, another cybercrime that participants attested to is the denial of service attacks. A respondent stated that "Denial-of-service attack is another cybercrime type that the university's network has been exposed to". Participants stated that cybercriminal adopt DoS attacks mainly so as to make the university network resources unavailable to staff and students. According to Burden and Palmer (2003), denial-of-service attacks are usually designed to disrupt the access and use of Internet resources from legitimate users. Investigations by Pilling (2013) showed that universities globally have lost valuable information to denial of service attacks. This losses occurred either through the disruption of Internet access or through the illegal utilisation of Internet resources.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

Saravanan and Asokan (2011) stated that denial of service attacks occur when a cybercriminal attacks the server of an organisation by loading them with millions of spoof messages. The large amount of spoof messages eventually consumes all the available bandwidth of the organisation. The servers that are loaded with the spoof messages often crashes or freezes at some point, making it difficult for legitimate users to access them (Burden and Palmer, 2003).

Participant indicated that there are cases when the university servers respond very slowly to the request of users. This, they opined is as a result of the demands on the servers. This huge amount of data is mostly sent through amplified attacks, and the limited processing capacity to handle the huge amount of data. For example, instead of sending 4Mix (a Mix is an Internet traffic model that describes user behaviour using a number of systems) of web traffic, an attacker can send 20Mix; the line would be congested and there would be slower response by the server. Attackers often aim at bandwidth, memory or CPU, depending on what they are trying to obtain.

6.6 Malware

Participants identified Malware as another cybercrime that ABU Network is susceptible to. Malware (known as malicious software) is any program or file that is harmful to a computer and/or computer network. Malware includes computer viruses, ransomware, worms, Trojan horses and spyware (Bergman et al., 2013). These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission.

A. Botnet Attack: A form of malware that participants indicated is botnet. According to Bleaken (2010), botnet is a program that facilitates an attack from coordinated systems. The botnet is a group of computers connected in a coordinated fashion for malicious purposes. Each computer in a botnet is called a bot. these bots form a network of compromised computers, which is controlled by a third party and used to transmit malware or spam, or to launch attacks. A participant remarked that in 2016, computers were infected with malicious software sent as e-mail spam to several computers on the university network. This brought down the e-mail server for several months. This eventually led to the close-down of the e-mail server for many months, with lecturers not able to read their mails. Sérgio et al. (2012) also believed that the main purpose of botnets is for cybercriminal to employ enslaved computers for malicious activities in order to steal confidential information, disrupt service and carry out identity theft. The effect of botnet attack is disastrous and often lead to damages to organisational information systems, and loss of trust by Internet users (Gercke, 2012).

B. Means of Malware Distribution

Malware distribution can occur in many different ways. According to OECD (2007), malware distribution refer to the means in which malware is propagated. Examples of means through which malware is propagated include; USB devices, Internet Relay Chat, Bluetooth, e-mail. In line with this, the interviewees in this study pointed out that the most common means of malware distribution on the university network is through plugging in USB devices with malicious content, and Internal Users crime.

6.7 Plugging in USB Devices with Malicious Contents: Most of the participants expressed that USB device is sometimes employed by cybercriminals as a means of installing malware on the university network. These devices could be Flash Drives, Phones, Digital Cameras, and Biometric devices for thumbprints. Plugging in these USB devices with malicious content (like viruses and worms) in order to get access to the university network sometimes requires paying a disloyal employee some amount of

Online: ISSN 2645-2960; Print ISSN: 2141-3959

money or the use of computers on the university network. These computers include computers used in the Computer Based Test (CBT) Centres and the computers in the MTN Net Library.

6.8 Distribution by Download: Participants explained that malware can also be distributed by download of free software (from uncertified websites and websites that are censored/blocked by the administrators of the network), by users of the university network. Manuel et al. (2009) stated that attacks in the form of distribution-by-downloads is any download of software programs that occurs without a user's authorisation or knowledge. In a typical distribution-by-download attack, merely visiting a web site that embodies the malicious content can result in the infection of users' machine or device with malware which, as an after effect, often enslaves the user's machine to become a member of a botnet (Manuel et al., 2009, Marco et al., 2010). The malicious code or program that is installed for the execution of the attack then has typically full control over the user's computer system (Marco et al., 2010). Another participant from the software development unit (SDU) stated that attack in the form of distribution-by-download is any download of files, images, and documents that occurs without a user's authorization. For example, pornographic videos, images and documents are blocked from users by the network administrators.

