Defeating the 21st century demon “Cybercrime” on corporate bodies in Nigeria: Is security intelligence a weapon? A quantitative study [version 1; peer review: awaiting peer review]

Muyiwa B. Afolabi, Gbolahan Ayodamola Raji

Department of Intelligence and Security Studies, Afe Babalola University, Ado - Ekiti, P.M.B 5454, Ekiti, 360001, Nigeria

Abstract
Background: This paper unveils the role of security intelligence in facilitating the war against cybercrime in organizations. It introduces the term cybercrime and security intelligence with financial organizations in Nigeria. Since the invention of information and communication technology in Nigeria, citizens have become fascinated and engrossed. Unfortunately, this opened the door for people with malicious intent to attack individuals, organizations, and nations. Thus, this paper examines the problem of information vulnerability, identifies the level of cybercrime in financial entities, establishes the type of cybercrime, and assesses security intelligence awareness among staff and customers. Methods: The paper employed the simple-random sampling technique, using a primary and secondary source of information, analyzing frequency counts, percentages, and charts for the demographic variables, and used chi-square through SPSS data processing. Results: The results state the ubiquity of cybercrime among financial organizations and reveals that phishing scams, website spoofing, piracy, ransomware, and hacking are the top cyber-crime types commonly used. Conclusions: Thus, the administration of security intelligence can reduce internal and external threats in an organization. Furthermore, the paper states that security intelligence intervention is independent of the nature of cybercrime across the organization. However, the paper recommends that organizations need to enlighten their staff and customers with measures to safeguard information against cybercrime with the usage of security intelligence techniques and other proactive measures.

Keywords
Intelligence, Threat, Crime, Security Intelligence, Cybercrime, Information Security, Corporate Entity.
Introduction

Information trade has spread and become more productive using recent innovative advances all over the planet, such as texting and online entertainment stages. Therefore, access to information has become easier (Jeff, 2020). As innovation keeps on advancing, so do the benefits and challenges. As a result of the rapid spread of this innovation among people, the electronic interchanges have become the main mode of working both small- and large-scale businesses. This has created dangers and vulnerability due to dependence on this innovation (Said & Noha, 2019). As a general public that runs to a great extent on innovation, people and associations are likewise too dependent on it and, similarly, as innovation brings ever more noteworthy advantages, it also creates risks and opens up a space for cybercrime, modern undercover work, and digital assaults. Subsequently, safeguarding this has become a principal need (Anthony, 2016).

As indicated by Artur (2015), there have been reports that evaluate the causes, elements, and impacts of digital dangers. In this manner, the multiplication of reports is a significant indication of the rising conspicuousness of digital assaults among private and public establishments including citizens across the globe. Cybercrime is an essential illustration of transnational crime. PC networks interface with all nations of the world, and cyber criminals can damage anywhere on the planet from their home. The potential risk for an individual is when he visits an unsecured website and becomes susceptible to viruses. In a company, the internal network can be hacked and inaccessible for 24 hours or trade secrets being stolen, while in governmental bodies the public websites can be blocked or state papers published on the web (Koops & Brenner, 2006). The most unmistakable type of cybercrime is identity fraud, in which lawbreakers utilize the Internet to take individual data from different clients. The most complete meaning of cybercrime is a criminal activity involving an information technology infrastructure, including unlawful access, information obstruction, frameworks impedance, abuse of gadgets, phony (ID theft), and electronic fraud (Adebayo, 2017).

Cybercrime attacks are significant threats to financial business and corporate entities in Nigeria and across the globe. Thus, corporate and financial entities like Leadway Assurance Nigeria and Bode Ogunleye & Associates, etc., with over five decades of operations, have a Cyber-risks insurance policy for preventing cyber-attacks (Businessday, 2021). However, the policy is designed by a team highly experienced in cyber-security breaches. Thus, due to the veracity of cybercrime, new methods are needed to help prevent future financial loss in the event of an incidence (Raji, 2022).

