IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 29, Issue 1, Series 3 (January, 2024) 40-50
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Cyber Security Risk Assessment In The Banking Sector: Challenges And Ways Forward

Bala Modi[1] And Rebecca Akinmolayan [2]
[1]*reader In Department Of Computer Science, Gombe State University, Gombe-Nigeria.*
[2]*stanbic Ibtc Bank Plc.*

ABSTRACT
The study employs a cross sectional descriptive survey design to gather information from respondents on cyber security risk assessment in banking sector: challenges and ways forward. One major observation made in the research is that, information attacks can be launched by anyone, from anywhere. This indeed emphasizes the need for the government security agencies and banks information security experts to note that there is need to keep up with technological and security advancements. It will always be a lost battle if security professionals are miles behind the cyber criminals.
KEYWORDS: *Cybercrime, IT, Fraud, Banking Sector.*

Date of Submission: 02-01-2024 Date of Acceptance: 12-01-2024

I. INTRODUCTION

The role that Information and Communications Technology (ICT) plays in all aspects of human endeavors is well documented and evident. ICT has integrated different economies of the world, through the aid of electronics via the internet. Many corporate organizations, including banks now depend on ICT and computer networks to perform basic as well as complex tasks. The electronic market is now open to everybody, including criminals. It is projected that by 2021, global Cyber security spending will reach $170bn, a 126% increase from $75bn in 2015.

According to the World Economic Forum's report Globalization 4.0, more organizations than ever are conducting business online (Davos, 2019). The spate of rising preponderance of digital footprints and sophistication in cyber-attacks has prompted the urgency to intensely secure data and other organizational resources from exposure to activities of cybercriminals.

From business, industry, government to not-for-profit organizations, the internet has simplified business processes such as sorting, summarizing, coding, editing, customized and generic report generation in a real-time processing mode. However, it has also brought unintended consequences such as criminal activities, spamming, credit card frauds, Automated Teller Machine (ATM) frauds, phishing, identity theft and a blossoming haven for cybercriminal miscreants to perpetrate their insidious acts (Olumide, 2010). The advent of the internet to us was both welcome and full of disadvantages.

The exceptional outbreak of cyber-crime in Nigeria in recent times has been quite alarming, and the negative impact on the socio-economy of the country is highly disturbing. Over the past twenty years, immoral cyberspace users have continued to use the internet to commit crimes; this has evoked mixed feelings of admiration and fear in the general populace along with a growing unease about the state of cyber and personal security. This phenomenon has seen sophisticated and extraordinary increase recently and has called for quick response in providing laws that would protect the cyber space and its users. Statistically, all over the world, there has been a form of cyber-crime committed every day since 2006 (Schaeffer, 2009).

Prior to the year 2001, the phenomenon of cyber-crime was not globally associated with Nigeria. This resonates with the fact that in Nigeria we came into realization of the full potential of the internet right about that time. Since then, however, the country has acquired a world-wide notoriety in criminal activities, especially financial scams, facilitated through the use of the Internet (Roseline, 2012). Nigerian cyber criminals are daily devising new ways of perpetrating this form of crime and the existing methods of tracking these criminals are no longer suitable to deal with their new tricks. The victims as well show increasing naivety and gullibility at the prospects incited by these fraudsters (Thompson, 1989).

As such it is imperative to know that even basic cyber security awareness may not translate into sufficient or appropriate cyber security protection knowledge to mitigate cyber risks and hazards against victims. As a result, it is critical to increase cyber security knowledge through training programs that use

theoretical lectures and simulators to provide exposure to cyber security protection infrastructure (Limna, Kraiwanit & Siripipattanakul (2022). Attention should be on operational, usage, and process aspects of improving user familiarity and translating it into effective cyber security mitigation behaviour (Zwilling et al., 2022).

Technological development has improved daily life in areas such as online banking and shopping. The digital domain has become an important factor in the world and information and communication technology has proved to be a very vital factor in productivity, growth and innovation (Rosewarne, 2014). In recent years, the world has greatly developed technologically and the development has also affected accounting practices (Ernst and Young, 2013). However, the growth of the information and communication technology environment is accompanied by new and serious threats. Cyber-attacks now have the ability to greatly harm the society in new and critical ways. Online fraud and cyber-attacks are just a few examples of computer related crimes that are committed on an extremely large scale every day (Gercke, 2006).

Our specific research objectives are:

- ✓ To determine methodologies used to hack into banking systems
- ✓ To highlight potential risks involved in the loss of data and other banking related information
- ✓ To provide possible remedies to the identified problems

This study would, at the end, serve as a pointer to the importance of properly securing banking cyber space. It will highlight new methodologies used by hackers to gain access to banking data and information and societal monies. The study will also serve as reference for future studies and researchers.