6.9 Internal Users: Participants explained that internal users within the university network aid the distribution of various kinds of malwares in organisations via the use of malicious software. Respondents stated that most internal fraudsters are often very knowledgeable about the systems they want to exploit. As supported by Hemavathy *et al*.(2005), internal perpetrators are dangerous to an organisation because most of them possess exclusive and administrative rights to organisational resources. This enables them to avoid being detected by the various security mechanisms available on the network. One of the cyber security analysts stated that: "Attacks aided by cyber channels against enterprises could either be internal or sneaker based. In the case of internal attackers, the attackers have the necessary authorisation to Information Systems, know how the system works and therefore find it easy to use the system to their advantage. However, some respondents stated that internal fraudsters are in some cases not careful or experienced enough to completely remain anonymous during the period of their activities, and usually end up being caught.

6.10 Pharming Attacks

Responses from the participants identified pharming as a type of cybercrime affecting the University. A participant opined that pharming is common crime during Admission period at Ahmadu Bello University. Targets are directed to web pages controlled by the cybercriminals and are asked to pay money to be given admission into the University. According to Gercke (2012), pharming is a cyber attack intended to redirect a website's traffic to a fake website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into real IP addresses (GFI, 2009). According to Robert (2015), pharming requires unprotected access to target a computer, such as altering a customer's computer IP address. Once a victim is lured to the website, an unpatched computer would download a Trojan horse in a file called "iexplorer.exe" from the cybercriminal server. The victim's computer displays an error message and recommends that the user shut off their firewall and antivirus software. Without the firewall the victim's computer becomes vulnerable. When the user visits any of the targeted banking sites, they will be redirected to a mock-up of the bank's Web site. This site then collects the victim's login credentials and transfers them to the criminals. The victim is then passed back to the legitimate site where they were already logged in, making the attack invisible.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

6.11.Website Defacement Attacks

Participants stated that website defacement is another form of attacks that affect the university network. Website defacement is an attack that changes the visual appearance of the site or a webpage. These are typically the work of cybercriminals, who break into a web server and replace the hosted website with one of their own (Alhamed and Alsuhaibany, 2013). A participant explained that the new content on the website attracts the attention of the victims with the intention to motivate and lure victim into supplying the necessary information that could be used against them. According to Hinckley et al. (2012), this attack could be in a form of denial of service attacks, port scan attack, or through SQL injection and cross site scripting attacks.

6.12. Port Scan Attacks

Walter *et al.*(2011) stated that port scan is viewed as an attack technique that dispatches legitimate user requests to a range of server address ports on a network host, with the aim of discovering an open or active port (e.g. File Transfer Service (FTP)). Once an open port or service is discovered by an attacker, the computer with the open port can be easily compromised, infected with a virus or lose valuable data (Walter et al., 2011). The responses of the participants indicated that malicious programs capable of port scanning were seen to be frequently used by attackers to exploit vulnerabilities in the university network. One of the participants stated that: “the university network has seen lots of port scans on the server infrastructure side. The university network has also seen lots of "SYN" programs running on their web service that are constantly looking for vulnerabilities to exploit.” According to Bogdanoski et al. (2013), A SYN program is a form of denial of service attack in which an attacker sends a succession of SYN requests to a target’s system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. Participants felt that the risk of port scan attacks is often common with the web servers of the university network involved in creating port connections. One of the participants stated that: “After building a secure architecture and acquiring the necessary monitoring software, it would be very easy to know when a web server is port scanning a virtual box”. Since a virtual box only makes SQL connections on a particular port, an attempt by a cybercriminal to use web server to make connections on different ports or search for different host should immediately raise a red flag as a result of the network security protocols monitoring software.

