An Assessment of Cybersecurity Technologies in the Selected Universities in Southwestern Nigeria

Gbonjubola Oluwafunmilayo Binuyo
African Institute for Science Policy and Innovation
Obafemi Awolowo University, Ile Ife, Nigeria

ABSTRACT

The study identified the forms of cybercrimes in selected universities in Southwestern Nigeria. It determined the cyber security techniques and polices adopted by the selected Universities. It examined the effectiveness of cyber securities adopted by the selected Universities. Hence, primary data were obtained through the administration of questionnaire on 33 ICT administrators from each of the selected nine (9) universities in Southwestern Nigeria, making 297 respondents. Secondary data were sourced from publications. Data collected were analysed using descriptive and inferential statistics. The result showed that common types of cybercrimes in the selected institutions were hacking 66.3%), credit card fraud (58.5%), spamming (52.2%), software piracy (60.7%), identity theft (55.2%), sweet heart swindle (53.3%) and malicious programme/virus (54.4%). The results also showed that most cybercriminals used password cracker (83%), network sniffer (50.4%) and key logger (44.4%) to perpetrate their illicit acts. Also, the results indicated the adopted cyber securities mechanism in the selected universities which include identity (ID) and Password (100%), Public Key Cryptography (33.3%), Biometric Authentication (29.6%) and Digital Signature (18.5%). There was a significant ($F=7.043$; $p<0.05$) relationship between frequency of cyber-attack on Servers/Web Services and the deployment of Multi-Layer Authentication, Digital Signature ($F=16.611$, $p<0.05$) and Public Key Cryptography ($F=6.750$, $p<0.05$). The study concluded that major technologies used for cybercrimes in the universities in Southwestern Nigeria were password cracker, key logger and network sniffer. The study also concluded that the common types of cybercrime in the universities were hacking, credit card fraud, spamming, software piracy, identity theft, pornography, sweet heat swindle and malicious programmes (virus). The study further concluded that authentication protocols deployed majorly by universities in Southwestern Nigeria were Kerberos, internet protocol (IP) securities, CHAP and MS-CHAP. The study concluded that all the universities deployed identity (ID) and password authentication for security access control while privacy policy, network security policy and employee training regarding confidential information were the cyber security policy adopted by most of the universities in Southwestern Nigeria. The study concluded that the deployment of Cyber securities such as public key cryptography and digital signature inhibits threats on servers and services of the universities. This study concluded that universities in Southwestern Nigeria that did not deploy multi-layer authentication, digital signature and public key cryptography on their internet servers are susceptible to cybercrime frequently.

Keywords

Cybercrimes, Cybersecurity, Universities, Nigeria

1. INTRODUCTION

Nigeria is a developing nation and not the only economy where cybercrimes are being committed. The rate of cybercrime is on the increase in the economy due to lack of security awareness and under reportage. Though, the knowledge of some internet users is noticeably just for conversation with their colleagues and majority might not be in the position of protecting their information on their gadgets from virus [1]. The level of cybercrime in Nigeria institutions is growing in line with the rate of growth in digital information. The extent of organizations' experiencing security breaches are increasing in nature [2].

Cybercrime is a criminal offence committed using the Internet as a component of the crime [3]. In addition to that, cybercrimes are offences that are committed against individuals or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks [1]. There is need for effective and efficient cybersecurity in order to avert the impending cybercrime problem in Nigeria.

Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets [4]. Cyber security represents a complex and evolving challenge for government, industry and higher education. The main challenge for all is how to develop appropriate security measures and practices that reflect their organizational models and priorities [5] against cybercrime.

Securing of network environments is one of the tasks that will probably never end because Information Technology field is such a dynamic one where new invention will never present ideal secure situation for either systems or network. It is not that the highest security cannot be achieved, but in many cases, as security tightens up, freedom is sacrificed; especially if data containing sensitive information is to be protected. Without hacking tools, it is impossible for Certified Security Professionals within the confines of the ethics of their professions, legally to discover intrusion possibility. However, using these same tools, (many of which are freely available on the Internet) crackers gain unauthorized access into network environment when they take advantage of any vulnerability [5]. Universities and allied institutions need to be protected from cybercrimes.

Universities and allied educational institutions face a variety of cyber security threats. These include disruption to the functioning of university's network and targeted attempts to obtain valuable information from networks and their users. Data produced by the universities are often core intellectual assets which must be secured to achieve set academic and/or commercial targets. However, most Cyber Security Techniques adopted to secure most Nigerian Universities' networks and data are prone to hacking. There are divers' studies on cybercrime and cyber securities in developing and developed economies [3], [1], [5], [6], [7]. Little is known in the literature about the common cybercrimes, cyber securities mechanism and policies adopted by the universities in Southwestern Nigeria. Therefore, there is need to assess the forms of cybercrimes, cyber security techniques and policies adopted in the selected universities in Southwestern Nigeria, hence this study.