II. LITERATURE REVIEW

As technology has developed so have also the definitions of cyberspace, cyber security and cybercrimes. It has been argued that since computer crime may involve all categories of crime, a definition must emphasize the particularity, the knowledge or the use of computer technology. Cyber-space refers to the boundless space known as the internet. It refers to the interdependent network of information technology components that underpin many of our communications technologies in place today.

The International Telecommunications Union (2014) defines Cyber security as 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. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

Basically, Cyber security is the protection of systems, networks and data in cyberspace and is essential even as more people get connected to the internet across the world. The International Telecommunications Union (ITU) also notes that the three broad security objectives are ensuring Availability; Integrity (which may include authenticity and non-repudiation), and Confidentiality. While these are the bedrock of a secure network, achieving these three objectives is no mean feat as it requires the integration of various functions such as robust systems engineering and configuration management; effective cyber security or information assurance policy and comprehensive training of personnel.

Cyber-security measures are put in place because any information stored on a computer or electronic device or on the Internet can be hacked, and with the proper measures in place, this can be prevented. As the world is more reliant on computers than ever before, cyber security has become essential. In order to ensure that a system is secure, one must understand the risks and vulnerabilities inherent to that specific device or network and whether or not these vulnerabilities are exploitable.

According to the ITU (2014) Cyber security refers to 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. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment - the internet.

Farhat *et.al*, (2011) define a cyber-attack as an attack initiated from a computer against a website, computer system or individual computer (collectively, a single computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it. They further noted that cyber-attacks may take the following forms:

1. Gaining, or attempting to gain, unauthorized access to a computer system or its data;
2. Unwanted disruption or denial of service attacks, including the take down of entire web sites;

3. Installation of viruses or malicious code (malware) on a computer system;
4. Unauthorized use of a computer system for processing or storing data;
5. Changes to the characteristics of a computer system's hardware, firmware or software without the owner's knowledge, instruction or consent;

Inappropriate use of computer systems by employees or former employees.

From the various definitions given above, one could rightly say that cyber-attack is a criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud".

One of the largest hacks in history involved a financial institution which had its servers hijacked. The stolen data, in this case, was used to commit ongoing fraud schemes yielding some $100 million. More recently, the Security and Exchange Commission (S.E.C) announced its computer system had been hacked in 2016. The hack provided the thieves with private information that may have been exploited to commit insider trading. Not only is this hack an issue in the crime itself, but is also notable in its undermining of the public's trust in the financial system itself. Although the repercussions are somewhat unknown at this time, the Security and Exchange Commission (S.E.C) recognizes that there will continue to be attacks and that a key factor of cyber risks management is resilience and recovery (Stevenson and Tejadasept, 2017).

III. METHODOLOGY

A total of 100 samples were randomly selected across banks operating in Gombe. This study employed random sampling technique to draw 100 respondents from five (5) banks within the study area (i.e., Gombe City). There are a total number of sixteen banks in the study area. The five sample banks will be randomly selected from these banks. This will bring it to 20 respondents per bank. The selected banks include Guaranty Trust Bank (GTB), First Bank, Stanbic IBTC, Zenith Bank and Access Bank.

The main data collation instrument employed in this study was a 20-item questionnaire; the questions simply required respondents to give information on their knowledge level about cyber security and how cybersecure their various organisations are.

The validity of instrument was to ensure that the instrument measures what it is supposed to measure. The questionnaire was carefully and thoroughly scrutinised by the project supervisor and necessary corrections were observed to avoid bias in order to achieve the project's objectives.

Data for the study was collected through administration of the research instrument. The the consent of the participants was sort first by initial introduction as well as presentation of the aim and objectives of the study before administering the questionnaire. Thus, those who showed the willingness to participate were issued with one copy of the questionnaire. The participants were instructed to complete all items on the questionnaire after which they were retrieved for collation and analysis.

In order to analyse the data and make inferences for the study, the table method of data analysis was used to derive useful meaning from the data collected from the respondents through the questionnaires.

IV. FINDINGS

In this subsection, we carried out the trend analysis; presented the results of the various tests, presented the descriptive statistics and correlation results and then the regression results.

Trend analysis

Table 1.1: Sex of respondents

		Frequency	Percent	Valid Percnt	Cumulative Percent
Valid	MALE	53	53.0	53.0	53.0
	FEMALE	44	44.0	44.0	97.0
	NO RESPONSE	3	3.0	3.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table above shows data on the genders of the respondents in the various banks. The table shows that 53% of the respondents are males and 44% are females. The table further showed that 3 of the respondents

left their gender status anonymous. The results from Table 1.1 show that, there are 9% male respondents more than their female counterparts. From the findings, there are more male staff conversant with the methodologies used to hack into banking systems compared to their female counterparts. This simply means that the male users are more likely to proffer possible remedies to the identified problems.

