Internet Banking in Nigeria:
Cyber Security Breaches, Practices and Capability

Victoria Wang, Harrison Nnaji & Jeyong Jung

Abstract

This paper reports the findings from a research project on cyber security in the Nigerian Internet banking industry, by presenting the main cyber security breaches it has experienced, along with its cyber security capability and practices. An online survey was conducted with 100 experienced professional working in both the Nigerian banking and banking security service sectors. Our findings reveal a transformation of the Nigerian cybercrime industry from low-tech cyber-enabled crimes to high-tech sophisticated breaches, with viruses, worms or Trojan infections; electronic spam mails; and hacking being the top three most experienced breaches. In term of cyber security practices, banking professionals have received adequate management in both support and training. The lack of advanced technologies to prevent and address cyber security breaches and the unsatisfactory level of legislative compliance, together, appear to be the primary factors that have reduced cyber security capability in our sample of banks.

Keywords: Nigeria, Internet Banking, cyber security, breaches, capability, practices

1. Introduction

The past decade has seen a rapid adoption of the Internet in virtually all sectors of the economy, but particularly the banking sector. In 2017, internet banking was expected to grow to a global user base of 2 billion by 2020 (Reportlinker, 2017). A few months later, in February 2018, it was estimated that over 2 billion global users would access banking services via a range of mobile devices, including smartphones, tablets, PCs and smartwatches. This would be reached by 2018 – 2 years earlier than previously anticipated (Juniper Research, 2018). Based on the current rate of growth, the global population is expected to reach 7.76 billion by 2020 (UN, 2017), therefore slightly over a quarter (25.8%) of the global population will be using internet banking by 2020.

The implementation of internet banking has, on the one hand, brought about many benefits. These include reduced costs, expansion of the market, and improvements in the speed of service (Oruç and Tatar, 2017). On the other hand, internet banking creates a significant new opportunity for criminals to commit various types of crime – both traditional organised crimes (Lavorgna and Sergi, 2014) and cyber security breaches (Deloitte, 2017). Cyber-mediated breaches of security targeting financial institutions had, in fact, increased by more than 30% between 2015 and 2017, where more than $3 trillion was siphoned from the system (Dunkley, 2017). It is stated that financial services (e.g., banks) fall victim to cyber security attacks 300 times more frequently than businesses in other services (Schaffer, 2018).

Nigeria has itself been heavily affected by cybercrime (Doyon-Martin, 2015; United Nations Office on Drugs and Crime, 2011; Zylberberg and Klimburg, 2015), to the extent of being identified as the 4th global hot spot of cybercrime just behind Russia, China and Brazil (Rayman,

2014). Financially, cybercrime costs the Nigerian economy around US 500 million dollars annually (Shiloh & Fassassi, 2016). In terms of types of crime, both Nigerian perpetrators and victims are more likely to be implicated in money-related cases, rather than socio-political crimes (Ibrahim, 2016). Nigeria has, in fact, suffered from a reputation of being a haven of cyber-enabled fraudulent activities (Ebenezer et al., 2016; Ojedokun and Eraye, 2012). These would include the notorious 419 scam that spread around the world from 1980s onwards (Arewa, 2018) and more recently 'online advanced fee fraud' (Osho and Onoja, 2015).

Yet, Nigerian cybercrime is itself in constant transformation, launching ever more sophisticated and organized attacks (Hinchliffe, 2017). With the recent emergence and growth of internet banking in Nigeria, financial institutions have become ever more reliant on computer systems to perform their daily businesses (Lagazio et al., 2014). This, in turn, has provided a new opportunity that perpetrators of cybercrime may exploit (Raghavan and Parthiban, 2014). Cyber security breaches have, in fact, become one of the main threats affecting the Nigerian banking industry, generating considerable damage to this sector (Ojeka et al., 2017).

There is, however, a significant short fall in the literature concerning research on cyber security in the nation's banking sector. This could be attributed both to the secretive and competitive nature of the banking industry in general, and to the characteristics of Nigerian society in particular. This would include political instability, high levels of traditional crime, and poverty (e.g., Ibrahim, 2016). As a result of this, exploratory empirical research is now needed to begin to address this challenge. In this paper, we present the findings of such research. It is a small-scale research of an exploratory nature that begins to explore the types of cyber secuirty breach experienced in the

Nigerian banking industry, along with this industry's current cyber securitiy practices and general capability. An online survey was conducted with 100 randomly selected experienced professionals working in the Nigerian banking sector and banking security service sector.

2. Internet banking in Nigeria and its associated threats – An overview

Nigeria has been investing heavily in the development of information technologies. It was estimated in December 2017 that more than 50% of its population now uses the internet. This is almost 100 million individuals (Internet World Stats, 2018 a, b), making it the 8th largest globally with the highest number of Internet users. This development of information technologies has also accelerated the growth of the Nigerian economy. For example, during the same period, its GDP increased from 369 billion USD to 405 billion USD between 2010 and 2016 (World Bank, n. d.), while its Internet penetration increased from 11.5% to 25.7% (Statistica, 2018).

Internet banking was first introduced to Nigeria in 2003 (Oni and Ayo, 2010). The event was marked by the introduction of Guidelines on Electronic Banking in Nigeria (CBN, 2003) by the Central Bank of Nigeria (CBN). A recapitalization of the Nigerian banking industry took place soon afterwards, with only 25 banks out of the previous 89 banks in Nigeria surviving this recapitalization. Those that survived were known to have engaged in the use of internet technologies for effective and efficient delivery of banking services (Akanbi et al., 2014; Udo et al., 2012). The term 'internet banking' tends to be used interchangeably with online banking. They refer to a range of banking services via a range of technical platforms and electronic devices, such as the internet, computers, mobile phones, and bank cards (Martins et al., 2014; Rawashdeh, 2015). The range of banking services include i) Automated Teller Machines (ATMs); ii) Point of Sale

terminals (POS terminals) that handle cheque verification, credit authorization, cash deposit and withdrawal, and cash payment; iii) Personal Computer (PC) and mobile phone banking that primarily uses personal computers and mobile phones as banking devices; iv) card systems that use plastic smart cards with embedded integrated circuits to settle financial transactions.

In the last few years, customers' appetite in Nigeria for internet banking has grown rapidly. Internet banking services have also developed rapidly with banks expanding their delivery channels online, providing almost all offline banking services via the Internet (Tarhini et al., 2015). Despite these benefits, however, its adoption still remains remarkably low in Nigeria, with just over 40% of customers having used online banking platforms for one or more banking activities (KPMG, 2017). The main barriers to a greater acceptance of internet banking in Nigeria have proved to be the lack of security and trust, limited privacy, and an inadequate telecommunications infrastructure; along with a low literacy level, and an unreliable electricity supply (Agboola, 2006; Akanbi et al., 2014; Auta, 2010; Chiemeke et al., 2006, KPMG, 2017, Udo et al., 2012). Yet of all these factors, security emerged as the most significant factor in Auta's (2010) research, which used an exploratory 'principle component factor analysis' to identify the underlying factors determining the success of internet banking in Nigeria.

The revolutionary service changes in the Nigeria banking industry have, in fact, brought about a new wave of security problems (Ehimen and Bola, 2010). Cyber security breaches have become a key phenomenon affecting the Nigerian banking industry (both the banks and their customers) (Tade, 2013). While there is not a standard method to measure the financial cost of these breaches (figures in different reports tend to vary significantly), the degree of financial damage experienced

by them is reported to be very high and increasing rapidly (Odunfa, 2014). According the report in 2013 of the Nigerian Inter-Bank Settlements Systems (NIBSS Plc), Nigerian banks lost 159 billion Nigerian Naira between 2000 and the first quarter of 2013 to cyber security breaches (Akwaja, 2014). Moreover, more than half of the loss occurred in 2010 when the internet became a popular banking tool (Ojeka et al., 2017). Nigeria had, more generally, lost around 500 billion Nigerian Naira between 2010 and 2017 on reported and unreported cases of online fraud/cybercrime across major sectors of the economy, which included both the banking and telecommunications sectors (Okamgba, 2017). Besides financial loss, reputational loss brought about by security breaches, while not quantifiable, may be even harder for banks to recover. The biggest cost of a data breach is indeed reputation in terms of the erosion of brand value (Ponemon Institute, 2017). Reputational loss of a bank may, in fact, reverberate through the whole banking system by increasing the reputational risk of other banks (Pennathur, 2001).