The remaining part of this study is ordered are follows; literature review, methodology, results and discussion, conclusion and recommendations.

2. LITERATURE REVIEW

Internet is the most technologically advanced medium of interaction that turned the world into a global village [8]. Internet open broad opportunities to obtain and exchange information [9] and knowledge sharing. Internet is the inter connection of computers across the world thereby creating unlimited opportunities for mankind [10]. In addition, internet has accelerated windows of opportunities for businesses and the removal of economic barriers hitherto faced by nations of the world among is airline business. The effective deployment of ICT in CRM (customer relation management) assisted the Airlines in rendering better services to their passengers and facilitated a robust performance of their operations [11]. Also, internet has helped Nigerian Institutions in knowledge production, sharing and online programmes.

Nigerian institution has a cyberspace that keeps expanding because data produced get accumulated over time. For example, a student's academic record is useful for tracking his/her performance academically and is used to determine the class of degree that the student eventually graduates with. Nevertheless, this same record is useful in preparing the student's transcript as requirement for advanced studies in the future. Every year, the University admits students; digital data keeps expanding and infrastructures meant to hold such information rights. Also, significantly, universities maintain websites and repositories that hold information about academic publications of scholars such as books, journals and magazines, institutional events and news, electronic resources online, student portal site, links to subscribed databases, etc. In addition, apart from the several content management systems of a university's enterprise, most sensitive digital data or information held by universities, especially researches with potential economic value are of different types. This poses a serious challenge of arriving at the exact judgment of the legal status and financial risks directly or indirectly posed by this information with respect to a particular university's Cyberspace rights [6]. How broad and efficient is the Nigeria Cyber Security Policies and Strategy?

The government of Nigeria in 2001 commissioned a body of experts to design a National Policy on Information Technology. It is however to be noted that the resultant policy does not offer much for the understanding, prevention and eradication of criminal activities in cyberspace [6]. In effect, the policy has not shown a sufficient commitment on the part of government to deal with the problem of cyber-criminality in the country. In particular, the task of the 'IT Task Force' that was recommended in the Policy is not specified, while no financial allocation was provided for the Task Force in the spending profile of the policy for combating crimes on the Internet [12].

The analysis of the Nigerian National Cyber Security Policy and Strategy shows that the documents are reasonably comprehensive in terms of content and the required contents expected to be typically contained in such documents are largely present. However, certain aspects which appear to be critical to the Nigerian scenario such as an explanation of the current national cyber security state, partnership with internet service providers, establishment of digital identity frameworks, and the development of a military cyber defense capability were seen to either be utterly absent or only barely implied [7]. Observed from the findings of this research, are certain areas of concern regarding the Nigerian National Cyber Security Policy and Strategy, for which the following recommendations are put forward for consideration in future reviews by [7]; first, the provision of comprehensive details of the current state of Nigerian cyber security should be contained in the policy and strategy, to provide immediate information to national industry stakeholders. Second, the national policy and strategy should be better localized, to adequately address national issues regarding cyber security. Three, attention should be paid to the development of a digital identity framework, as the policy and strategy documents are aimed at reducing threats and increasing security, which can be flawed without a proper form of citizen identification in cyberspace. Four, partnerships between the government and Internet Service Providers should be encouraged to better enhance national cyber security monitoring. Five, the development of a cyber defense military capability with the ability to provide cyber counterterrorism in the event of a cyber war should seriously be looked into and included in the documents. The afore mentioned recommendations were based on the historical nature of cybercrime in Nigeria cyberspace.

The historical nature of cybercrime in cyberspace has been studied by notable scholars. Their reports show that cybercrime has become one of the major security issues for law enforcement agencies and the world in general. [13] argued that cybercrimes differ from most terrestrial crimes in four ways which are: they are easy to learn; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present and they are often not clearly illegal. [14] stated that the prominent forms of cybercrime in Nigeria are cloning of websites, false representations, Internet purchase and other e – commerce kinds of fraud. [15] on the other hand stated that the most prevalent forms of cybercrime are website cloning, financial fraud, identity theft, credit card theft, cyber theft, cyber harassment, fraudulent electronic mails, cyber laundering and virus. There are some reasons for the high increase in cybercrime in the cyberspace.