Table 1.2: Age distribution of respondents

Frequency tabulation was used to present the age range distribution categories of the respondents. Table 1.2 presents the results:

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	12	12.0	12.0	12.0
	56	56.0	56.0	68.0
	31	31.0	31.0	99.0
	1	1.0	100.0	
	100	100.0	100.0	

Source: Fieldwork, 2021

From the results on Table 1.2, 56% which is the majority of the respondents belonged to the 30 – 39 age range whereas the least among the respondents belonged to above 50 years of age with 1%. Majority of the results were gotten from the young respondents. This implies that majority of the respondents were youth, they are very conversant with emerging technologies and adapt easily to its usage.

Table 1.3: Educational background of respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	School cert	0	0.0	0.0	0.0
	Diploma	27	27.0	27.0	27.0
	University	51	51.0	51.0	78.0
	Postgraduate	22	22.0	22.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table above shows that the majority of the respondents which represents 51% had attained Bachelor's Degree, while 22% of the respondents had a Postgraduate degree. The results show that none of the respondents used their secondary school certificate to procure the banking job. Therefore, this implies that, majority of the respondents were educated, technologically advanced, and excellent adaptors who have grown with the trend and are able to respond to the research questions accordingly.

Table 1.4: **Duration of stay of respondents in the bank**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 2 years	13	13.0	13.0	13.0
	More than 2 years but less than5years	23	23.0	23.0	36.0
	More than 2 years but less than 10years	33	33.0	33.0	69.0
	Ten years and above	31	31.0	31.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table above show data on the duration of the stay of the respondents at the bank. While 13% of the respondents have worked at the bank for less than 2 years, 33% and 31% of the sampled respondents have worked at the bank for more than 5 years but less than 10 years and more than 10 years respectively.

This implies that more than half of the respondents have enough experience in the system and have

been able to highlight potential risks involved in the loss of data and other banking related information.

Table 1.5: Responsibility at the Bank

Office Held	No of Respondents	Percentage (%)
Customer Service Officer	25	25
Cash officer	40	40
Asset Custodian	15	15
Head of operations	5	5
Consumer/commercial Banking Officer	7	7
Manager	8	8
Total	**100**	**100**

Source: Fieldwork, 2021

The table above shows data on the responsibilities of the respondents in the various banks. The table shows that 25% of the respondents are customer service officers, 40% are cash officers, 15% are asset custodians. They further showed that 5 of the respondents which is 5% of the sampled population are Head of Operation officers, 7% are consumer/commercial Banking Officers while 8% are branch managers. Cash officers which represent 40% of the respondents are at a very high risk of being exposed because of their job roles, followed by Asset custodians, Commercial Banking officers, Head of Operations and then lastly, managers.

Table 1.6: Cyber security needs to be increased for our hardware and data

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	AGREE	33	33.0	33.0	33.0
	STRONGLY AGREE	64	64.0	64.0	97.0
	UNDECIDED	3	3.0	3.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table above shows an analysis of responses received from the questionnaire. It shows that 33 respondents which represent 33% of the sampled respondents agree that the arrival of IoT (Internet of Things) and the clamour for more efficiency of our mobile devices has revamped the way people connect and businesses operate. But even as the drive for more connection and connectivity has increased, the same way the need for cyber security to be increased for our physical hardware, internet supply and corporate data 64 respondents representing 64% strongly agreed, and 3 respondents were undecided

Table 1.7: The procedures hackers employ to break into networks and information

Procedures	No of respondents	Percentage (%)
Mobile banking weak points	51	51
Trojans	40	40
Malware	57	57
App hijacking	5	5
Phishing	17	17
Key loggers	3	3
SIM swapping	2	2
Pharming	6	6
System hacking	80	80
Spamming	42	42

Source: Fieldwork, 2021

The table above shows that more respondents believe that system hacking, malware, mobile banking weak points, spamming and trojans are the most common methodologies used by hackers to gain access to

bank's network and information. In descending order respectively, these respondents represent 80%, 57%, 51%, 42% and 40% of the sampled respondents.

As for phishing, 17% of the respondents agreed to it as a common procedure. SIM swapping, key loggers, app hijacking and pharming were selected by 2%, 3%, 5% and 6% respectively.

Table 1.8: Cyber-breaches are more rampant and difficult to unravel.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	AGREE	53	53.0	53.0	53.0
	STRONGLY AGREE	45	45.0	45.0	95.0
	DISAGREE	2	2.0	2.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table above shows that 53 respondents which represent 53% of the sampled respondents agree that Cyber-breaches and attacks are becoming more rampant, and at the same time they are evolving, becoming complicated and more difficult to unravel, curb and solve, 45 respondents representing 45% strongly agreed, and 2 respondents representing 2% were undecided.