The most prominent types of cyber security breach in the global banking sector would include Phishing; cyber terrorism; malware attacks; Bank Verification Number (BVN) scams; fraud-identity theft; password sniffing; and theft of bank cards (Reyes et al., 2011). Interestingly, for Wada and Odulaja (2012), Phishing, cyber terrorism, electronic spam mails, cyber-stalking, and fake copy-cat websites, constitute the most prominent types of cyber security breach in the Nigerian banking industry. Four years later, Omodunbi et al. (2016) suggest that Bank Verification Number (BVN) Scams, Phishing, Theft of Bank Cards, Cyber-theft/Banking Fraud are the most prominent types of cyber security breach in this industry.

Phishing refers to the sending of unsolicited emails to the customers of monetary institutions, with the intention to encourage them to enter their information, such as username and password to access their account, usually into electronic forms in fake copy-cat websites (Hassan et al., 2012). These fake copy-cat websites take advantage of consumers who are not familiar with the exact web addresses and interfaces of their banks. The perpetrators are then asked to access online bank accounts of customers without their knowledge. The phishing scam is now perceived as a very common type of cyber security threat and is becoming one of the fastest growing threats affecting the financial sector in Nigeria (Akanle et al., 2016).

Cyber terrorism refers to the launching of attacks on organizations or governments to access or distort information stored in their computer systems (Nhan and Bachmann, 2010). Cyber extortion through Distributed Denial of Services attacks (DDOS) could be a possible method. It involves putting computer systems under DDOS attacks and demanding ransoms to restore services.

Cyber extortionists have, in recent years, increasingly attacked institutions' websites and networks, thus hampering their ability to function. Malware is a term used to refer to viruses, worms, Trojans and other malicious software that enter a computer without the knowledge of the owner (Bossler and Holt, 2009). In the financial sector, Trojan horse has emerged as one of the most common techniques used to create an automated attack on computer systems. This is known as a salami attack, in which small amounts of resources are stolen, a slice at a time, from a larger pool, without being noticed (ibid.).

Bank Verification Number (BVN) scam is another form of cyber security threat, particularly in Nigeria that affects the banking industry (Taylor et al., 2014). A BVN is a biometric identification system that uses an 11-digit number as a universal identifier across all banks in the country. The primary reason for the introduction of this system, by the central bank of Nigeria, has been to link all the bank accounts of an individual in order to minimize fraudulent activities (Brody et al., 2007). Its implementation, however, also provided fraudsters with an opportunity through which to carry out fraudulent activities on a much larger scale.

Identity theft refers to the legitimate use of an account to retrieve crucial information relating to the account (Brody et al., 2007). In Nigeria, fake online banking web pages have increasingly been used by fraudsters to retrieve valuable information from users' accounts, such as pin numbers and usernames (Olasanmi, 2010). Generally, the use of false 'copy-cat' websites has emerged as one of the latest trends in online deception. These take advantage of internet users, who are unaccustomed to the internet and/or do not know the exact web address/interface of the organisation that they want to access online (Ahmad et al., 2010).

Password sniffing has also emerged as a foremost cyber secuirty threat affecting the banking sector (Olasanmi, 2010). The threat involves the use of programs that are specifically designed to monitor all traffic in an organisation's network. When a user types in his/her username and password as requested by the system, the sniffing program collects all that information (Stabek et al., 2010). Additional programs are then used to filter the information gathered, pulling out some important details, while covering up the existence of password sniffers. Evidence suggests that a significant

number of financial institutions across the globe are now affected by attacks linked to password sniffing (Brody et al., 2007).

A further but now common cyber security threat remains the theft of bank cards. This has, however, evolved from physically stealing a card to stealing the card numbers online (Asokhia, 2010). Now, perpetrators do not have to be in the same location as the victims in order to steal their identities. For example, hidden cameras can be used by perpetrators to record customers' ATM card pins. Perpetrators can also use ATM skimming, which involves putting an electric device on an ATM to record the information from the magnetic strip of a bank card whenever an individual inserts the card (FBI, 2011). Information obtained from this process could be used to perform a range of criminal activities, e.g., internet order fraud (Asokhia, 2010).

3. Methods

A quantitative methodological approach provided the basis for our research. By way of an online survey, we explored the current status of cyber security in the Nigerian banking industry. Our three research questions were:

1. What are the key types of cyber security breach experienced in the Nigerian banking industry?
2. What are the key security practices employed in the Nigerian banking industry?
3. What is the level of security capability of the Nigeria banking industry?

The survey was carried out in the spring of 2017 via the Online Survey (formally BOS) after obtaining an ethical approval from the host university. In total, 15 banks and 27 banking security

services were involved in this research. To gather good quality data, we insisted on two conditions: 1) information security officers included in our research must have worked in the information security department in any banking environment for at least two years; and 2) bank directors and managers included must have been involved in the design and implementation of information security programs in their institutions. From those organisations, a sample of 115 participants was randomly recruited from individuals befitting one of those two conditions, and 100 of them completed the survey (incomplete questionnaires were not included in the final analysis). The 100 participants came from two sectors: i) the Nigerian banking sector (72%); and ii) the Nigerian banking security service sector (28%). Just under one third, 33% of them were female and 67% were male. The gender difference occurred, of course, by chance since they were selected randomly. In terms of age, 46% of them were older than 35, and the rest were between 25 and 35 (see: Table 1).

In terms of their professions, 18% of our participants were Information Technology (IT) experts, 27% were managers, 28% were banking industry security service providers, and 27% were security practitioners in the banking industry (see: Table 1; below).

Table 1: Demographic characteristics of participants

	Items		**Total**	**Percentage**
Age	25-35 years		54	54%
	36-45 years		32	32%
	Above 45 years		14	14%
Gender	Males		67	67%
	Females		33	33%
	Banking sector	IT experts	18	18%

Profession		Security practitioners	27	27%
		Bank managers and directors	27	27%
	Banking security service providers		28	28%

To develop this highly specific and hard to research sample, we contacted managers of various Nigerian banks that had fully integrated internet banking into their operations. We asked them to act as gate keepers to select suitable participants. Next, a link to the survey – with a participant consent form detailing the aim of this research, the ways that data collected could be used, and various ethical issues in the first screen – was sent to those selected. Via clicking the start button in the first screen, the participants confirmed both their consent and that of their employers'. The data collected was analysed by the Statistical Package for the Social Sciences (SPSS Version 21). During this research, we observed various ethical standards set out by the host University's Ethics Committee. We paid particular attention to our participants' right to withdraw at any time, their privacy and anonymity, and data confidentiality.

This is, of course, an initial exploratory exercise on an area with only a limited literature. The findings are presented and discussed based on the quantitative online survey. According to Brinkmann (2014), this method, is highly inflexible and it limits participants' contribution to the research. As a result, unearthing new insights about the research topic becomes difficult because participants are restricted in terms of what they are asked to express. To further explore our research questions, a mixed-method methodology, with both a larger survey research and qualitative face-to-face interviews, will need to be employed to provide room for data

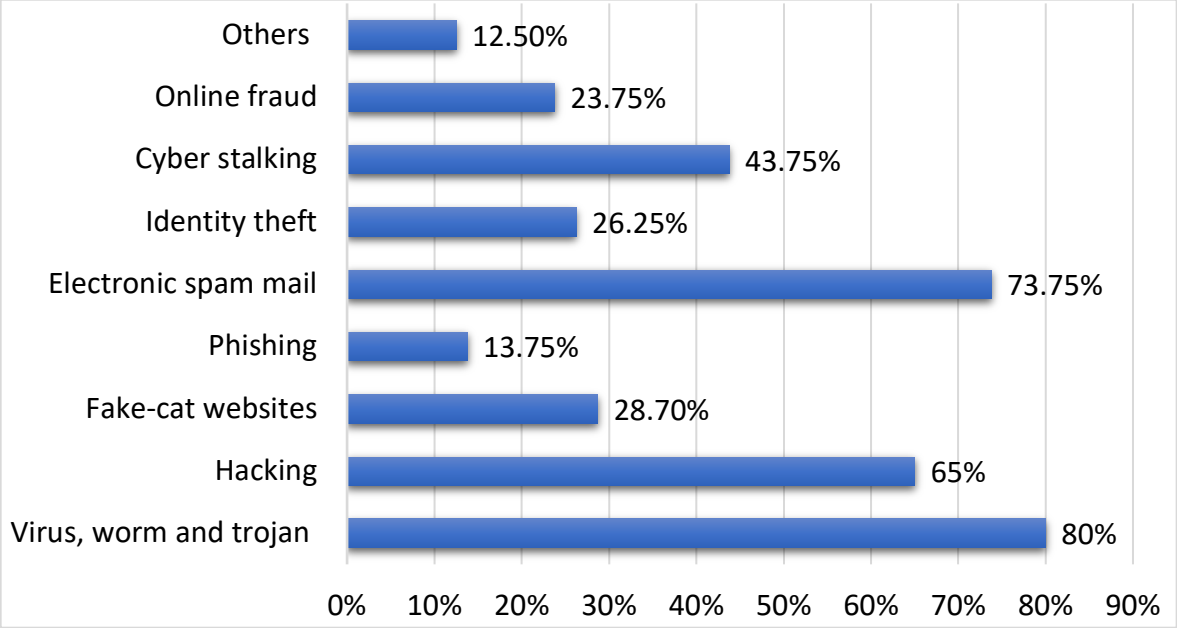
triangulation, and thus to generate findings that are more reliable and generalisable (Taylor et al., 2015).