In any case, new sorts of cybercrime dangers that normally bring about information misfortune and data abuse have arisen at the same time. Consequently, keeping up with information security in complex frameworks is significant and important, especially in associations where there is a greater number of people that are cooperating with the web. Hence, Security intelligence looks into information vulnerability and how to defend an organization from internal and external threats as well as the procedures or tools designed to gather and analyze that information to aid policymakers in the organization.

Problem statement

In the US, in January 2003, cybercriminals launched an attack on a nuclear power plant which caused its shut down. The attack by the cybercriminals happened using a Slammer worm. In 2010, the Stuxnet worm was able to attack thousands of networks, according to security firm Symantec. It also targeted the Bushehr nuclear power plant in Iran (Said & Noha, 2019).

Cyber-attacks are costly and can result in various problems such as financial loss, reputation damage, and psychological distress. They can also affect individuals’ social connections and organizational devices. The cost of maintaining and protecting an organization’s networks and systems can vary depending on the nature of the attack. For instance, a successful penetration can lead to the loss of a customer’s existing account or new customers (Said & Noha, 2019).

Nigeria’s cybercrime experiences have become one of the most common avenues for money laundering and corporate spying. According to a report published by the World Economic Forum, more businesses are doing business online than ever before (Umaru, 2017). In other words, financial services, e-commerce, insurance, airlines, media, oil and gas, and education are all affected by cybercrime (Omodunbi, Odiase, Olaniyan & Esan, 2016). However, within Nigerian corporate entities, vulnerability is a problem. Factors like corruption, lack of standards in national central control, a lack of infrastructure, a lack of national functional databases, Domestic and international law enforcement, the proliferation of cybercafés, unemployment, and poverty are issues of vulnerability. Additionally, the porous nature of the Internet is the element that has made individuals, organizations, and citizens in Nigeria so vulnerable to cybercrime (Adebayo, 2017).
Organizations have to be dedicated to protecting their assets and the information of their consumers. In light of the aforementioned issues, the problem statement for this paper is to consider cybercrime as follows: Theft on cooperative bodies looking at information vulnerability, such as personal and financial information among employees and consumers, as well as a managerial role in policy formulation for proactive safeguards in a financial organization.

Objectives
The paper aims to assess cybercrime attacks on corporate entities, while the objective of the paper is to assess cybercrime in financial institutions. The specific objectives are to:

i. Examine the level of cybercrime in financial institutions in Nigeria.

ii. Establish the nature of cybercrime attacks on financial institutions in Nigeria.

iii. Assess security intelligence awareness among staff and customers of financial institutions in Nigeria.

Conceptual framework
Cybercrime
A crime in which a computer is the object of the crime (hacking, phishing, spamming) or is utilized as a tool to conduct an offense. Child pornography and hate crimes are classified as cybercrimes (Giuseppe, Damian & Wille, 2021). According to the EU Cyber Security Strategy 2013, “cybercrime refers to a wide range of illegal activities in which computers and information systems are used as a significant tool or as a primary target. “Other equivalent phrases, such as ‘virtual crime,’ ‘net-crime,’ ‘hi-tech crime,’ or ‘computer crime/e-crimes,’ are also frequently used to include a spectrum of illegal actions that involve information and communication technology “ICT” in nature (Wall, 2004). The lack of clarity can be perplexing and alarming, and some people have taken to labeling any violation involving a computer or portion of one as a cybercrime (Wall, 2004).

Categories of cybercrime
Traditional offenses (such as fraud, forgery, and identity theft), content-related offenses (such as online distribution of child pornography or incitement to racial hatred), and offenses specific to information systems and computers all fall under the umbrella of internet crime. E-crimes are indeed a new fashion fad, steadily gaining pace as the web keeps on infiltrating each area of our general public, and nobody can foresee the future. Cybercrime can be divided into two general categories:

i. Crimes that directly harm computer networks and gadgets. Computer viruses, malicious code, and malware are a few examples.

ii. Criminality perpetrated with PC or gadgets, the essential objective of which is autonomous of the PC or gadgets. The following are digital crime models: Misrepresentation and wholesale fraud, phishing tricks, and data fighting (Omodunbi, Odiase, Olaniyan & Esan, 2016).