6.13. SQL Injection and Cross Site Scripting Attacks

SQL injection is a type of exploit whereby the cybercriminal injects Structure Query Language (SQL) code through a web application in order to gain access to recourses, or make changes to data (Awodele et al., 2012). Here, the attacker injects SQL commands to exploit non validated input vulnerabilities in a web application database backend and consequently execute arbitrary SQL commands through the web application. Because programmers use sequential commands with user input, it makes it easier for cybercriminals to inject commands (Kar and Panigrahi, 2013). From the responses of the participants, it was reported that, SQL injection and Cross Site scripting attacks are also techniques used by cybercriminals in order to obtain valuable information from the university network. One of the participants asserted that, the university network experienced SQL injection in 2015 were some students changed the content of the website in which about 52 students were lured into paying their school fees into different account. Symantec (2012) believed that cross-site scripting and Structured Query Language (SQL) injection techniques are the most widely used attack methods by cybercriminals. Adam *et al.* (2009) believed that SQL Injection and cross-site scripting attacks (XSS) are common types of attacks that can be employed by an attacker to craft input to a target application in order to gain access or alter

Online: ISSN 2645-2960; Print ISSN: 2141-3959

user data, and execute malicious code. Etienne (2008) stated that organisations should always validate user supplied data, enforce data types for all inputs, employ the least privilege rule, filter input data via white-list and black-list filtering, snort-based solutions, and host based IDSs. This is in order to censor the types of content that are allowed for downloading by the different categories of users of the network.

With respect to Cross site scripting attacks, Philipp et al. (2007) stated that cross-site scripting can be prevented in an organisation by properly validating input from users, employing static analysis on the server side of an organisation, and deploying anomaly based intrusion detection systems in organisations. In a typical drive-by-download attack, merely visiting a web site that embodies the malicious content can result in the infection of a user's machine or device with malware which, as an after effect, often enslaves the user's machine to become a member of a botnet (Manuel *et al.*, 2009, Marco *et al.*, 2010). The malicious code or program that is installed for the execution of the attack then has typically full control over the user's computer system (Marco *et al.*, 2010). Ahmadu Bello University Network remains vulnerable to cyber piracy attacks except if there are adequate security measures in place to prevent the depletion of resources on Information Systems by cybercriminals. The presence of suitable target as a construct of the routine activity theory stipulates that networks without adequate and capable security protocols in place would often be vulnerable to cybercrimes (Felson and Cohen, 1979). The responses of the various respondents, in line with the theme on the types of cybercrimes prevalent on the university network, provide answers to the research question that seeks to determine the types of cybercrimes that Ahmadu Bello University Network could be susceptible to.

7. Conclusion

Findings from the study revealed that the University is continuously susceptible to different types of cybercrime. Among the cybercrimes are: social engineering, denial of service attacks, malware attacks, pharming attacks, SQL injection and cross-site scripting attacks, website defacement, and port scan attacks. In the 21st century, cybercrime attacks in universities have become rampant globally. Historically, university's infrastructure has been based on an open access with very little restrictions on access to information. These infrastructures stimulate learning and its environment. It, however, increases cyber threat. Once breached, universities can be left with high financial losses and loss of valuable information such as students and staff members' personal information. Cybercriminals frequently device dynamic and sophisticated means in which they perpetrate their illicit activities. In equal measure, universities should also be making effort to deploy and explore more divergent means of curtailing the menace of the cybercriminals. Hence, proper use of cybercrime control measures, as suggested in this study, could help in safeguarding and protecting students and staff members' information, and the university's information systems, at large, from cybercrimes and cybercriminals.

8. Recommendation

Based on the findings of this study, it is recommended that a behavioural approach to cybercrime be implemented across the university. This can be achieved by motivation of staff of the ICICT directorate. Salary increases, cash incentives for hardworking staff and training of staff on a regular basis. These could be a step in the right direction for effective management of the University Network.

There is also the need for the University to be more security conscious of students who participate in projects such as website development. This is because of a recent event in which some students were caught trying to allocate rooms to their colleagues and also lure victims in paying school fees into

Online: ISSN 2645-2960; Print ISSN: 2141-3959

different account that is similar to that of the University. Also the University should put in place adequate data protection measures that can help with the handling of employee data.