4. Main findings

4.1. Cyber security breaches

The participants were asked to indicate whether they had experienced any of the cyber security breaches enlisted in Figure 1 in their respective institutions during the past six months (see: Figure 1; below).

Figure 1: Experience of cyber security breaches in the Nigerian banking industry (N = 80)

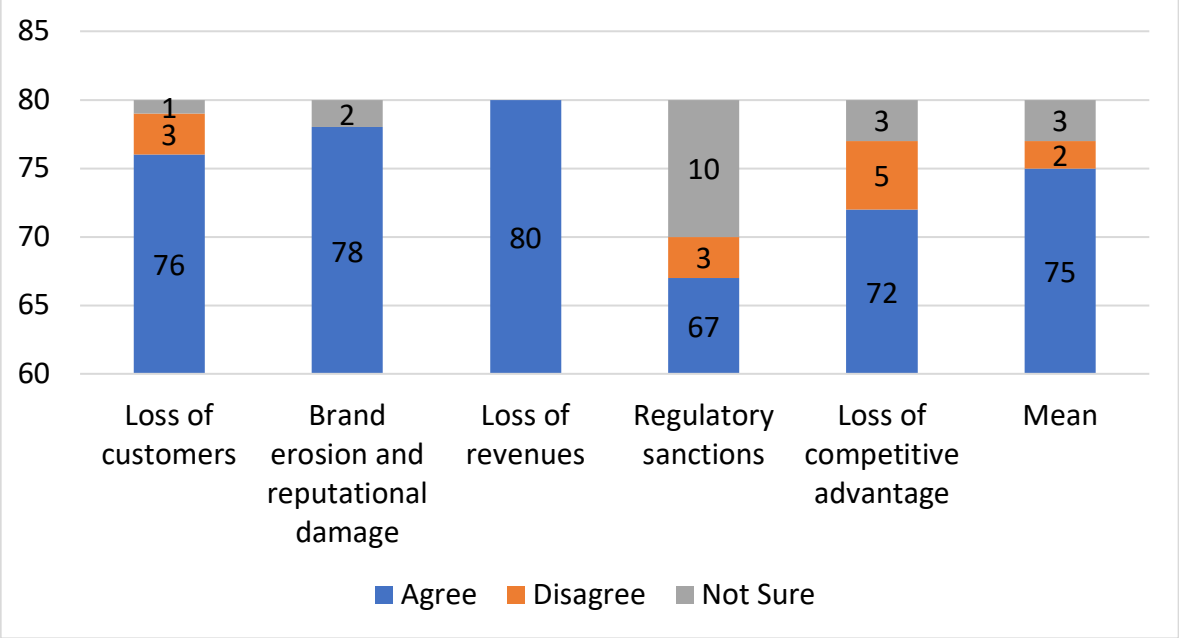


80 out of the 100 participants (80%) reported having experienced one or more types of breaches at work, whereas 20 of them reported not having experienced any of these breaches at work. The most significant four types of cyber security beaches experienced were i) virus, worm, and trojan infections (80%); ii) electronic spam emails (73.8%); iii) hacking (65%); and iv) cyberstalking

(online harassment or abuse) (43.75%). The category labelled 'others' includes ATM card theft and password sniffing, which altogether were reported to have been experienced by 12.5% of the participants. It should be noted that only 23.75% of the participants reported having experience online fraud.

The 80 participants, who reported having experienced one or more types of breaches at work during the past six months, were next asked to indicate the types of negative impacts that those breaches had on their respective banks. On average, 75 (93.3%) of the 80 participants agreed that those cyber security breaches had negatively impacted upon the banking sector. All of them considered 'loss of revenues' as a negative impact; 78 (97.5%) of them considered 'brand erosion and reputational damage' as a negative impact; and 76 (95%) of them considered 'loss of customers' as a negative impact (see: Figure 2; below). Fewer participants 67 (83.8%) considered 'regulatory sanctions' as a negative impact.

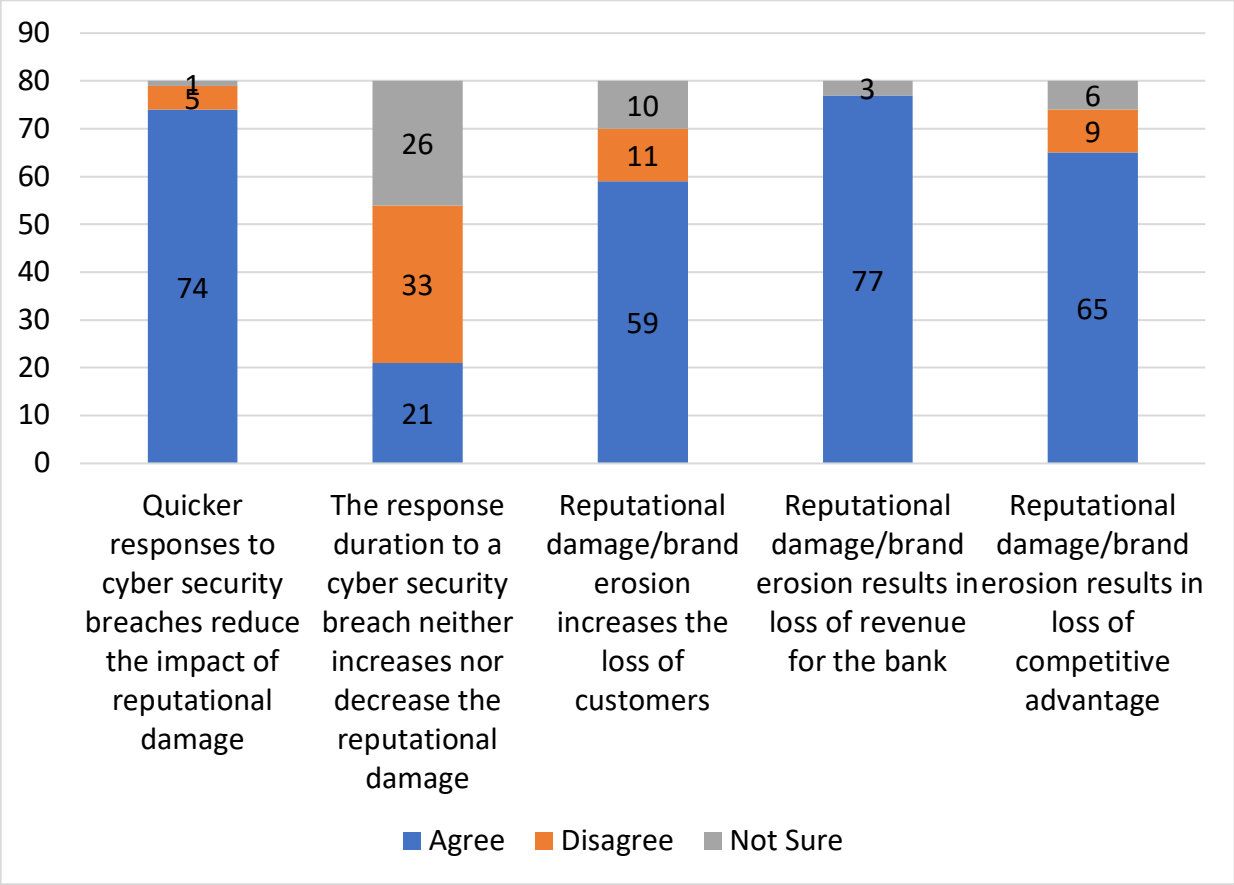
Figure 2: Impacts of cyber security breaches (N=80)



4.2. Cyber security practices

The amount of time that it takes for an organisation to respond to a cyber security breach is critical in reducing any possible negative impact, especially in terms of reputational damage. The investigation team must determine the root cause of the breach and the scope of its potential reach (e.g., levels of systems penetration and amounts of data stolen) in order to develop a response plan (Global Risks Report, 2015). As argued in Section 2, reputational damage, although not quantifiable, could lead to significant collateral damage. Our participants were next asked to indicate whether they 'Agreed', 'Disagreed' or were 'Not Sure' about the impact of the five situations, indicated in the figure below, on the performance of their banks after detecting a cyber-security breach (see: Figure 3; below).