Cyber-crime is classified as follows by Charles, Zacchaeus, and Fashina (2006): Financial crimes that cause a company’s ability to perform e-commerce to be disrupted (or electronic commerce). The act of duplicating copyrighted material is known as piracy. Hacking is the process of gaining unauthorized access to a computer system or network and, in certain cases, abusing that access. Cyber-terrorism is the result of hacking attacks meant to cause terror. Financial crimes (forgery, theft, industrial espionage, sabotage and extortion, product piracy, and so on) intrusions of privacy, the spread of illegal and harmful information, the promotion of prostitution and other moral crimes, and organized crime are all examples of cybercrime. Cybercrime crosses the line into terrorism at its most serious levels, covering attacks on human life, national security establishments, key infrastructure, and other vital arteries of society.

In general, there are three forms of cybercrime attacks. They are:

a) Crime against the Individual: (a) Person (b) Property of an individual.

b) Crime against Organization: (a) Government (b) Firm, Company, and Group of Individuals.

c) Crime against Society.
Cybercrime on corporate bodies

According to Omodunbi, Odiase, Olaniyan, and Esan (2016), the internet’s contribution to Nigeria’s development has had a favorable impact on different sectors of the country. However, these industries, such as banking, e-commerce, and education, are all affected by cybercrime. Cybercrime is on the rise at an alarming rate, with cases becoming more sophisticated. As a result, the focus of this research will be on the specific methods in which cybercrime is perpetrated in Nigeria, particularly in the e-commerce and banking industries.

Thus, according to Omodunbi, Odiase, Olaniyan, and Esan stated in Michael, Boniface, and Olumide (2014), the Nigerian economy, which includes an immense number of e-businesses, is significantly threatened by the rapid development in e-crime. E-commerce is the purchase, sale, and marketing of goods and services to clients using technology, notably the Internet.

As explained by Ewepu (2016), not very many e-wrongdoings are found in this area on the grounds that most organizations are more concerned with the misfortune from negative exposure than the wrongdoings. Senator Iroegbu estimated the annual cost of cybercrime to Nigeria at 0.08 percent of the country’s GDP or approximately 127 billion Naira. Omodunbi, Odiase, Olaniyan, and Esan also discussed some of the ways E-commerce crimes are committed in Nigeria. These are some examples:

a) Programming Robbery (Theft of Patent Rights): For an average Nigerian, the concept of “Copyright” does not imply anything. Illicit generation and conveyance of programming, games, films/recordings, and sound are alluded to as theft (Omodunbi, Odiase, Olaniyan, and Esan, 2016).

b) Fraudulent sales and Counterfeit: There is no such thing as false deals of items that already exist or are reproduced, which is an act that is becoming more common. Many individuals have been misled by well-known online business sites (Omodunbi, Odiase, Olaniyan, and Esan, 2016).

c) Data and Airtime Theft (DAT): This is an exceptionally normal trick among the present youth. They get “Cheat Codes” illicitly and use them to acquire great many versatile information and limitless broadcast appointment without paying the expected charges. Likewise, cybercafés have created ways of associating with the organization of web access suppliers (Omodunbi, Odiase, Olaniyan, and Esan, 2016).

Scams using Bank Verification Numbers (BVNs), Bank Card Theft, Phishing, and Cyber-theft/Banking Fraud are four different ways cybercrime is carried out in the banking sector, according to Omodunbi, Odiase, Olaniyan, and Esan (2016).

a) Scams involving Bank Verification Numbers (BVNs): BVN is a biometric identification system that uses an 11-digit number as a nationwide identifying number. BVN enabled thieves to steal money and also carry out criminal methods. Several people received wrong and unapproved instant messages and calls requesting personal information such as account information.