The cause of increase in cybercrime in Nigeria cyberspace may be attributed to urbanization, unemployment, quest for wealth, weak implementation of cybercrime law, inadequate equipped law agencies and negative role models [16]. First, urbanization which is the massive movement of people from rural settlement to cities. Second, unemployment which can be defined as the number of people who are willing to work but unable to secure job. Third, quest for wealth from impropriate means due to pear group. Fourth, weak implementation of cybercrime laws and inadequate equipped law agencies and technologies. Fifth, negative role models in society. There are some categories of cybercrimes.

The categories of cybercrimes are hacking, cyber-theft, virus and worms, spamming, financial fraud, Identity Theft, Credit Card Theft, Fraudulent Electronic Mails (Phishing), cyber harassment, cyber laundering and website cloning [17]. First, hacking is defined as the use of weaknesses and loop holes in operating systems to destroy data and steal important information from a victim's computer. It is normally done through the use of a backdoor program installed on the computer. A lot of hackers also try to gain access to resources through the use of password hacking software [17]. Second, cyber-theft which is defined as the use of computers and communication systems to steal information in electronic format. Hackers crack into the systems of banks and transfer money into their own bank accounts [17]. Third, viruses and worms are computer programs that are designed to damage computers. It is named virus because, it spreads from one computer to another like a biological virus. A worm usually exploits loop holes in software or the operating system. It appears to do one thing but does something else. The system may accept it as one thing. Upon execution, it may release a virus, worm or logic bomb. A logic bomb is an attack triggered by an event, like computer clock reaching a certain date [17]. Fourth, spamming is the sending of an unsolicited email. Email spam is becoming a serious issue amongst businesses, due to the cost overhead it causes not only in regards to bandwidth consumption but also to the amount of time spent downloading/eliminating spam mail [18]. Fifth, financial frauds are commonly called "Phishing' scams, and involve a level of social engineering as they require the perpetrators to pose as a trustworthy representative of an organization, commonly the victim's bank [17]. Sixth, identity theft, credit card theft, fraudulent electronic mails (phishing). Phishing is an act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in order to scam the user into surrendering private information that will be used for identity theft [17]. Seventh, cyber harassment is electronically and intentionally carrying out threatening acts against individuals. Such acts include cyber-stalking [17]. Eight, cyber laundering is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination [17]. Nine, website cloning is the emergence of fake 'copy-cat' web sites that take advantage of consumers what are unfamiliar with the internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, is instead unwittingly entering details into a fraudster's personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud [17]. Haven identified the categories of cybercrime, there is need to explicitly explain cyber security mechanism.

The cyber security mechanisms put in place to control and manage the negative implication of cybercrime in cyberspace includes among others; physical security, authentication, authorization, accounting (auditing), encryption, firewall and cyber security vulnerability [19], [20], [21]. First, physical security which refers to limiting access to key network resources by keeping the resources behind a locked door and protected from natural and human-made disasters. Physical security can protect a network from inadvertent misuses of network equipment by untrained employees and contractors. It can also protect the network from hackers, competitors, and terrorists walking in off the street and changing equipment configurations.

Second, authentication identifies who is requesting network services. Authentication usually refers to authenticating users but can also refer to authenticating devices or software processes. Most security policies state that to access a network and its services, a user must enter a login ID and password that are authenticated by a security server. To maximize security, one-time (dynamic) passwords can be used. With one-time password systems, a user's password always changes. This is often accomplished with a security card, also called a Smartcard. Also, public key cryptography which is based on very complex mathematical problems that require very specialized knowledge for authenticating the legitimacy of the user(s). Not only that, digital signature and multi-layer multifactor authentication (MFA) is a security system in which more than one form of authentication is implemented to verify the legitimacy of a transaction. The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a computer system or network. In addition, authentication protocols are capable of simply authenticating the connecting party as well as authenticating itself to the connecting party. This overview described [20] several authentication protocols used when designing a security system such as Secure Sockets Layer (SSL), Internet Protocol Security (IP SEC), Secure Shell, Kerberos.

Third, authentication controls who can access network resources and limit what they can do after they have accessed the resources [19]. Authorization grants privileges to processes and users. Authorization allows a security administrator control parts of a network (for example, directories and files on servers). Fourth, Accounting (Auditing) effectively analyze the security of a network and respond to security incidents, procedures to be established for collecting network activity data. The collected data would include user- and hostnames for login and logout attempts, and previous and new access rights for a change of access rights. Each entry in the audit log should be time stamped [19].