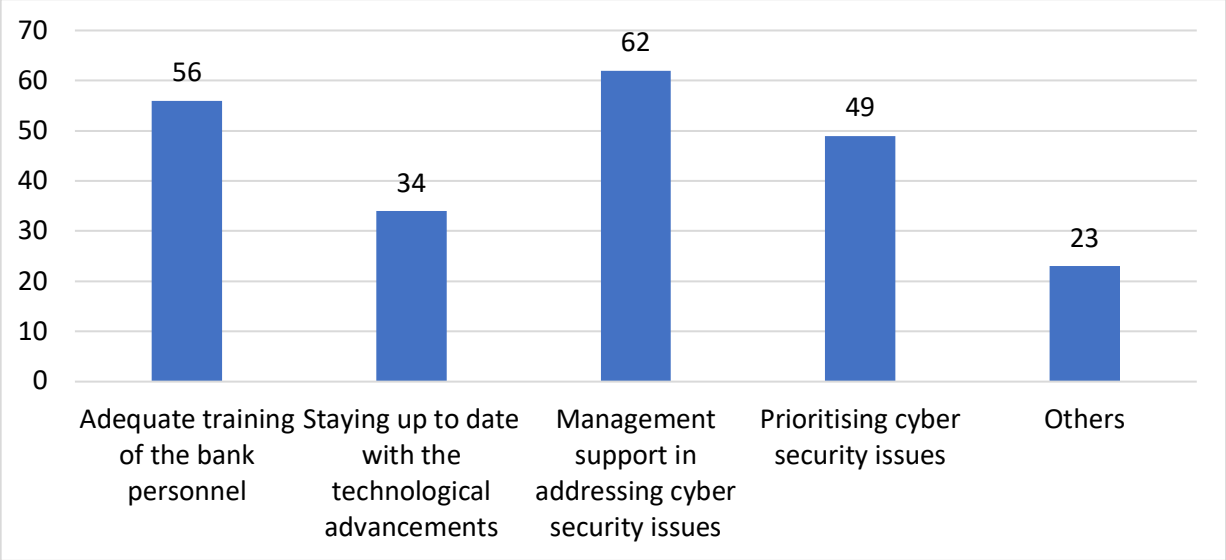
Figure 3: Duration of response and reputational damage (N = 80)



Most of the participants (74; 92.5%) agreed that a 'quick response to cyber threats could significantly reduce the impact of reputational damage' on the banks (see: Figure 3). Over a quarter (26.3%; 21) agreed that 'the response duration to a cyber-attack neither increased nor decreased reputational damage'. In terms of the consequences of reputational damage/brand erosion, 96.3% (77) agreed that these resulted in loss of revenue for the bank. Moreover, 81.3% (65) of them agreed that these resulted in a loss of competitive advantage; 73.8% (59) confirmed that these resulted in the loss of customers.

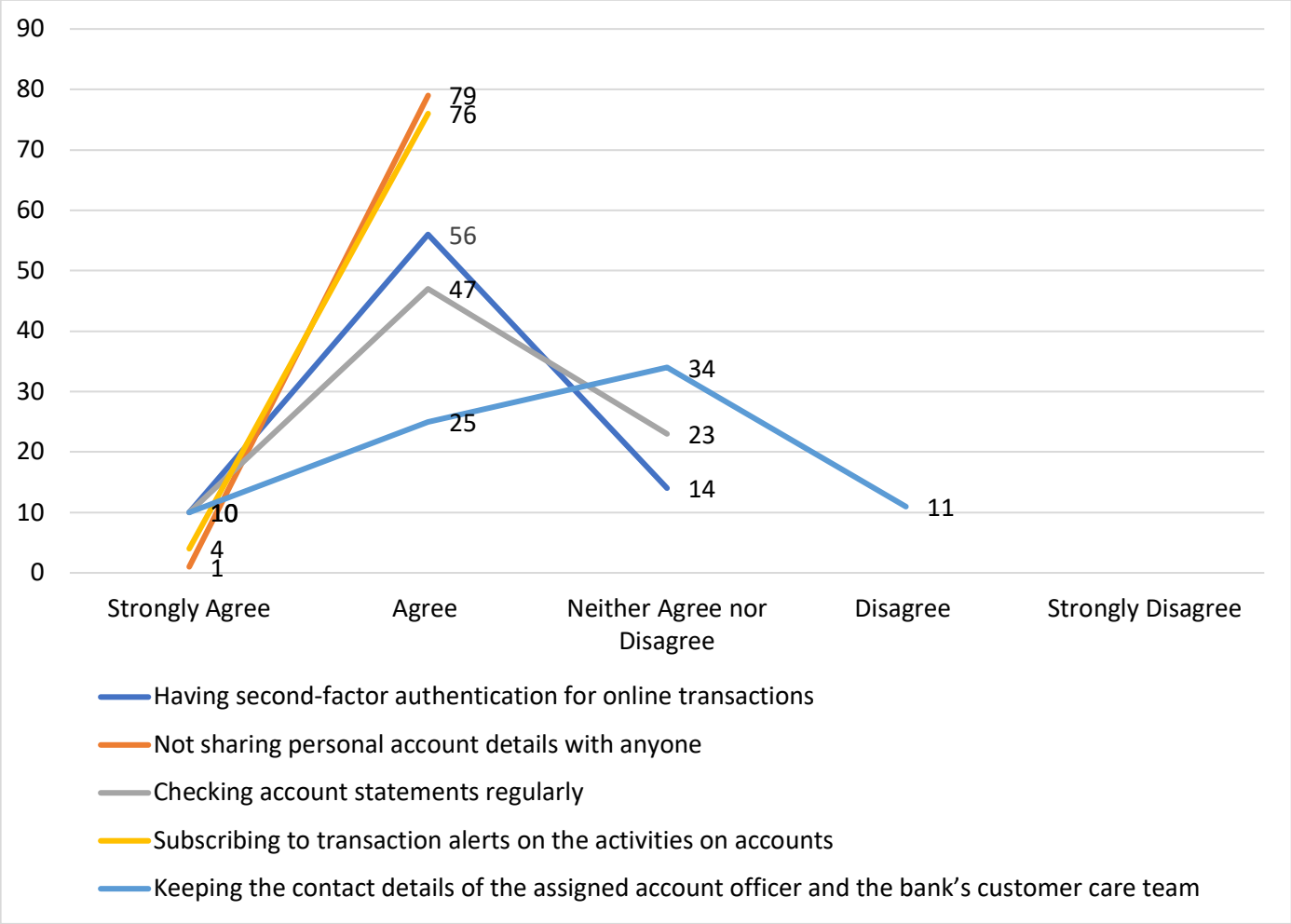
In terms of general security practices to prevent potential cyber threats that the banks had carried out, 70% (56) of participants indicated that their respective banks had invested in 'adequate training for their employees to detect and handle any potential cyber security threats' (see: Figure 4; below). Over 75% (62) indicated that the management of their respective banks had provided the 'necessary support to address cyber security issues'. Some of the support activities outlined included ensuring that computers and servers were installed with updated anti-virus software; establishing cyber security plans and committees; and providing any support required by information security teams. Over 60% (49) stated that their banks 'prioritised cyber security issues'. It appears that the lack of advanced technologies to prevent and address cyber security threats is a significant problem confronting Nigerian banks. Just over 40% (34) of the participants indicated that their banks 'stay up to date with the latest technologies'.

Figure 4: Practices employed by banks to prevent potential cyber security threats (n=80)



Further, using a 5-point Likert scale, we asked the participants to rate their respective banks' existing practices to protect their customers (see: Figure 5; below).