Finally, the University should be very proactive to the issues of cybercrimes. The University should organize regular seminars and workshops aimed at enhancing collaborative efforts between Government and the University on issues related to cyber security, also engage staff for international training as a form of motivation. Furthermore, the University should collaborate on a regular basis or be involved in software development projects that would provide better means of combating cybercrimes within the University. It is also recommended that the university should enhance and improve the level of cooperation and trust that exists with other agencies such as National Security Agency (NSA), Central Intelligence Agency (CIA), Inter-Service Intelligence (II), and European Union Agency for Network and Security (EUANS) in order to combat cybercrimes.

References

Abbas, A., El-Saddik, A. & Miri, A. (2006). A comprehensive approach to desingning Internet security taxonomy.

Adam, K., Philip, J. G., Karthick, J. & Michael, D. E. (2009) Automatic creation of SQL Injection and cross-site scripting attacks. ICSE '09 Proceedings of the 31st International Conference on Software Engineering 2009 Vancouver, BC IEEE Computer Society Washington, DC, USA, 199-209.

Alhamed, M. & Alsuhaibany, O. M. (2013). Website defacement incident handling system, method, and computer program storage device. Google Patents.

Amit, R. & Schoemaker, P. J. (2012). Strategic Assets and Organizational Rent. *Strategische Managementtheorie,* 14**,** 325.

AndersoN, J. R. 2008. *Security engineering: a guide to building dependable distributed systems*.

Ani, L. (2011). Cyber Crime And National Security: The Role of the Penal And Procedural Law. *Law and Security in Nigeria***,** 200-202.

Appel, E. J.(2014). *Cybervetting: Internet Searches for Vetting, Investigations, and Open-Source Intelligence*, Crc Press.

Awodele, O., Onuiri, E. E. & Okolie, S. O. (2012). Vulnerabilities in Network Infrastructures and Prevention/Containment Measures. Proceedings of Informing Science & IT Education Conference (InSITE).

Barton (2011). Physical security management protocol

Bergman, N., Stanfield, M., Rouse, J., Scambray, J., Geethakumar, S., Deshmukh, S., MATSUMOTO, S., STEVEN, J. & PRICE, M. (2013). *Hacking exposed: Mobile security secrets & solutions*, McGraw-Hill.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

Bleaken, D. (2010). Botwars: the fight against criminal cyber networks. *Computer Fraud & Security,* 2010**,** 17-19.

Bogdanoski, M., Shuminoski, T. & Risteski, A. (2013). Analysis of the SYN flood DoS attack. *International Journal of Computer Network and Information Security,* 5**,** 1.

Borgatti, S. P. 1999. Element of Research: Theoretical Framework.

Burden, K. & Palmer, C. (2003). Internet crime: Cyber Crime — A new breed of criminal? *Computer Law & Security Review,* 19**,** 222-227.

Castell, M. (2013). Mitigating online account takeovers: The case for education. Federal Reserve Bank of Atlanta, Retail Payments Risk Forum, survey paper, April, available at www. frbatlanta. org/documents/rprf/rprf_pubs/130408_survey_paper. pdf,.

Chen, Bose, I., Leung, A. C. M. & Guo, C. (2011). Assessing the severity of phishing attacks: A hybrid data mining approach. *Decision Support Systems,* 50**,** 662-672.

Dimaggio, P., Hargittai, E., Neuman, W. R. & Robinson, J. P. (2001). Social implications of the Internet. *Annual review of sociology***,** 307-336.

Etienne, Z. P. (2008). Preventing SQL Injections in Online Applications: Study, Recommendations and Java Solution Prototype Based on the SQL DOM. *Application security conference.* Ghent, Belgium: OWASP.

Felson, M. & Cohen, L. E. (1979). Human ecology and crime: A routine activity approach. *Human Ecology,* 8**,** 389-406.

Gao, H., Ren, Z., Chang, X., Liu, X. & Aickelin, U. (2010). A new graphical password scheme resistant to shoulder-surfing. Cyberworlds (CW), 2010

Gardere, W. S. (2014). Cybercrime is getting worse - 5 reasons.

Gercke, M. (2012). *Understanding cybercrime: Phenomena , challenges and legal response,* Geneva, Switzerland, TU Telecommunication Development Bureau.