Fifth, Encryption is a process that scrambles data and protect it from being read by anyone but the intended receiver. An encryption device encrypts data before placing it on a network. A decryption device decrypts the data before passing it to an application. A router, server, end system, or dedicated device can act as an encryption or decryption device. Data that is encrypted is called ciphered data (or simply encrypted data). Data that is not encrypted is called plain text or clear text [19]. Sixth, Firewall is a device that enforces security policies at the boundary between two or more networks [17]. A firewall can be a router with Access Control Lists, a dedicated hardware appliance, or software running on a PC or UNIX system. Firewalls are especially important at the boundary between the enterprise network and the Internet. Seventh, Cyber Security Vulnerabilities are weaknesses in a system or its design that allow an intruder to execute commands, access unauthorized data, and/or conduct denial-of service attacks [22], [23]. Vulnerabilities can be found in variety of areas in the Information Technology (IT) systems. In particular, they can be weaknesses in system hardware or software, weaknesses in policies and procedures used in the systems and weaknesses of the system users themselves [24].

Eight, Vulnerability Scanner does scan the vulnerability present in the software because a large number of applications are becoming online, but how secure are these products is a matter of concern as it is related to the user's security who will be ultimately using the application [25]. Thus, it becomes necessary to find out vulnerabilities present in the software application that may cause a severe risk to the user's security.

Nine, Computer forensics uses computer investigation and analysis techniques to collect evidence regarding what happened on a computer that is admissible in a court of law [26]. Computer forensics requires a well-balanced combination of technical skills, legal acumen, and ethical conduct. Computer forensics specialists use powerful software tools to uncover data to be sorted through, and then must figure out the important facts and how to properly present them in a court of law. Computer forensics is defined as "the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law" [26]. The goal of computer forensics is to carry out a structured investigation while documenting a chain of evidence to discover exactly what happened on a computer and who was responsible for it. The main priority of computer forensics is accuracy. Forensic practitioners must follow strict guidelines and maintain the highest standards of work ethic to achieve accuracy because emphasis must be on evidential integrity and security.

Ten**,** Penetration testing is a series of activities undertaken to identify and exploit security vulnerabilities. It helps confirm the effectiveness or ineffectiveness of the security measures that have been implemented [27]. Penetration testing is a comprehensive method to test the complete, integrated, operational, and trusted computing base that consists of hardware, software and people [28]. The process involves an active analysis of the system for any potential vulnerability, including poor or improper system configuration, hardware and software flaws, and operational weaknesses in the process or technical countermeasures.

Based on the prevalence of cybercrime in cyber space, the mechanisms adopted in curtailing the menace and institutional policies in Nigeria is highly encouraged to be studied.

3. METHODOLOGY

This study was carried out in three purposively selected states in Southwestern Nigeria namely Oyo, Osun and Ondo states. The study was limited to nine universities in Nigeria such as Obafemi Awolowo University, Ile-Ife; Osun State University, Osogbo; Redeemers University, Ede; University of Ibadan; Lead City University, Ibadan; Ladoke Akintola University of Technology, Osogbo; Federal University of Technology Akure; Adekunle Ajasin University Akungba; and Elizade University Ilara-Mokin among others in Southwestern Nigeria. The choice is informed by integrating the perspectives of cyber securities technology of federal, state- and privately-owned universities in the Southwestern Nigeria. Primary data were obtained through the administration of questionnaire. Thirty-three (33) questionnaire were administered to each of the ICT administrators of the selected nine universities in Osun, Oyo and Ondo states making a total of 297 respondents. The questionnaire elicited information on the techniques used for cybercrimes and the type of cybercrimes that is common to the selected institutions. It also elicited information on cyber security techniques adopted by the institutions and the effectiveness of cyber securities technologies Mechanism deployed by the selected institutions. Secondary data were sourced from publications. Data collected were analysed using appropriate descriptive and inferential statistics.

4. RESULTS AND DISCUSSION

Table 1 shows the type of technologies used for cybercrimes in the selected nine universities in Southwestern Nigeria. The respondents reports that cybercrimes committed in the institution are done with the aid of the use of Password Cracker (83%), Key Logger (44.4%), Network Sniffer (50.4%), Exploit (49.6%), Port Scanner (31.5%), Vulnerability Scanner (26.7%), Metaspoilt (15.9%), Backtrack (24.8%), Aircrack-ng (17%), Ksmet (13%), Wireshark (22.2%) and Cisco Scanner (20%). This study indicates that 'most of the cybercrimes are committed with the use of Network Sniffer, Password Cracker and Key Logger among others to perpetrate cybercrime. Also, Table 1 further shows the common types of cybercrimes in the selected institutions. The most common type of cybercrime reported was hacking (66.3%), followed by software piracy (60.7%), credit card fraud (58.5%), malicious programme/virus dissemination (54.4%), sweet heart swindle (53.3%), spamming (52.2%), identity theft (52.2%), website cloning/ phishing (48.1%), pornography (50.7%), and cyber defamation (48.9%). This study indicates that 'hacking and credit card fraud are among the most common types of cybercrime in higher institutions. This corroborated [15],[17].