Table 1.9: New danger prototype facing institutions worldwide

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	AGREE	51	51.0	51.0	51.0
	STRONGLY AGREE	44	44.0	44.0	95.0
	DISAGREE	5	5.0	5.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table above shows that 51 respondents which represent 51% of the sampled population agree that organizations across the world face a new risk paradigm, one that encompasses cyber and physical threat**s**, 44 respondents representing 44% strongly agreed, and 5 respondents representing 5% were undecided.

Table 1.10: Businesses have to be concerned about loss of money and credibility

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	AGREE	18	18.0	18.0	18.0
	STRONGLY AGREE	69.0	69.0	69.0	87.0
	DISAGREE	2	2.0	2.0	89.0
	UNDECIDED	11	11.0	11.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table above shows that 18 respondents which represent 18% of the sampled population agree that in the world of today, the primary targets for hackers are banks, credit unions, and financial organizations of all types. Aside the financial losses, all businesses have to be concerned about the following: reputational damage leading to diminishing of the trust of the customer, employee safety and brand credibility, 69 respondents strongly agree, 2 respondents representing 2% disagreed that this is not the case and 11 which represents 11% were undecided.

Table 1.11: The cost of losing money and credibility cannot be easily quantified

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	AGREE	38	38.0	38.0	38.0
	STRONGLY AGREE	51	51.0	51.0	89.0
	DISAGREE	2	2.0	2.0	91.0
	UNDECIDED	9	9.0	9.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table above shows that 38 respondents which represent 38% of the sampled population agree **t**he consequence in terms of diminishing of the trust of the customers /clients of brand credibility is most overwhelming and the cost cannot be easily quantified**, 5**1 respondents representing 51% strongly agreed, 2

respondents which represents 2% were disagreed while 9 respondents which represents 9% were undecided.

Table 1.12: Staff are given security awareness handbooks

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	AGREE	42	42.0	42.0	42.0
	STRONGLY AGREE	45	45.0	45.0	87.0
	DISAGREE	2	2.0	2.0	89.0
	STRONGLY DISAGREE	11	11.0	11.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

When asked on whether Information system security awareness manuals are provided to staff by the bank management, the table shows that 42 respondents which represent 42% of the sampled population agree that information technology and security awareness handbooks are given to staff by the management of the bank, 45 respondents representing 45% strongly agreed. This implies that a higher percentage of staff in banks are not ignorant and are aware of the methodologies used by hackers to gain access to the banks' data and also the risks associated with the loss of that data. 2 respondents which represents 2% of the sampled population disagreed while 11 respondents representing 11 respondents was undecided.

Table 1.13: Institutions need to cooperate to lessen intimidations successfully

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	AGREE	32	32.0	32.0	32.0
	STRONGLY AGREE	67	67.0	67.0	99.0
	UNDECIDED	1	1.0	1.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The responses in the table 1.13 received on the question implies majority are conscious of the need for institutions to cooperate in order to lessen these intimidations successfully. This shows that 32 respondents which represent 32% of the sampled population agreed, 67 respondents representing 67% strongly agreed while 1 respondent which represent 1% was undecided.

Table 1.14: Noteworthy profits to cooperating to be cyber intelligent.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	AGREE	32	32.0	32.0	32.0
	STRONGLY AGREE	66	66.0	66.0	98.0
	DISAGREE	2	2.0	2.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table shows responses received on benefits to be enjoyed if financial institutions across the country and globe should collaborate. Coming together and harnessing the human and technology resources we have from all departments can efficiently identify dangers; change trends and swiftly access valuable data to make sure our security and safety targets are achieved.

Responses received show that 32 respondents which represents 32% of the sampled population agreed, 66 respondents which represent 66% strongly agreed with the option, and 2 respondents (2%) were undecided.

Table 1.15: Merging physical and cyber security transmutes notifications into actionable intelligence.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	AGREE	44	44.0	44.0	44.0
	STRONGLY AGREE	47	47.0	47.0	91.0
	UNDECIDED	9	9.0	9.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table above shows that 44 respondents which represent 44% of the sampled population agree the merging of physical and cyber security together transmutes notifications into actionable intelligence and this

enables end users to join the bits of every scenario and give a joint feedback to the appropriate analysts and operators. 47 respondents representing 47% strongly agreed, 9 respondents which represent 9% were undecided.

Table 1.16: The Nigerian government and stakeholders can do more for cybersecurity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	AGREE	20	20.0	20.0	20.0
	STRONGLY AGREE	73	73.0	73.0	93.0
	UNDECIDED	7	7.0	7.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table above shows that 73 respondents representing 73% strongly agree that there is more that could be done to secure financial institutions from cyberattacks by the Nigerian government and other stakeholders, 7 respondents which represent 7% were undecided.