Figure 5: Effectiveness of practices to protect customers from cyber security breaches (N = 80)



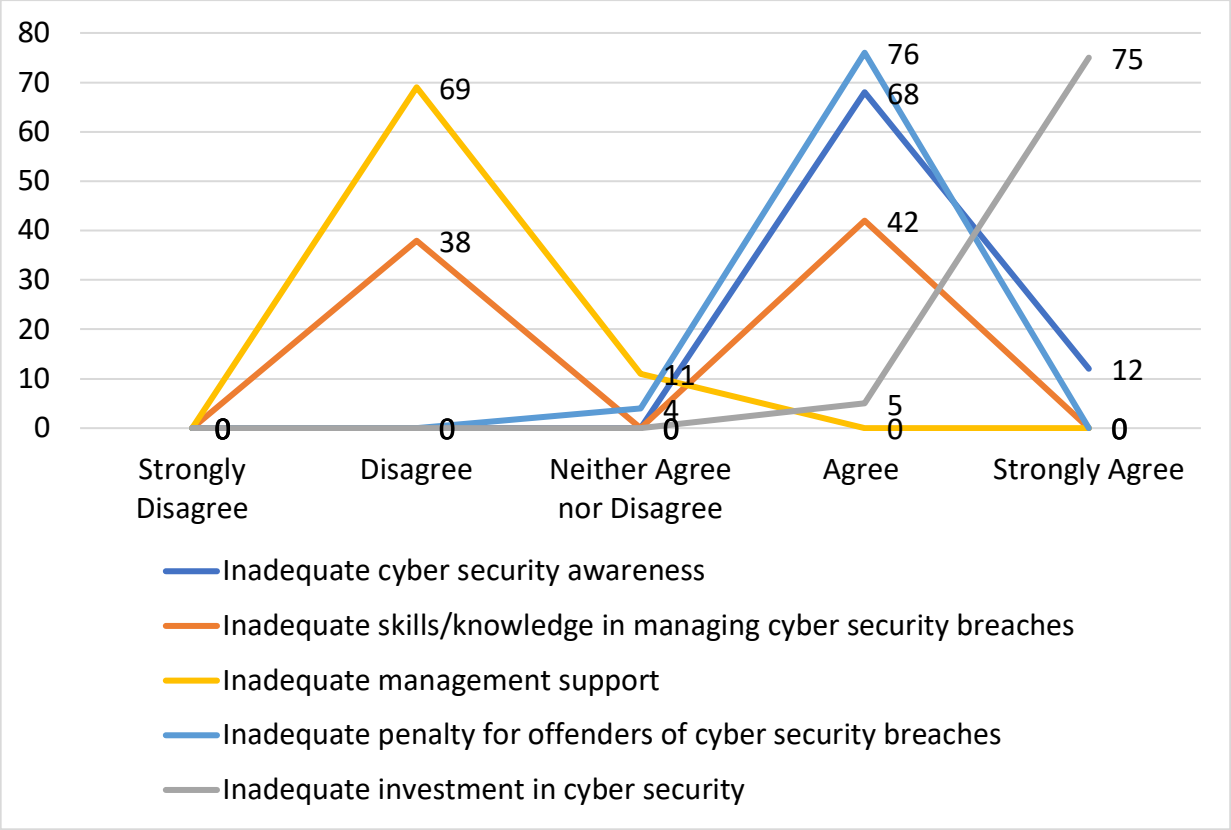
Our data indicated that all of our participants (80) agreed or strongly agreed that 'subscribing to transaction alerts on the activities on accounts' and 'not sharing personal account details with anyone' are effective preventative measures. More than 80% (66) of them agreed or strongly agreed that 'having second-factor authentication for online transactions' is an effective preventative measure. They also considered 'checking account statements regularly'; and 'keeping

contact details of assigned account officers and the bank's customer care team' as being far less effective than the other three measures.

4.3. Cyber security capability

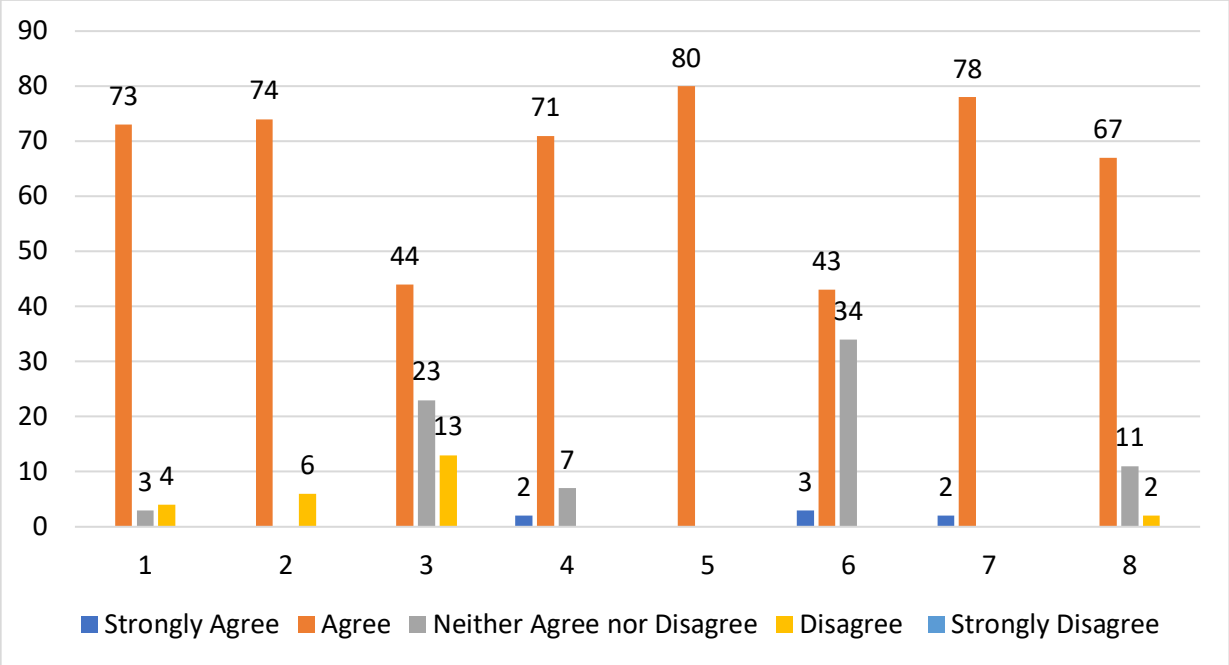
Nigerian banks are facing many difficulties in managing appropriate responses to cyber security threats when these occur. All of our participants (N = 80) agreed or strongly agreed that i) there was 'inadequate cyber security awareness' among participants to effectively detect these threats; and ii) there was 'inadequate investment in cyber security' in this aspect (see: Figure 6). 95% (76) of the participants agreed that the penalties charged for offenders of cyber threats were also inadequate. 52.5% (42) of them agreed that there are 'inadequate skills/knowledge in managing cyber security breaches'. However, ironically none agreed or strongly agreed that there was 'inadequate management support'. In fact, 86.3% (69) of our participants openly disagreed with this statement.

Figure 6: Key challenges in managing appropriate responses to cyber security threats (N = 80)



In terms of the levels of confidence in their banks' readiness to deal with specific cyber security breaches and their related issues, most of our participants expressed varying levels of confidence (see: Figure 7). However, fewer expressed their confidence in the banks' ability to 'detect anomalous activities and to complying with the state data breach regulations'. This suggests in turn that if correct measures are put in place, cyber security breaches in the Nigerian banking industry could be significantly reduced.

Figure 7: Readiness to deal with potential cyber security breaches (N = 80)



1	Detecting malicious insider activity/threat
2	Detecting hijacking of privileged users' credentials by a hacker
3	Detecting anomalous or abnormal activities
4	Receiving latest intelligence on emerging cyber threats
5	Detecting malware (malicious software intended to damage the banking systems)
6	Complying with state data breach regulations
7	Notifying customer and law enforcement when breaches of security occur
8	Blocking DoS attacks, which cause a denial of service for the bank customers

5. Discussion

5.1. Cyber security breaches facing the Nigerian banking industry

Overall, just about all types of breaches have been experienced in the Nigerian banking industry. Cyber-dependent crimes, such as virus, worm or Trojan infections (80%) and hacking (65%) are

among the most commonly experienced cyber security breaches (see: Figure 1). At the same time, cyber-enabled crimes that are traditionally associated with Nigerian criminals, such as Phishing (13.75%), online fraud (23.75%) and fake-cat websites (28.70%) are experienced at much lower rates.

This finding coincides with current research highlighting a transformation of the Nigerian cybercrime industry from low-tech cyber-enabled crimes (e.g., fraud) to high-tech sophisticated and organised attacks (e.g., hacking) (Hinchliffe, 2017). It is not therefore a surprise, following this that the banking industry is experiencing this transformational wave as it is where the money is; and Nigerian criminals are, of course, primarily motivated by financial incentives (Ibrahim, 2016).

Cyber-dependent breaches, such as virus, worm or Trojan infections and hacking, could be more prevalent than cyber-enabled breaches, for two main reason. These are i) force amplification and ii) entry barrier. Force amplification refers to the use of digital technologies to enable a criminal to interact with potential victims on a global basis (e.g., phishing). Entry barriers indicate that a significant feature of all technologies is their power to reduce the entry barrier for people to commit crime (e.g., copyright theft through digital replication of any copyright protected information) (Hargreaves and Prince, 2013). The more dominant a role digital technologies play in a crime, the more the impact of the crime is amplified. Moreover, at the same time, the entry requirement to this crime becomes easier. The level of cyber-dependent or techno-centric breaches in the Nigerian banking sector is also indicative of a more technologically advanced cybercrime industry in Nigeria. This might be related to the rapid growth in technology and its tech-savvy younger

population (Ojedokun and Eraye, 2012; Williams, 2018). The ease of entry to crime may also explain the prevalence of electronic spam mails (73.75%) (see: Figure 1).