Table 1 Technologies use and common type of cybercrime in the selected institutions

Technologies use for cybercrimes	Frequency	Percentage
Password Cracker	224	83
Key Logger	120	44.4
Network Sniffer	136	50.4
Exploit	66	24.4
Port Scanner	85	31.5
Vulnerability Scanner	72	26.7
Metaspoilt	43	15.9
Backtrack	67	24.8
Aircrack-ng	46	17
Ksmet	35	13
Wireshark	60	22.2
Cisco Scanner	54	20
Common types of cyber crime		
Hacking	179	66.3
Credit Card Fraud	158	58.5
Spamming	141	52.2
Software Piracy	164	60.7
Identity theft	141	52.2
Website cloning/Phishing	130	48.1
Pornography	137	50.7
Sweet heart Swindle (Social Network)	144	53.3
Cyber defamation	132	48.9
Malicious programme (Virus)	147	54.4

Table 2 presents the cyber securities technologies adopted by the selected institutions by showing the authentication protocols, security access control and cyber security policy adopted. The Table shows that authentication protocols adopted by the selected institutions were Radius (55.6%), CHAP and MS-CHAP (37.0%), Kerberos (22.2%), IP SEC (22.2%), EAP (18.5%), PAP and SPAP (7.4%) and Microsoft NTLM (3.7%).

Table 2 further shows the security access control adopted by the selected institutions. It can be seen that most of the universities use ID and Password Authentication (100%), the second most widely used access control is Public Key Cryptography (33.3%), followed by Biometric authentication (29.6%), Smart Card Authentication (25.9%), Multi-Layer Authentication (22.2%) and then Digital Signature/Certificate (18.5%) in descending order of importance. These cybersecurities corroborated with [19],[20],[21].

Table 2 Cyber Securities technologies adopted by the selected institutions

Characteristics	Frequency	Percentage
Authentication protocols adopted		
Kerberos	6	22.2
IP SEC	6	22.2
Microsoft NTLM	1	3.7
PAP and SPAP	2	7.4
CHAP and MS-CHAP	10	37.0
EAP	5	18.5
Radius	15	55.6
Security access control adopted		
ID and Password Authentication	270	100
Public Key Cryptography	90	33.3
Biometric Authentication	80	29.6
Smart Card Authentication	70	25.9
Multi-Layer Authentication	60	22.2
Digital Signature/Certificate	50	18.5
Cyber Security Policy adopted		
Privacy policy	7	25.9
Network security policy	7	25.9
Theft Prevention programme	4	14.8
Incidence response plan	5	18.5
Continuity/Disaster recovery plan	4	14.8
Laptop/computer use policy	5	18.5
Employee training regarding confidential information	7	25.9

This study affirmed that the use of ID and Password Authentication is prevalence organization to controlling cyber security challenges in developing nations.

In addition, Table 2 presents the adopted cyber security policy in the selected Southwestern Universities. It can be inferred from the Table that minority of the institutions do have cyber security policy. The Table shows that only 25.9% of the institutions have privacy policy, Network Security Policy (25.9%), Theft Prevention Programme (14.8%), Incidence Response Plan (18.5%), Continuity/Disaster Recovery Plan (14.8%), Laptop/Computer use Policy (18.5%) and Employee Training Regarding Confidential Information (25.9%). Based on that low number of selected institutions that adopted cyber security policy, there is high chances that users on their cyberspace are not informed on don’t and does on their cyberspace which simply means that they are not check and they can do anything they like through the use of cybercrime technologies to commit the common cybercrimes identified in Table 1. Hence, lack of cyber security policies could lead to compromise and abuse of information security network and systems.

The cyber securities as defined in this study include multi-layer authentication, public key cryptography authentication mechanism and digital signature/certificate (SSL) authentication mechanism. The three-cybersecurity effectiveness were presented in from Table 3 to Table 5.

Table 3 presents the effectiveness of multi-layer authentication mechanism on server and services. The Table shows that most of the institutions’ websites that were targeted by hackers frequently (81%), did not deploy Multi-Layer Authentication. While those that were rarely (80%) targeted deployed multilayer authentication. Hence, there was a significant relationship between frequency of cyber security threat on websites and whether the institution deployed Multi-Layer Authentication [χ_1^2 = 7.043, p = 0.008*].

Also, the Table further shows that most of the institutions’ authentication application that were targeted by hackers frequently (77.3%), did not deploy Multi-Layer Authentication. While those that were rarely (75%) targeted deployed multilayer authentication. Hence, there was a significant relationship between frequency of cyber security threat on websites and whether the institution deployed Multi-Layer Authentication [χ_1^2 = 4.342, p = 0.037*].