Gfi (2009). Attachment spam – the latest trend. USA.

Goldsmith, J. L. & Wu, T. (2006). *Who controls the Internet?: illusions of a borderless world*, Oxford University Press New York.

Grimes, R. A. (2015). Reasons for Internt crime.

Groff, E. R. (2008). Adding the temporal and spatial aspects of routine activities: A further test of routine activity theory. *Security Journal,* 21**,** 95-116.

Grover, V. & SAEED, K. A. (2004). Strategic orientation and performance of internet-based businesses. *Information Systems Journal,* 14**,** 23-42.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

Halder, D. & JAISHANKAR, K. (2011). *Cyber crime and the victimization of women: laws, rights and regulations*, Information Science Reference.

Hassan, A. B., FUNMI, D. & MAKINDE, J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology*, 2.

Hemavathy, A., PRAVIN, M., AVICHAL, S. & FLEIZACH, C. (2005). Cybercriminal Activity. Available: http://sysnet.ucsd.edu/~cfleizac/WhiteTeam-CyberCrime.pdf [Accessed 15 May 2014].

Hinckley, K., BI, X., PAHUD, M. & BUXTON, B. (2012). Informal information gathering techniques for active reading. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 1893-1896.

Ionescu, L. (2012). Corruption, Unemployment, and the Global Financial Crisis. *Economics, Management, and Financial Markets***,** 127-132.

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E. & PU, C. (2011). Reverse social engineering attacks in online social networks. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 55-74.

Jaishankar (2011). Expanding cyber criminology with an avant-garde anthology. *Cyber Criminology*.

Jegede, A. E. (2010). Globalization, Media Culture and Socio-Economic Security in Nigeria. *Mass Communication A Book of Readings***,** 228-247.

junxiao, S. & SARA, S. (2012). Phishing. *CSc 566, Computer Security Research Reports.* USA: University of Arizona.

Kahoka (2015). Vulnerabilities and Causes of Cybercrime.

Kar, D. & Panigrahi, S. (2013). Prevention of SQL Injection attack using query transformation and hashing. Advance Computing Conference (IACC), IEEE 3rd International, 2013. IEEE, 1317-1323.

Kaspersky, L. (2013). The evolution of phishing attacks: 2011-2013. Kaspersky Lab ZAO, Moscow, Russia.

Kumar, M., Garfinkel, T., Boneh, D. & Winograd, T. (2007). Reducing shoulder-surfing by using gaze-based password entry. Proceedings of the 3rd symposium on Usable privacy and security. ACM, 13-19.

Lee, K., Bae, K. & Yim, K. (2009). Hardware approach to solving password exposure problem through keyboards sniff.

Levy, P. S. & Lemeshow, S. (2013). *Sampling of populations: methods and applications*, John Wiley & Sons.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S. & Ignatuschtschenko, E. (2013). Comprehensive study on cybercrime. *United Nations Office on Drugs and Crime***,** 38-39.

ManueL, E., Peter, W., Christopher, K. & Engin, K. Defending Browsers against Drive-by Downloads: Mitigating Heap-spraying Code Injection Attacks. DIMVA '09 Proceedings of the 6th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment Springer-Verlag Berlin, Heidelberg. 88-106.

Marco, C., Christopher, K. & Giovanni, V. (2010). Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code. *International World Wide Web Conference.* Raleigh, North Carolina, USA.

Meke, E. S. (2012). Urbanisation and Cybercrime in Nigeria: Causes and Consequences.

Millet, A. (2015). *Airlines vulnerabilities to a cyber-attack and the potential consequences.* Utica College.

Murray, J. H. (2017). *Hamlet on the holodeck: The future of narrative in cyberspace*, Mit Press.

Mustaine, E. E. & Tewksbury, R. (1999). A routine activity theory explanation for women's stalking victimizations. *Violence Against Women,* 5**,** 43-62.

Nadiah, S. (2014). Causes and Effects of Cyber Crime.

Navarro, J. N. & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum,* 32**,** 81-94.

Nir Kshetri (2019). Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management,22: 77-81, DOI: 10.1080/1097198X.2019.1603527

OECD (2007). Malicious Software (Malware): A Security threat to the Internet Economy. Seoul, Korea: Organisation For Economic Cooperation and Development; Directorate for Science, Technology and Industry Committe for Information, Computer and Communications Policy.