The Nigerian banking industry may have a greater awareness of traditional cyber-enabled crimes, such as fraud, fake-cat websites, and identity theft. Yet, it may be still trying to catch up with some of the more technologically advanced breaches. It is easy, in general, for a criminal to infiltrate another user's computers using viruses, worms, or Trojan infections. This is because most people rarely have effective digital defensive systems, such as updated antivirus software (Internet Society Organization, 2016). Moreover, developing countries are now becoming ideal testing grounds for cyber attackers – hackers appear to be testing their skills in English-speaking African countries (Frenkel, 2017). Another possibility could be that the rapidly growing Nigerian economy is now attracting high-tech criminals from other countries. The National Information Technology Development Agency (NITDA), for example, has raised an alarm over potential cyber-attacks that target the Nigerian banking industry (Mohammed, 2018). Elsewhere, the Kaspersky report, on a group of North Korean hackers, has discovered them attacking large banks across 18 different countries, including Nigeria, even though the Central Bank of Nigeria remains unware of this (Olawoyin, 2017).

In terms of impacts resulting from these breaches, loss of revenues (100%) is the most significant. This is followed by brand erosion and reputational damage (97.5%) (see: Figure 2). These findings are, in fact, supported by a number of studies. Two previous investigations (Oates, 2001; Raghavan and Parthiban, 2014), for example, reported that a significant amount of money was syphoned through account takeover or wire transfer, and this has increased concerns about the safety and

reliability of financial institutions. Account takeover has indeed grown significantly. According to Javelin Strategy and Research (2018), losses from account takeover in 2017 tripled over the past year, reaching $5.1 billion. The loss of customers (95%) and competitive advantage (90%) are relatively low. This could be related to the fact that most of the banks suffer from cyber security breaches in Nigeria. In Nigeria, financial institutions and their related firms lose up to 127 billion Nigerian Naira to cybercrime annually (Okafor, 2017) as mobile banking has become the new target of West African cyber criminals (Vanguard, 2017).

Nigeria is the 1st country to legally define Cybercrime in its Cybercrime Act 2015 (Okoh & Chukwueke, 2016). It has also specified duties on its financial institutions, including verifying their customers' identities; tracking and keeping data on their customers; and reporting of all attacks or disruptions to the Computer Emergency Response Team (CERT). 83% (67 out of 80) of our participants reported having regulatory sanctions as an impact of cyber security breaches. 12.5% (10) of them were unsure about this questions and a further 4% (3) of them disagreed with its being an impact (see: Figure 2). Based on our findings, the Cybercrime Act 2015 has not had its full effect in protecting Nigerian industries, including the banking industry. This is substantiated by the fact that this Act failed to criminalise basic hackings or unauthorised access in a comprehensive manner (Omotubora, 2016). Another aspect which needs to be considered is that enacting an Act and enforcing one, are very different matters. Regardless of the innate shortcomings within the Cybercrime Act 2015, it is worth asking whether the Nigerian authorities are capable of implementing and enforcing this Act (Eboibi, 2017).

5.2. Cyber security practices employed in the Nigerian banking industry

Cyber security practices, based on our findings, are given appropriate management support in addressing cyber security issues. There is also adequate training of banking personal in the Nigerian banking industry (see: Figure 4). Over 60% of the participants' banks now prioritise cyber security issues. However, despite this, the levels of intrusion continue to soar. This is because the banks may be struggling to stay up to date with the latest technological advances. Just over 40% of our participants, in fact, thought their banks were technologically up to date (see: Figure 4). Current security practices in the Nigerian banking industry are no longer adequate to combat the increasingly sophisticated cyber-dependent breaches.

Almost 40% of the banks in this sample, more importantly, do not prioritise cyber security issues. Furthermore, there could still be a general lack of awareness of cyber security related issues in the Nigerian banking industry, particularly in relation to responding to security breaches. Over 40% (33 out of 80) of our participants, for example, considered the response duration to a cyber security breach neither increased nor decreased reputational damage. A further 33% were unsure about this (see: Figure 3). 5 out of the 80 professionals did not disagree that quicker responses to cyber security breaches reduced the impact of reputational damage. Over 25% of the participants did not think reputational damage/brand erosion increased the loss of customers; while almost 20% of them did not think reputational damage/brand erosion resulted in the loss of competitive advantage (see: Figure 3). These results contrasted with the literature on the relationship between breach responses and reputational damage. Previous research indicated that responding appropriately to a breach had a significant impact on mitigating reputational damage, and vice versa (e.g., Brown, 2016; Goldberg, 2013). In 2011, Sony's poor response, for example, to its security breach tarnished

its corporate image (The Guardian, 2011) and the corporation was subsequently sued by its insurance firm (Goldberg, 2013).

The prevention of cyber security breaches requires not only the commitment of the banking industry but also their service users (Idowu, 2016; Olayemi, 2014). According to Idowu (2016), educating the public on various forms of cyber threats and how to identify these can significantly reduce the amount of cyber security breaches encountered by bank customers. Our findings indicate that the majority of our participants (95%) considered simple customer practices as the most effective ways of preventing cyber security breaches. These include not sharing personal account details and subscribing to transaction alerts (see: Figure 5).

5.3. Cyber security capability of the Nigerian banking industry

Banking institutions, when faced with cyber security threats, may fall into organisational crisis which can threaten the stability of financial markets. Thus, an unpredictable situation or a significant threat can have adverse impacts on the organisation, the stakeholders or the industry if not addressed properly (Johnson, 2015; Miller, 2009). Despite all the technological interventions that a bank could put in place to fight cyber security threats, technology alone is, of itself, not enough to protect the bank (Arachchilage and Love, 2014). Thus, security practices also must include conventional, technological and behavioural interventions (Wada and Odulaja, 2012).

Our findings on the key challenges facing the Nigerian banking industry suggest the need for a holistic approach. Here both socio-technical (Kayworth and Whitten, 2010; Safa et al., 2015) and socio-legal measures (Gerber and Von Solms, 2008), to strengthen its security capability are

needed. Yet inadequate penalties for offenders of cyber security breaches (97.5% agreed) and inadequate cyber security awareness (85% agreed) are likely to be the most severe challenges facing the Nigeria banking industry (see: Figure 6).

The weak implementation of the Cybercrime Act 2015 and inadequately equipped law enforcement agencies are, in fact, the key contributing factors to high cybercrime rate in Nigeria. According to Hassan et al. (2012), cyber criminals have regularly exploited the existing gaps in penal proceedings to conduct their illegal activities. Moreover, the nation lacks some of the sophisticated technical equipment required to track cyber criminals and to deliver them to justice. In support of this, Dada et al. (2013) argued that African countries have failed to deal adequately with cases of cybercrime because their law enforcement agencies, as far as intelligence, infrastructure and personnel are concerned, are insufficiently equipped. Our findings also show that the level of legislative compliance is quite unsatisfactory in the banks. Just less than 55% (53.75%; 43 out of 80) of our participants agreed that their banks comply with state data breach regulations.

In terms of technological capability, it appears that the Nigerian banking industry is able to exercise a range of essential preventative measures with sufficient management support, such as ensuring that computers and servers were installed with updated anti-virus software (see: Figure 3). When it comes to staying up to date with technological advancements (42.5%), however, the banks appear to be unable to keep up (see: Figure 3). These findings are consistent with our other findings on the readiness of the banks to deal with potential cyber security breaches (see: Figure 7). The banks are able to detect some obvious intrusions, such as malware (100%), malicious insider

activity/threat (91.25%), and hijacking of privileged users' credentials by a hacker (92.5%) (see: Figure 7). However, the banks' readiness to detect anomalous or abnormal activities (55%) in general is significantly lower (see: Figure 7). This is, perhaps, because the detection of abnormal activities requires more advanced behavioural analytics software based on Artificial Intelligence (Rehman and Saba, 2014) and Machine Learning (Ji et al., 2016). Their readiness to block Denial of Service (DoS) attacks (83.75%) is lower than their general readiness to detect (see: Figure 7). This may explain the high levels of breach experienced by the banks (see: Figure 1). There appears to be a gap between their ability to detect intrusions and their ability to deal with these. Detecting and responding to threats are, however, very different, and also require different technologies and approaches. In this respect, when it comes to managing risks and threats, it is of real importance to seek to reduce the time between breach detection and breach response (Brewer, 2015).

6. Conclusion

In conclusion, our findings suggest a high level of cyber security breaches in the Nigerian banking industry. More banks suffer, in general, from cyber-dependent breaches, such as virus, worms, and Trojan infections, and hacking, than cyber-enabled breaches. Of course, some cyber-enabled breaches, e.g., electronic spam mail, continue to rise at a high rate. Other types of cyber-enabled breaches are, however, experienced less by banks in this sample. Cyber security breaches targeting Nigerian banks are becoming more technologically sophisticated. In sharp contrast, while the banks are trying to protect themselves and their customers, their current security practices are no longer adequate to combat the increasingly sophisticated cyber-dependent breaches that they experience. There is, in particular, a significant lack of advanced technologies to prevent cyber security threats, and also to respond to cyber security breaches after these have been detected.