Table 1.17: Employees are supplied with I.T security policies handbooks

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	YES	89	89.0	89.0	89.0
	NO	11	11.0	11.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table above shows responses received on the availability of IT security policies and procedure manual for employees. It is received that 89 respondents indicated that the bank has Information Technology security policies and procedure handbooks for employee orientation while 11 respondents indicated otherwise. This implies that the staff in the banks nationwide have been equipped to know the procedures used by hackers, they are also aware of the risks that come with losses and also means they know they are the first line of defence to protect the bank's data and information.

Table 1.18: How often does the organisation carry out information systems security awareness exercise?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	MONTHLY	11	11.0	11.0	11.0
	QUARTERLY	44	44.0	44.0	55.0
	HALF YEARLY	11	11.0	11.0	66.0
	YEARLY	22	22.0	22.0	88.0
	NOT DONE AT ALL	12	12.0	12.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table above shows responses on how often the sampled financial institutions carryout system security awareness exercise. They show that 12 respondents which represent 12% of the sampled population said the exercise is not done in the bank, 11 respondents indicated that it is done monthly, 44 respondents said it is done on a quarterly basis. This is a very active way to make all staff up-to-date on the importance of being alert and not to be seen or caught off guard. Another 11 respondents said it is done after six months (i.e., half of the year), and 22 respondents representing 22% of the respondents said it is done yearly.

Table 1.19: Who are the audiences to the information system security awareness in the institution?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	TOP LEVEL MANAGERS ONLY	22	22.0	22.0	22.0
	SUPERVISORS ONLY	7	7.0	7.0	29.0
	PERMANENT STAFF ONLY	4	4.0	4.0	33.0
	EVERYONE	67	67.0	67.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table above shows responses on who the audiences to the information system security awareness in the institution are. They show that while 67 respondents said it cuts across all staff of all cadre whether permanent or contract staff (exclusive of cleaners and security personnel). This means a great percentage of bank staff are fully equipped and integrated to combat financial crime.

22 respondents which represent 22% of the sampled population said top level managers are the audiences for system information security awareness, 7 which represents 7% of the respondents indicated that it is the supervisors only, 4 (4%) of the respondents said it is only permanent staff excluding contract staff which increases the potential risks and the knowledge gap needs to be filled.

Table 1.20: Are information system security awareness manuals provided to staff

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	YES	89	89.0	89.0	89.0
	NO	11	11.0	11.0	100.0
	Total	100	100.0	100.0	

Source: Fieldwork, 2021

The table shows responses received on the availability of IT security policies and procedure manual for employees. It is received that 89 respondents indicated that the bank has IT security policies and procedure manuals for employee reference while 11 respondents indicated otherwise.

V. CONCLUSION AND RECOMMENDATIONS

From the findings of the study, one could easily deduce that information has become a key resource within financial organizations. Business success or failure is often determined by the quality of information gathered and the ability to store, share and use this information to gain competitive advantage. The emergence of the Internet of Things and a demand for more mobile capabilities has changed the way people and businesses connect.

But as the need for connectivity increases, so too does the need for increased security for physical assets, networks, and valuable corporate data. As technology advances, so also does the methodologies used by hackers to gain access to bank networks and information. This has made cyber-attacks more prevalent, more sophisticated and harder to address. Once an attack is said to be successful, the affected loses credibility to its customers this adversely affects the brand name and its reputation.

The importance of information system security awareness manuals to staff of financial institutions cannot be overemphasised. Numerous benefits of information system security awareness program include; the institution staff and users become knowledgeable about the vulnerabilities in the technology they use, the threats to information they handle, policies they must comply with and the tools at their disposal to help them overcome threats. Another benefit to awareness training that is not always considered is the deterrent factor of being monitored.

According to Maiwald and Sieglein (2002) if users are made aware of the policies they must follow and then told the company's ability to monitor compliance, they are less likely to conduct mischief. Collaboration between these financial institutions has proven by studies to be beneficial as the mutual understanding serve as a front against internet fraudsters. Audiences to the information system security awareness in financial institutions should involve staff at all levels of the organisation. Awareness training increases the ability to hold employees accountable for their actions.

Further, as Wilk (1993) states, one principal purpose of information system security awareness is to reduce errors and omissions. It can also reduce fraud and unauthorized activity by increasing employees' knowledge of accountability and the penalties associated with such actions. Both the dissemination and the enforcement of cyber security policies are critical issues that are strengthened through awareness programs. Employees cannot be expected to follow policies and procedures of which they are unaware. Awareness stimulates and motivates those being trained to care about security and to remind them of important security practices. Explaining what happens to an organization, its mission, customers, and employees if security fails motivates people to take security seriously. Penalties for non-compliance to standard can be abrupt for banks just not only financially but also in greatly increased oversight. Having compliance standard stimulates banks to focus on cybersecurity.

When a bank stays compliant, it ensures that it is meeting consensus security and protecting the customer data. One could never tell what area or means or when the fraudsters might try to access a bank's information system and the extent of damage that could be incurred if such should be allowed to happen. This makes cybersecurity is important for every profit and non-profit making institutions. Banks and other financial institutions carry important information about the customers and the attackers know it, so it important for banks and financial institutions to have a robust cyber security in place.