The Table still shows that most of the institutions’ E-portal that were targeted by hackers frequently (78.3%), did not deploy Multi-Layer Authentication. While those that were rarely (100%) targeted deployed multilayer authentication. Hence, there was a significant relationship between frequency of cyber security threat on websites and whether the institution deployed Multi-Layer Authentication [χ_1^2 = 7.630, p = 0.006*].

Table 3 indicates that most of the institutions’ Email application that were targeted by hackers frequently (77.3%), did not deploy Multi-Layer Authentication. While those that were rarely (75%) targeted deployed multilayer authentication. Hence, there was a significant relationship between frequency of cyber security threat on websites and whether the institution deployed Multi-Layer Authentication [χ_1^2 = 4.342, p = 0.037*].

Effectiveness of Public Key Cryptography Authentication Mechanism on Servers and Services

Table 4 shows the effectiveness of public key Cryptography Authentication Mechanism on Servers and Services. The Table shows that most of the institutions’ websites that were targeted by hackers frequently (75%), did not deploy Public Key Cryptography Authentication Mechanism. While those that were rarely (100%) targeted deployed Public Key Cryptography Authentication Mechanism. Hence, there was a significant relationship between frequency of cyber security

Table 3 Chi-square Test of Relationship Between Frequencies of Cyber-Attack on Server and Services and the Use of Multi-Layer Authentication

		Multi-Layer Authentication		**Sig.**	**Chi-Square**
CSTS	**Frequency**	**Yes**	**No**		
Website(s)	Rarely	(80.0%)	(20.0%)	0.008*	7.043
	Frequently	(19.0%)	(81.0%)		
Authentication Application	Rarely	(75.0%)	(25.0%)	0.037*	4.342
	Frequently	(22.7%)	(77.3%)		
E-portal	Rarely	(100.0%)	0 (0.0)	0.006*	7.630
	Frequently	(21.7%)	(78.3%)		
E-mail Application	Rarely	(75.0%)	(25.0%)	0.037*	4.342
	Frequently	(22.7%)	(77.3%)		

Keys

CSTS = Cyber security Threats on Servers / Services

*Sig. = 0.05

Table 4 Chi-square test of Relationship between frequencies of Cyber-Attack on Servers and Services and the use of Public Key Cryptography

		PCAM		**Total**	**Sig.**	**Chi-Square**
CSTSS		**Yes**	**No**			
Website(s)	Rarely	3 (100.0)	0 (0.0)	3	0.029*	6.750
	Frequently	6 (25.0)	18 (75.0)	24		
Authentication Application	Rarely	3 (75.0)	1 (25.0)	4	0.093**	3.668
	Frequently	6 (26.1)	17 (73.9)	23		
E-Portal	Rarely	2 (40.0)	3 (60.0)	5	0.029*	6.750
	Frequently	7 (31.8)	15 (68.2)	22		
E-mail Application	Rarely	3 (75.0)	1 (25.0)	4	0.093**	3.668
	Frequently	6 (26.1)	17 (73.9)	23		

Keys

PCAM = Public Key Cryptography Authentication Mechanism

CSTSS = Cyber security Threats on Servers / Services

*Sig. = 0.05; **Sig. = 0.10

Table: 5 Chi-square Test of Relationship Between Cyber-Attack on Server and Services and the Deployment of Digital Signature/Certificate (SSL) Authentication Mechanism.

		DDSC		**Total**	**Sig.**	**Chi-Square**
CSTSS		No	Yes			
Website(s)	Yes	23 (95.8)	1 (4.2)	24	0.000*	16.611
	No	0 (0.0)	2 (100.0)	2		
Email	Yes	20 (83.3)	4 (16.7)	24	0.007*	7.222

Application	No	0 (0.0)	2 (100.0)	2		
E-portal	Yes	21(87.5)	3 (12.5)	24	0.003*	9.100
	No	0 (0.0)	2 (100.0)	2		
E-learning Application	Yes	23 (95.8)	1 (4.2)	24	0.019*	5.462
	No	1 (50.0)	1 (50.0)	2		

Keys

DDSC = Deployment of Digital Signature/Certificate (SSL)

CSTSS = Cyber security Threats on Servers / Services

SSL = Secure Site Layer

*Sig. = 0.05

threat on websites and whether the institution deployed Public Key Cryptography Authentication Mechanism [χ_1^2 = 6.750, p = 0.029*].