Omodunbi, B. A. Odiase, P. O. Olaniyan, O. M and Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention *FUOYE Journal of Engineering and Technology, Volume 1, Issue 1*

Phair, N. & Hodges, M. (2007). *Cybercrime: the reality of the threat*, Nigel Phair.

Philipp, V., Florian, N., Nenad, J., Engin, K., Christopher, K. & Giovanni, V. (2007). Cross Site Scripting Prevention with Dynamic Data Tainting and Static Analysis. Proceeding of the Network and Distributed System Security Symposium Secure Systems Lab Technical University Vienna; Giovanni Vigna.

Pilling, R. (2013). Feature: Global threats, cyber-security nightmares and how to protect against them. *Computer Fraud & Security,* 2013**,** 14-18.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

Plan, O. Y. A., Plan-main, O. Y. A. & Stones, S. (2017). Review of the Roots of Youth Violence: Literature Reviews Volume 5.

Poonia, A. S., Bhardwaj, A. & Dangayach, G. (2013). Cyber Crime: Practices and Policies for Its Prevention.

Popper, K. 2013. *The poverty of historicism*, Routledge.

Pratt, T. C., Holtfreter, K. & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency,* 47**,** 267-296.

Ribadu, E. (2007). Cyber Crime and Commercial Fraud; A Nigerian Perspective. A paper presented at the Modern Law for Global Commerce, Vienna 9th – 12th July.

Robert, P. (2015). DNS Pharming attacks target .com.

Rouse, M. (2010). Search security. *TechTarget,[Online]. Available: http://searchsecurity. techtarget. com/definition/authentication.[Accessed 9 July 2016]*.

Saravanan, K. & Asokan, R. (2011). Distributed Denial Of Service (Ddos) Attacks Detection Mechanism. *International Journal of Computer Science, Engineering and Information Technology,* 1**,** 11.

Selwyn, N. (2008). A safe haven for misbehaving? An investigation of online misbehavior among university students. *Social Science Computer Review,* 26**,** 446-465.

Sérgio, S. C. S., Rodrigo, M. P. S., Raquel, C. G. P. & RONALDO, M. S. (2012). Botnets: A survey. *Computer Networks,* 57**,** 378-403.

Shimomura, T. & Markoff, J. (1995). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaws-by the Man Who Did It*, Hyperion Press.

Shinder, D. L. & CROSS, M. (2008). *Scene of the Cybercrime*, Syngress.

Strawbridge, G. (2019). *How Universities can protect themselves from Cyber Attacks*. [online] Available at: https://www.metacompliance.com/blog/how-universities-can-protect-themselves-from-cyber-attacks/ [Accessed 2 Aug. 2019].

Swan, M. (2015). *Blockchain: Blueprint for a new economy*, " O'Reilly Media, Inc.".

Symantec (2012). The Ongoing Malware Threat: How Malware Infects Websites and Harms Businesses — and What You Can Do to Stop It. *The Ongoing Malware Threat.* USA.

Symantec Corporation (2014). Internet Security Threat Report *2013 Trends.* Mountain View, Carlifornia, USA.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

Tari, F., Ozok, A. & Holden, S. H. (2006). A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. Proceedings of the second symposium on Usable privacy and security, ACM, 56-66.

United Nations Office Of Drugs And Crime, V. (2013). Comprehensive study on Cybercrime.

Walter, F., Patricio, Z., Marco, S. & Pablo, G. (2011). Alternative Engine to Detect and Block Port Scan Attacks using Virtual Network Environments. *International Journal of Computer Science and Network Security(IJCSNS),* 11**,** 14-23.

Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *The International Journal of Cyber Criminology,* 5**,** 736-749.

Wiedenbeck, S., Waters, J., Sobrado, L. & Birget, (2006). J.-C. Design and evaluation of a shoulder-surfing resistant graphical password scheme. Proceedings of the working conference on Advanced visual interfaces. ACM, 177-184.

Zittrain, J. L. (2006). The generative internet. *Harvard Law Review***,** 1974-2040.