REFERENCES

[1]. Abass J.S. (2009). A Survey Of Implementation Of Information Security Awareness Programs By Financial Institutions In Kenya
[2]. Adebusuyi, A. (2008): The Internet And Emergence Of Yahoo Boys Sub-Culture In Nigeria, International Journal Of Cyber-Criminology, 0794-2891, Vol.2(2) 368-381, July-December
[3]. Adeniran J.I. (2011) Bank Frauds In Nigeria: Underlying Causes, Effects And Possible Remedies. African Journal Of Accounting, Economics, Finance And Banking Research, 6(6): 62-79.
[4]. African Academic Network On Internet Policy. (2020) "Critical Data Security Issues In The Nigeria Banking Sector," African Academic Network On Internet Policy, P. 8,
[5]. Ali, A.Y., Pocock, K., & Hu, Q. (2014), The Effect Of Board Of Directors' It Awareness On Cio Compensation And Firm Performance. Journal On Decision Sciences, 45(3), 401-436.
[6]. Augustine, C. Odinma, M. (2010): Cybercrime & Cert: Issues & Probable Policies For Nigeria, Dbi Presentation, Nov 1-2.
[7]. Augustine K.V. (2010) Management Information Systems- Managing Information Technology In The Business Enterprise. New Delhi, Tata Mcgraw Hill Publishing Company
[8]. Benzmuller M. (2017). Cyber Crime: Prevention & Detection," International Journal Of Advanced Research In Computer And Communication Engineering, Vol. 4(3).
[9]. Bonger, W. (1916); Capitalism And Crime- Encyclopaedia Of Criminological Theory
[10]. Daniel, A. Sofaer, David Clark, Whitfield Diffie, (2008). Proceedings Of A Workshop On Deterring Cyberattacks: Informing Strategies And Developing Options For U.S. Policy
[11]. Cybercrimes Prohibition, Prevention Act Of The Federal Republic Of Nigeria (2015).
[12]. Davos, A., Laprie J. (2019): Dependability And Its Threats: A Taxonomy. Article Ifip Advances In Information And Communication Technology Broadhurst R. (2006): Developments In The Global Law Enforcement Of Cyber‐Crime, Policing: An International Journal Of Police Strategies & Management, Vol. 29 Issue: 3, Pp.408-433, Emerald Group Publishing Limited.
[13]. Ernst & Young, (2013), Viewpoints Issue 19; 2012. Available From: Http:// Www.Ey.Com/Publication/Vwluassets/Acls_Viewpoints_19_ May_2012/$File/Acls_Viewpoints_19_May_20102.Pdf.
[14]. European Network And Information Security Agency. (2006) Guide On How To Raise Information Security Awareness.
[15]. Farhat, R H Goudar. (2011). A Cyber Era Approach For Building Awareness In Cyber Security For Educational System In India Pritisaxena, Iacsit International Journal Of Information And Education Technology, Vol. 2, No. 2, April 2012 Iosr Journal Of Computer Engineering (Iosr-Jce)
[16]. Fong-Hao, L. (2007). Constructing Enterprise Information Network Security Risk Management Mechanism By Using Ontology ‖0-7695-2847-3/ Ieee.
[17]. Generali Global Assistance. (2017, October 30). Infographic: Help Your Customers Overcome Cybersecurity Fears By Promoting Cyber Awareness. Retrieved From: Http://Us.Generaliglobalassistance.Com/Blog/Customers-Cyber-Awareness/
[18]. Gercke, M. (2006)."The Slow Wake Of A Global Approach Against," Computer Law Review International, Vol. 2(2), P. 141.
[19]. Hassan, A. B., Lass, F. D. And Makinde J. (2012): Cyber Crime In Nigeria: Causes, Effects And The Way Out, Arpn Journal Of Science And Technology, Vol. 2(7), 626 –631.
[20]. Ibm. (2017). 2017 Ponemon Cost Of Data Breach Study. Retrieved From Https://Www.Ibm.Com/Security/Data-Breach