Also, Table 4 shows that most of the institutions' authentication application that were targeted by hackers frequently (73.9%), did not deploy Public Key Cryptography Authentication Mechanism. While those that were rarely (75%) targeted deployed Public Key Cryptography Authentication Mechanism. Hence, there was a significant relationship between frequency of cyber security threat on authentication application and whether the institution deployed Public Key Cryptography Authentication Mechanism [χ_1^2 = 3.668, p = 0.093**].

Table 4 still shows that most of the institutions' E-portal that were targeted by hackers frequently (68.2%), did not deploy Public Key Cryptography Authentication Mechanism. While those that were rarely (60%) targeted deployed Public Key Cryptography Authentication Mechanism. Hence, there was a significant relationship between frequency of cyber security threat on E-portal and whether the institution deployed Public Key Cryptography Authentication Mechanism [χ_1^2 = 6.750, p = 0.029 *].

The Table further shows that most of the institutions' E-mail application that were targeted by hackers frequently (73.9%), did not deploy Public Key Cryptography Authentication Mechanism. While those that were rarely (75%) targeted deployed Public Key Cryptography Authentication Mechanism. Hence, there was a significant relationship between frequency of cyber security threat on Email application and whether the institution deployed Public Key

Cryptography Authentication Mechanism [χ_1^2 = 3.668, p = 0.093**].

Effectiveness of Digital Signature/Certificate (SSL) Authentication Mechanism on Servers and Services

Table 5 presents the effectiveness of Digital Signature/Certificate Authentication Mechanism on Servers and Services. The Table indicates that most of the institutions' websites that were (95.8%) targeted by hackers did not deploy digital signature/certificate (SSL) authentication mechanism. While those that were not (75%) targeted deployed digital signature/certificate (SSL) authentication mechanism. Hence, there was a significant relationship between cyber security threat on institutions' websites and whether the institutions deployed digital signature/certificate (SSL) authentication mechanism [χ_1^2 = 16.611, p = 0.000*].

The Table 5 further indicates that most of the institutions' authentication application that were (83.3%) targeted by hackers did not deploy digital signature/certificate (SSL) authentication mechanism. While those that were not (100%) targeted deployed digital signature/certificate (SSL) authentication mechanism. Hence, there was a significant relationship between cyber security threat on institutions' Email application and whether the institutions deployed digital signature/certificate (SSL) authentication mechanism [χ_1^2 = 7.222, p = 0.007*]. Table 5 shows that most of the institutions' E-portal that were (87.5%) targeted by hackers did not deploy digital signature/certificate (SSL) authentication mechanism. While those that were not (100%) targeted deployed digital signature/certificate (SSL) authentication mechanism. Hence, there was a significant relationship between cyber security threat on institutions' E-portal and whether the institutions deployed digital signature/certificate (SSL) authentication mechanism [χ_1^2 = 9.100, p = 0.003*].

The Table 5 indicates that most of the institutions' E-learning application that were (95.8%) targeted by hackers did not deploy digital signature/certificate (SSL) authentication mechanism. While those that were not (50%) targeted deployed digital signature/certificate (SSL) authentication mechanism. Hence, there was a significant relationship between cyber security threat on institutions' E-learning application and whether the institutions deployed digital signature/certificate (SSL) authentication mechanism [χ_1^2 = 5.462, p = 0.019*].

5. CONCLUSION

The study concluded that major technologies used for cybercrimes in the universities in Southwestern Nigeria were password cracker, key logger and network sniffer. The study also concluded that the common types of cybercrime in the universities were hacking, credit card fraud, spamming, software piracy, identity theft, pornography, sweet heat swindle and malicious programmes (virus). The study further concluded that authentication protocols deployed majorly by universities in Southwestern Nigeria were Kerberos, internet protocol (IP) securities, CHAP and MS-CHAP. The study concluded that all the universities deployed identity (ID) and password authentication for security access control while privacy policy, network security policy and employee training regarding confidential information were the cyber security policy adopted by most of the universities in Southwestern Nigeria. The study concluded that the deployment of Cyber securities such as public key cryptography and digital signature inhibits threats on servers and services of the universities. However, the study concluded that the universities that did not deploy multi-layer authentication, digital signature and public key cryptography on their internet servers are susceptible to cybercrime frequently.

6. RECOMMENDATION

It is therefore recommended that Multi-Layer Authentication Cyber security techniques be introduced to reduce the rate of cyber security threat in Institutions.

7. ACKNOWLEDGMENTS

My thanks to the experts who have contributed towards development of this paper

8. REFERENCES

[1] Akogwu, S. (2012), an Assessment of the Level of Awareness on Cyber Crime among Internet Users in Ahmadu Bello University, Zaria Unpublished B.Sc. project submitted to the Department of Sociology, Ahmadu Bello University.