Moreover, although Nigeria has the 1st legislation against cybercrime globally, both its effectiveness and compliance levels remain low. More positively, there also appear to be adequate management support and training in cyber security issues and related concerns. However, both management support and training need to be updated on a regular basis and to be of a higher technical order to effectively combat the growth of cyber dependent breaches now confronting the Nigeria internet banking industry.

Cyber security breach remains one of the biggest security risks in the banking industry of most developing countries (The Nerve, 2016). Although small-scale, this research is of value as it provides some insights into the current state-of-the-art of cyber security breaches, practices and capability of the Nigeria internet banking industry. As argued in the earlier methods section, this is an initial exploratory exercise in an area with a very limited published literature. Further exploration of our research questions will require a mixed-method methodology, with both a larger survey research base and qualitative face-to-face interviews. It would also provide room for data triangulation, therefore generating results that are both more reliable and generalisable.

References

Agboola, A. A., 2006. Electronic Payment Systems and Tele-banking Services in Nigeria. Journal of Internet Banking and Commerce. 11 (3), 1-7.

Ahmad, M.K.A., Rosalim, R.V., Beng, L.Y., Fun, T.S., 2010. Security issues on banking systems. International Journal of Computer Science and Information Technologies. 1 (4), 268-272.

Akanbi, P.A., Ayodele, T.D., Adedipe, O.A., 2014. An Investigation into Some Factors Influencing the Intention to Use Internet Banking among Undergraduates in Nigeria. Research Journal of Finance and Accounting. 5, 1-9.

Akanle, O., Adesina, J.O., Akarah, E.P., 2016. Towards human dignity and the internet: The cybercrime (yahoo yahoo) phenomenon in Nigeria. African Journal of Science, Technology, Innovation and Development. 8 (2), 213-220.

Akwaja, C., 2014. Nigeria: Banks lose N159 Billion to Cyber Crime. Retrieved from https://allafrica.com/stories/201406230436.html.

Arachchilage, N.A.G., Love, S., 2014. Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior. 38, 304-312.

Arewa, A., 2018. Borderless crimes and digital forensic: Nigerian perspectives. Journal of Financial Crime. 25 (2), 619-631.

Asokhia, M.O., 2010. Enhancing national development and growth through combating cybercrime/Internet fraud: a comparative approach. Journal of Social Sciences. 23 (1), 13-19.

Auta, E.M., 2010. E-Banking in developing economy: empirical evidence from Nigeria. Journal of Quantitative Methods to e-Commerce. 5(2), 212-222.

Bossler, A.M., Holt, T.J., 2009. Online activities, guardianship, and malware infection: An examination of routine activities theory. International Journal of Cyber Criminology. 3 (1), 400-420.

Brewer, R., 2015. Cyber threats: reducing the time to detection and response. Network Security. 2015 (5), 5-8.

Brinkmann, S., 2014. Interview. In: Teo, T. (Ed.), Encyclopedia of Critical Psychology. Springer, New York., pp. 1008-1010.

Brody, R.G., Mulig, E., Kimball, V., 2007. Phishing, pharming and identity theft. Academy of Accounting and Financial Studies Journal. 11 (3), 43-56.

Brown, H. S., 2016. After the data breach: Managing the crisis and mitigating the impact. Journal of business continuity & emergency planning. 9 (4), 317-328.

Central Bank of Nigeria (CBN), 2003. Guidelines on Electronic Banking in Nigeria. Retrieved from https://www.arca.network/lib/E-BANKING-Regulation-document.pdf.

Chiemeke, S. C., Evwiekpaefe, A., Chete, F., 2006. The Adoption of Internet Banking in Nigeria: An Empirical Investigation. Journal of Internet Banking and Commerce. 11 (3), 1-10.

Dada, S.O., Owolabi, S.A., Okwu, A.T., 2013. Forensic accounting a panacea to alleviation of fraudulent practices in Nigeria. International Journal of Business Management and Economic Research. 4 (5), 787-792.

Deloitte, 2017. 2018 banking outlook. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-dcfs-2018-banking-outlook.pdf.

Doyon-Martin, J., 2015. Cybercrime in West Africa as a result of transboundary e-waste. Journal of Applied Security Research. 10 (2), 207-220.

Dunkley, E., 2017, March, 13. A tale of two cyber bank heists that reveals their vulnerability. Financial Times. Retrieved from https://www.ft.com/content/2bc83132-ee18-11e6-ba01-119a44939bb6?mhq5j=e3.

Ebenezer, A. J., Paula, A. M., Allo, T., 2016. Risk and Investment Decision Making in the Technological Age: A Dialysis of Cyber Fraud Complication in Nigeria. International Journal of Cyber Criminology. 10 (1), 62-78.

Eboibi, F. E., 2017. A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015. Computer Law & Security Review. 33 (5), 700-717.

Ehimen, O.R., Bola, A., 2010. Cybercrime in Nigeria. Business Intelligence Journal. 3 (1), 93-98.

FBI, 2011. Taking a Trip to the ATM? Retrieved from https://www.fbi.gov/news/stories/atm-skimming.

Frenkel, S., 2017, July, 2. Hackers find 'ideal testing ground' for attacks: developing countries. New York Times. Retrieved from https://www.nytimes.com/2017/07/02/technology/hackers-find-ideal-testing-ground-for-attacks-developing-countries.html.

Gerber, M., Von Solms, R. 2008. Information security requirements–interpreting the legal aspects. Computers & Security. 27 (5-6), 124-135.

Global Risks Report, 2015. Global Risks Report. World Economic Forum. Retrieved from https://www.ey.com/Publication/vwLUAssets/EY-cyber-breach-response-management/$FILE/EY-cyber-breach-response-management.pdf.

Goldberg, E., 2013. Preventing a data breach from becoming a disaster. Journal of business continuity & emergency planning. 6 (4), 295-303.

Hassan, A.B., Lass, F.D., Makinde, J., 2012. Cybercrime in Nigeria: Causes, effects and the way out. ARPN Journal of Science and Technology. 2 (7), 626-631.

Hargreaves, C., Prince, D. (2013), Understanding Cyber Criminals and Measuring Their Future Activities. Lancaster University. Retrieved from http://eprints.lancs.ac.uk/65477/1/Final_version_Understanding_cyber_criminals_and_measuring_their_activity.pdf.

Hinchliffe, A., 2017. Nigerian princes to kings of malware: the next evolution in Nigerian cybercrime. Computer Fraud & Security. 2017 (5), 5-9.

Ibrahim, S., 2016. Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. International Journal of Law, Crime and Justice. 47, 44-57.

Idowu, O.A., 2016. Cyber Fraud in the Commercial Banks among the Public in Ibadan Metropolis, Oyo State Nigeria. International Journal of Social Sciences. 10 (3), 160-176.

Internet society, 2016. Global Internet Report 2016. Retrieved from https://www.internetsociety.org/globalinternetreport/2016/.

Internet World Stats, 2018a. Internet Penetration in Africa – December 31, 2017. Retrieved from https://www.internetworldstats.com/stats1.htm.

Internet World Stats, 2018b. Top 20 countries with the highest number of Internet uses – December 31, 2017. Retrieved from https://www.internetworldstats.com/top20.htm.

Javelin Strategy and Research, 2018. Identity fraud hits all time high with 16.7 million U.S. victims in 2017. Retrieved from https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.

Ji, S. Y., Jeong, B. K., Choi, S., Jeong, D. H. 2016. A multi-level intrusion detection method for abnormal network behaviors. Journal of Network and Computer Applications. 62, 9-17.

Johnson, K. N., 2015. Cyber risks: Emerging risk management concerns for financial institutions. Georgia Law Review. 50, 131-142.

Juniper Research, 2018. Digital banking users to reach 2 billion this year, representing nearly 40% of global adult population (Press releases). Retrieved from https://www.juniperresearch.com/press/press-releases/digital-banking-users-to-reach-2-billion.

Kayworth, T., Whitten, D. 2010. Effective information security requires a balance of social and technology factors. MIS Quarterly Executive. 9 (3), 163-175.

KPMG, 2017. How can Nigerian banks start to improve internet banking penetration? Retrieved from https://home.kpmg.com/ng/en/home/insights/2017/11/how-can-nigerian-banks-start-to-improve-internet-banking-penetra.html.

Lagazio, M., Sherif, N., Cushman, M., 2014. A multi-level approach to understanding the impact of cybercrime on the financial sector. Computers & Security. 45, 58-74.