[21]. International Telecommunications Commission [Itu] (2011) "Making The Online World Safer" Http://Www.Itu.Int/Net/Itunews/Issues/2011/05/38.Aspx
[22]. Jack F & Ene R. (2014). Cyber Security: The Changing Role Of Audit Committee And Internal Audit. Available From: Https://Www.2.Deloitte.Com/ Content/Dam/Deloitte/Sg/Documents/Risk/Sea-Risk-Cyber-Security-Changing-Role-In-Audit-Noexp.Pdf.
[23]. Jackson, R.H. (2016). A Cyber Era Approach For Building Awareness In Cyber Security For Educational System In India Pritisaxena, Iacsit International Journal Of Information And Education Technology, Vol. 2, No. 2, April 2016
[24]. Jolaosho A.O. (1996): Some Popular Perceptions Of Poverty In Nigeria, Quoted In Undp Human Development Report On Nigeria. Lagos: Undp.
[25]. Kaspersky Lab. (2017, June 14). Cyber Threats To Online Banking Services Cost Banks Nearly $1.8 Million. Retrieved From Https://Usa.Kaspersky.Com/About/Press-Releases/2017_Cyberthreats-To-Online-Banking-Services-Cost-Banks-Nearly-18-Million
[26]. Khan E.R. (1999). Developing The Theoretical And Conceptual Framework. Retrieved From: Http:// Journclasses.Pbworks.Com/F/ Theoretical+Framewor.Ppt.
[27]. Laura A. (2011). Cyber Crime And National Security: The Role Of The Penal And Procedural Law.
[28]. Lewis J.A. (2013), Raising The Bar For Cyber Security. Washington, Dc: Technology And Public Policy, Centre For Strategic And International Studies.
[29]. Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2022). The Relationship Between Cyber Security Awareness, Knowledge, And Behavioural Choice Protection Among Mobile Banking Users In Thailand. International Journal Of Computing Sciences Research. Advanced Online Publication.Https://Doi.Org/10.25147/Ijcsr.2017.001.1.123
[30]. Lindros, K. & Tittel, E. (2016, May 4). What Is Cyber Insurance And Why You Need It. Retrieved From: Https://Www.Cio.Com/Article/3065655/Cyber-Attacks-Espionage/What-Is-Cyber-Insurance-And-Why-You-Need-It.Html
[31]. Longe, O. B, Chiemeke, S. (2008): Cyber Crime And Criminality In Nigeria – What Roles Are Internet Access Points In Playing?, European Journal Of Social Sciences – Volume 6, Number 4
[32]. Maiwald, E. & Sieglein W. (2002), Security Planning And Disaster Recovery, New York
[33]. Mcquade, S (2006). Understanding And Managing Cybercrime, Boston: Allyn & Bacon.
[34]. Meke, E.S.N. (2012) Urbanization And Cyber Crime In Nigeria: Causes And Consequences.
[35]. Miller, S. A. (2006). Children's Understanding Of Second Order Mental States. Psychological Bulletin, 135(5), 749–773
[36]. Mitnick. K. (1999) The Art Of Deception: Controlling The Human Element Of Security, New York Macmillan Publishing Company
[37]. Mohsin, O. B, (2006). Cyber Crime And Criminality In Nigeria – What Roles Are Internet Access Points In Playing?, European Journal Of Social Sciences – Volume 6, Number 4
[38]. Moore, M. (2016). Don't Ignore Ddos Protection When Attack Trends Change. Retrieved From Https://Betanews. Com/2017/06/26/Ddos-Protection-Do-Not-Ignore-Trends-Change/
[39]. Morgan, S. (2016, January 27). Bank Of America's Unlimited Cybersecurity Budget Sums Up Spending Plans In A War Against Hackers. Retrieved From Https://Www.Forbes.Com/Sites/Stevemorgan/2016/01/27/Bank-Of-Americas-Unlimited-Cybersecurity-Budget-Sums-Up-Spending-Plans-In-A-War-Against-Hackers/#925202a264cd
[40]. Morris, D. (2016, October 22). How Hackers Make Money From Ddos Attacks. Retrieved From