[2] British Security Standard 7790/ISO Standard 17799: Information Security Management, London: British Standards Institute, 1999, Section 6.1.1-2.

[3] Shinder, D.L. (2002), Scene of the Cybercrime: Computer Forensics Handbook. Syngress Publishing Inc. 88 Hingham Street, USA.

[4] International Telecommunication Union (ITU), (2016). Available from http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (Accessed on 11th April, 2016)

[5] Hammonds W. (2013). Cyber security and universities: managing their risks. Retrieved February 14, 2016 from http://www.universitiesuk.ac.uk/highereducation/Documents/2013/CyberSecurityAndUniversities.pdf

[6] Roseline, O. and Moses, O. (2012). Cyber Capacity without Cyber Security: A case study of Nigeria's National Policy for Information Technology (NPFIT). The Journal of Philosophy, Science & Law, 12(1), pp. 1-14.

[7] Osho O., and Onoja A., (2015). National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. International Journal of Cyber Criminology (IJCC) Vol. 9 (1): 120–143. DOI: 10.5281/zenodo.22390.

[8] Agba, P.C. (2002), International Communication Principles, Concepts and Issues. In Okunna, C.S. (ed) Techniques of Mass Communication: A Multi-dimensional Approach. Enugu: New Generation Books.

[9] Vladimir, G. (2005), International Cooperation in Fighting Cyber Crime. Available from www.crimeresearch.org (Accessed on 7th December, 2015)

[10] Oyewole and Obeta (2002), An Introduction to Cyber Crime. Retrieved on September 2011 from http//www.crimeresearch.org/articules/cyber-crime

[11] Binuyo, G. O., Olasupo, J.O., and Ogunjemilua, E. M. (2016). A Study of the Application of Information and Communications Technology in Customer Relationship Management in Selected Airlines in Nigeria. International Journal of Computer Applications, 139(1), 24 – 30.

[12] Nigerian National Policy for Information Technology (2001): Cyber security policies in Nigeria, Federal Ministry of Science and Technology, Abuja.

[13] McConnell L. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institution in Zaria-Kaduna State, Nigeria. American International Journal of Contemporary Research, 3(9), pp. 98-113.

[14] 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.

[15] Olugbodi, K. (2010), Fighting Cyber Crime in Nigeria. Retrieved September 10, 2011 from http//www.guide2nigeria,com/news_articles_About_Nigeria

[16] Adebusuyi, A. (2008): The Internet and Emergence of Yahoo boys sub-Culture in Nigeria, International Journal of Cyber-Criminology, 0794-2891, 2 (2) 368-381.

[17] Frank I. and Odunayo E. (2013). “Approach to Cyber Security Issues in Nigeria: Challenges and Solution”. International Journal of Cognitive Research in science, engineering and education 1(1), pp. 2-9.

[18] Rouse M. (2005). Definition of Spam. Available fromhttp://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol. (Accessed on September 16th, 2015)

[19] Oppenheimer P. (2010). Developing Network Security Strategies. Pearson Education, Cisco Press, October 4, 2016.

[20] Duncan, A.J., Creese, S. and Goldsmith, M. (2012). “Insider attacks in cloud computing, in Trust, Security and Privacy in Computing and Communications (Trust Com)”, IEEE 11th International Conference, pp. 857–862.

[21] Tamara S. (2014). Security of Multifactor Authentication Model to Improve Authentication Systems. Information and Knowledge Management, 4(6), pp. 81-86.

[22] Pipkin, D.L, (2000). Information Security. Upper Saddle River, NJ: Prentice Hall

[23] Bertino, E., Martino, L. D., Paci, F. and Squicciarini, A. C. (2010). “Web services threats, vulnerabilities, and countermeasures,” in Security for Web Services and Service-Oriented Architectures. Springer, 2010, pp. 25–44.

[24] Kizza, J.M., (2013). Guide to Computer Network Security. Department of Computer Science and Engineering, University of Tennessee-Chattanooga, USA.

[25] Nilsson J., (2006). “Vulnerability Scanners”, Unpublished Master of Science Thesis submitted to Department of Computer and System Sciences, Royal Institute of Technology, Kista, Sweden.

[26] Bassett R., Bass L. and O'Brien P. (2006). Computer Forensics: An Essential Ingredient forCyber Security. Journal of information Science and Technology (JIST) 3(1), pp. 23-29.

[27] McGraw, G. (2006). Software Security: Building Security In, Adison Wesley Professional.

[28] Bacudio G., Yuan X., Chu B. and Jones M. (2011). An overview of Penetration Testing. International Journal of Network Security and Its Applications, 3(6), pp. 19.