Lavorgna, A., Sergi, A., 2014. Types of organised crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of Internet technologies. International Journal of Law, Crime and Justice. 42 (1), 16-32.

Martins, C., Oliveira, T., Popovič, A., 2014. Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. International Journal of Information Management. 34 (1), 1-13.

Miller, K., 2009. Organizational Communication; Approaches and Processes. Wadsworth Cengage Learning, Boston.

Mohammed, Z., 2018. NITDA Raises Alarm Over Potential Cyber Attacks To Banks, Govt Agencies, Others. Retrieved from https://www.nigerianews.net/nitda-raises-alarm-potential-cyber-attacks-banks-govt-agencies/.

Nhan, J., Bachmann, M., 2010. Developments in cyber criminology. In: Maguire, M., Okada, D. (Eds.), Critical issues in crime and justice: Thought, policy, and practice. Sage, London, pp. 164-183.

Oates, B. 2001. Cyber crime: How technology makes it easy and what to do about it. Information Systems Security. 9:6, 1-6.

Odunfa, A., 2014, Nigeria: Report on Cyber Threat Calls for Quick Passage of 2012 Bill. Retrieved from http://www.allafrica.com/ stories/201405080279.Html.

Ojedokun, U. A., Eraye, M. C. 2012. Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. International Journal of Cyber Criminology. 6 (2), 1001-1013.

Ojeka S.A., Ben-Caleb E., Ekpe, E-O.I., 2017. Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. International Review of Management and Marketing. 7 (2), 340-346.

Okafor, C., 2017. Oracle: Nigerian banks, others lose N127bn annually to cybercrime. Oracle. Retrieved from https://www.thisdaylive.com/index.php/2017/05/14/oracle-nigerian-banks-others-lose-n127bn-annually-to-cybercrime/.

Okamgba, J., 2017. Online Fraud Drains Nigeria Over N500 billion in 7 years. Retrieved from https://cfatech.ng/online-fraud-drains-nigeria-over-n500-billion-in-7-years/

Okoh, J., Chukwueke, E.D., 2016. The Nigerian Cybercrime Act 2015 and its implication for financial institutions and service providers. Financier Worldwide. Retrieved from

https://www.financierworldwide.com/the-nigerian-cybercrime-act-2015-and-its-implications-for-financial-institutions-and-service-providers#.XKylU5hKiUk.

Olawoyin, O., 2017. North Korean hackers attack banks in Nigeria, 17 other countries – Kaspersky. Premium Times. Retrieved from https://www.premiumtimesng.com/news/top-news/228166-north-korean-hackers-attack-banks-in-nigeria-17-other-countries-kaspersky.html.

Olasanmi, O.O., 2010. Computer crimes and counter measures in the Nigerian banking sector. Journal of Internet Banking and Commerce. 15 (1), 1-10.

Olayemi, O.J., 2014. A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology. 6 (3), 116-125.

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M, Esan, A. O. 2016. Cybercrimes in Nigeria: Analysis, Detection and Prevention. FUOYE Journal of Engineering and Technology. 1(1), 37-42.

Omotubora, A. O., 2016. Comparative perspectives on cybercrime legislation in Nigeria and the UK-a case for revisiting the" hacking" offences under the Nigerian Cybercrime Act 2015. European Journal of Law and Technology. 7 (3), 1-15.

Oni, A.A., Ayo, C.K., 2010. An empirical investigation of the level of users' acceptance of e-banking in Nigeria. Journal of Internet Banking and Commerce. 15, 1-13.

Oruç, Ö.E., Tatar, Ç., 2017. An investigation of factors that affect internet banking usage based on structural equation modelling. Computers in Human Behavior. 66, 232-235.

Osho, O., Onoja, A.D., 2015. National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. International Journal of Cyber Criminology. 9 (1), 120-143.

Pennathur, A.K., 2001. “Clicks and bricks”: e-Risk Management for banks in the age of the Internet. Journal of banking & finance. 25(11), 2103-2123.

Ponemon Institute, 2017. The impact of data breaches on reputation & share value. Retrieved from https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf.

Raghavan, A.R., Parthiban, L., 2014. The effect of cybercrime on a Bank’s finances. International Journal of Current Research & Academic Review. 2 (2), 173-178.

Rayman, N. 2014. The world’s top 5 cybercrime hotspots. Retrieved from http://time.com/3087768/the-worlds-5-cybercrime-hotspots/.

Rawashdeh, A., 2015. Factors affecting adoption of internet banking in Jordan: Chartered accountant’s perspective. International Journal of Bank Marketing. 33 (4), 510-529.

Rehman, A., Saba, T. 2014. Evaluation of artificial intelligent techniques to secure information in enterprises. Artificial Intelligence Review. 42 (4), 1029-1044.

Reportlinker, 2017. Global Online Banking Industry – Forecast. Retrieved from https://www.reportlinker.com/d0114191199/Global-Online-Banking-Industry-Forecast.html?pos=1

Reyes, A., Brittson, R., O'Shea, K., Steele, J., 2011. Cyber-crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors. Syngress, Rockland, MA.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., Herawan, T. 2015. Information security conscious care behaviour formation in organizations. Computers & Security. 53, 65-78.

Schaffer, P., 2018, March, 20. The cost of a cybersecurity breach for financial institutions. ITSP Magazine. Retrieved from https://www.itspmagazine.com/from-the-newsroom/the-cost-of-a-cybersecurity-breach-for-financial-institutions.

Shiloh, J., Fassassi, A., 2016. Cybercrime in Africa: Facts and figures. Retrieved from https://www.scidev.net/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html.

Stabek, A., Watters, P., Layton, R., 2010. The seven scam types: mapping the terrain of cybercrime. In Cybercrime and Trustworthy Computing Workshop (CTC), 2010 Second Cybercrime and Trustworthy Computing Workshop (pp. 41-51). IEEE.

Statistica, 2018. Percentage of population using the internet in Nigeria from 2000 to 2016. Retrieved from https://www.statista.com/statistics/643755/nigeria-internet-penetration/

Tade, O., 2013. A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon. Human Affairs. 23 (4), 689-705.

Tarhini, A., Mgbemena, C., Trab, M.S.A., Masa'deh, R., 2015. User adoption of online banking in Nigeria: A qualitative study. The Journal of Internet Banking and Commerce. 20 (3).

Taylor, S.J., Bogdan, R., DeVault, M., 2015. Introduction to qualitative research methods: A guidebook and resource. John Wiley & Sons, New Jersey.

Taylor, R.W., Fritsch, E.J., Liederbach, J., 2014. Digital crime and digital terrorism, third ed. Prentice Hall Press, New Jersey.

The Guardian, 2011, May, 1. Sony bosses apologise over theft of data from PlayStation Network. Retrieved from https://www.theguardian.com/technology/2011/may/01/sony-playstation-data-security

The Nerve, 2016. Nigeria financial service industry affected most by cybercrime - Cisco. Retrieved from http://thenerveafrica.com/9310/cisco-says-nigeria-financial-services-industry-one-affected-cybercrime/.

Udo, G.J., Bagchi, K.K., Kirs, P.J., 2012. Exploring the role of espoused values on e-service adoption: A comparative analysis of the US and Nigerian users. Computers in Human Behavior. 28, 1768-1781.

UN, 2017. World Population Prospects 2017. Retrieved from https://esa.un.org/unpd/wpp/.

United Nations Office on Drugs and Crime, 2011. West Africa takes lead in fighting 419 scams: First regional even on combating cybercrime held in Nigeria. Retrieved from http://www.unodc.org/nigeria/en/1st-west-africa-cybercrime-summit.html.

Vanguard, 2017. Cybercrime: Mobile banking, target of cyber criminals. Vanguard. Retrieved from https://www.vanguardngr.com/2017/10/cybercrime-mobile-banking-target-cyber-criminals/.

Wada, F., Odulaja, G.O., 2012. Assessing Cyber Crime and its Impact on E-Banking in Nigeria Using Social Theories. African Journal of Computing and ICT. 4 (2), 69-82.

Williams, S., 2018. Mini Docu: Nigerian children are more tech savvy than you think they are, but… . Techcity. Retrieved from https://www.techcityng.com/mini-docu-nigerian-children-are-more-tech-savvy-than-you-think-they-are-but/.

World Bank, n.d. World Bank national accounts data. Retrieved from https://data.worldbank.org/indicator/NY.GDP.MKTP.CD

Zylberberg, H., Klimburg, A., 2015. Capacity Building: Developing Access. Norwegian Institute of International Affairs. Retrieved from

https://brage.bibsys.no/xmlui/bitstream/handle/11250/301986/NUPI_Report_6_15.pdf?sequence=3