Http://Fortune. Com/2016/10/22/Ddos-Attack-Hacker-Profit/
[41]. Neil, M (2016). Bank Tellers May Pose Greater Threat To Customers Than Hackers, Ny Times Says Retrieved From Http://Www.Abajournal.Com/News/Article/Bank_Tellers_May_Pose_Greater_Threat_To_ Customers_Than_Hackers_Ny_Times_Say
[42]. Nigeria Electronic Fraud Forum (Neff) Annual Report Of 2018
[43]. Nitda (2020). Towards A Systematic Approach For Improving Information Security Risk Management Methods‖, In Proc. 18th Annual Ieee International Symposium On Personal, Indoor And Mobile Radio Communication (Pimrc), 2007.
[44]. Odumesi O. J. (2014). A Socio-Technological Analysis Of Cybercrime And Cyber Security In Nigeria International Journal Of Sociology And Anthropology · April 2014 Doi: 10.5897/Ijsa2013.0510
[45]. Odunfa, A. (2014), Nigeria: Report On Cyber Threat Calls For Quick Passage Of 2012 Bill. Available From: Http://Www.Allafrica.Com/ Stories/201405080279.Html.
[46]. Oliver, E. O. (2015): Being Lecture Delivered At Dbi/George Mason University Conference On Cyber Security Holding, Department Of Information Management Technology Federal University Of Technology, Owerri, 1-2 Nov.
[47]. Olumide, O. O., Victor, F. B. (2010): E-Crime In Nigeria: Trends, Tricks, And Treatment. The Pacific Journal Of Sciencea And Technology, Volume 11. Number 1. May 2010 (Spring)
[48]. Oren, S. (2017, June 29). Protecting Financial Institutions – Q&A With Deep Instinct's Shimon Noam Oren. Retrieved From Http://Www.Itproportal.Com/Features/Protecting-Financial-Institutions-Qa-With-Deep-Instincts-Shimon-Noam-Oren/
[49]. Osagwu P. (2019, March 8), Cyber Attack: 60% Of Nigerian Businesses Attached In 2018, Vanguard, Retrieved From Https://Www.Vanguardngr.Com/2019/03/Cyber-Attack-60-Of-Nigerian-Businesses-Attacked-In-2018/
[50]. Ponemon. (August 2015). The Cost Of Phishing And The Value Of Employee Training. Retrieved From Https:// Info.Wombatsecurity.Com/Hubfs/Ponemon_Institute_Cost_Of_Phishing.Pdf
[51]. Quinney, R. (1973,1977). Crime Control In Capitalist Society
[52]. Rainie, L. (2016, September 21). The State Of Privacy In Post-Snowden America. Retrieved From Http://Www. Pewresearch.Org/Fact-Tank/2016/09/21/The-State-Of-Privacy-In-America/
[53]. Rasmussen, T. (2005) Building A Security Awareness Program, Computer Technology Research Corporation.
[54]. Ravi, S, (2012) Study Of Latest Emerging Trends On Cyber Security And Its Challenges To Society. International Journal Of Scientific & Engineering Research, Volume 3, Issue 6, June -2012 1 Issn 2229-5518 Ijser
[55]. Roberts, J.J. (2017, June 21). Here Are 10 Of The Biggest Corporate Hacks In History. Retrieved From Http://Fortune.Com/2017/06/22/Cybersecurity-Hacks-History/
[56]. Roseline, O. M. (2012): Cyber Capacity Without Cyber Security: A Case Study Of Nigeria's National Policy For Information Technology (Npfit), The Journal Of Philosophy, Science & Law Volume 12, May 30, 2012, Retrieved From Www.Miami.Edu/Ethics/Jpsl
[57]. Rosewarne, S. (2014), Migrant Domestic Work: From Precarious To Precarisation. Journal Fuer Entwicklungspolitik (Austrian Journal Of Development Studies), 30(4), 133-154.
[58]. Schaeffer, B. S., Et' Al. (2009): Cyber Crime And Cyber Security: A White Paper For Franchisors, Licensors, And Others
[59]. Securities And Exchange Commission. (2018). "Commission Statement And Guidance On Public Company Cyber Security Disclosures".
[60]. Shin, L. (2017, January 14). Be Prepared: The Top 'Social Engineering' Scams Of 2017. Retrieved From Https://Www.Forbes.Com/Sites/Laurashin/2017/01/04/Be-Prepared-The-Top-Social-Engineering-Scams-Of- 2017/#247030887fec
[61]. Stevenson, A. & Tejadasept, C. (2017, September 20). S.E.C. Says It Was A Victim Of Computer Hacking Last Year. Retrieved From Https://Www.Nytimes.Com/2017/09/20/Business/Sec-Hacking-Attack.Html
[62]. Strassmann, P. A. (2009): Cyber Security For The Department Of Defense, Retrieved July 10, 2011 From Http://Www.Strassmann.Com/Pubs/Dod/Cybersecurity-Draft-V1.Pdf
[63]. The Internet Engineering Task Force (Ietf) (2007) Guide On How To Raise Information Security Awareness.
[64]. Thomas, F, (2007). Institute For Advance Management System Research (Iamsr) ―A Dss For Information Security Analysis: Computer Support In A Company's Risk Management‖0-7803-3280-6/ 1996 Ieee
[65]. Thompson, D. (1989): Police Powers-Where's The Evidence, Proceedings Of The Australian Computer Abuse Inaugural Conference.
[66]. Wada, F. & Odulaja G.O. (2012): Assessing Cyber Crime And Its Impact On E-Banking In Nigeria Using Social Theories. African Journal Of Computing & Icts. Vol 5., No. 1, Pp 69-82.
[67]. Wade H. Baker And Linda Wallace ―Is Information Security Under Control? Investigating Quality In Information Security Management‖ 1540- 7993/ 2007 Ieee
[68]. Wilk, R.J. (1993) Security And Control Of Your Pc/Micro Network, International Association For Computer System Security, New York Usa
[69]. Woods, C. C. (2001), "Information Security Policies", Pentasafe Security Technologies, Texas – Usa
[70]. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge And Behavior: A Comparative Study. Journal Of Computer Information Systems, 62(1), 82-97.