b) Phishing is the robbery of one’s personality. This entails taking individual data from clueless clients as well as committing fraud against legitimate, authorized businesses and financial institutions. When people receive regular emails from a website after entering their email address to subscribe for updates, the user becomes accustomed to receiving such emails. Fraudsters have devised a method to order goods by impersonating authorized organizational websites. Hackers can steal users’ credit card information when they enter it into the seller’s Internet website for an online transaction. This information can be retrieved using a variety of applications, for example, key lumberjacks in cybercafés or cloned sites.

c) Digital burglary/Banking Misrepresentation: Criminals take advantage of security flaws in different banking institutions to send funds to multiple domains as well as their own. Hackers send small sums of money, such as 5 Naira, which are frequently ignored by customers who believe the money was taken to pay for SMS or ATM withdrawal fees. The majority of fraudsters profit from doing this for over a million accounts.

Cybercrime in Nigeria

The introduction of these three major inventions, computers, the Internet, and mobile phones, in Nigeria in 1999, resulted in a massive outbreak of cybercrime. Fraudsters utilize the obscurity given by the internet to dupe clueless casualties
According to the Institute of Digital Communication South Africa, software piracy costs Nigeria approximately $80 million per year (Ibikunle & Eweniyi, 2013). According to the National Fraud Information Centre American, the Nigerian financial schemes were the quickest developing web-based trick in 2001, with ninety percent of that growth attributable to an increase in identity theft, internet scoffing, and phishing scam attacks on organizations in Nigeria and around the world.

Sergei Panteleevich Mavrodi, the founder of the MMM Ponzi scheme, expanded his operation in Nigeria in 2016. The percentage offer was high, which enticed many Nigerians to invest; however, accounts were later frozen in December 2016. Igba, Elizabeth, Aja, Simon, Egbe, and Ogodo (2018) noted “Greed is another destructive wind in Nigeria that encourages people to commit criminal acts because many people want to get rich quickly by any means”. Poor parenting has contributed to criminality because some parents have little to offer in terms of strong morals. Poverty affects approximately 71 percent of Nigerian households, with nearly 77 percent of urban and 68 percent of rural families considered poor, and maybe motivated to engage in cybercrime due to a lack of a source of income. The vast majority of undergraduate students are impoverished.

However, peer pressure among the youth, both rich and poor, living in urban or rural areas, motivates them to carry out cybercrime attacks. According to Ebelogu et al. (2019), cybercrimes in Nigeria fall into several categories, including Internet fraud, hacking, software piracy, pornography, credit card or ATM fraud, denial of service attack, virus dissemination, phishing, and cyber plagiarism, cyber-stalking, and cyber-defamation. He went on to say that cyber-attacks on financial institutions are becoming more common, sophisticated, and widespread. Although large-scale denial-of-service attacks against larger financial institutions receive the most attention, community and regional banks, credit unions, money transmitters, and third-party service providers (such as credit and payment processors) have also been targeted in recent years. As per the Proshare (2020) report, the assessed yearly monetary misfortune in Nigeria because of cybercrime was N250 billion in 2017 and N288 billion in 2018, despite the fact that an expected 95% of cybercrime goes undetected.

Security intelligence

Literature on this concept has been written by scholars and authors, with various points of view, perceptions, and definitions. Security intelligence, according to Peter Gill’s broad definition (1994), is the state’s gathering of information in an attempt to counter perceived security threats such as espionage, sabotage, foreign-influenced activities, political violence, and subversion (Kieran & Dennis, 2001).

Security Intelligence is focused on providing actionable and insightful intelligence that can help businesses reduce their risk and operational effort (John, 2011). Through security intelligence, a security manager can develop and implement effective security plans and budgets. The use of security intelligence can help improve the efficiency of the security department by allowing it to make more informed decisions. It can also help the security team respond faster to a threat. Security intelligence is focused on identifying and analyzing a threat before it can be considered for inclusion in a management plan. This process usually involves coming up with a preferred model that takes into account the threat’s goals and capabilities (Clifton & David, 2013).

Mark et al. (2015) emphasized the widespread misunderstanding of security intelligence, pointing out that there is no agreed-upon definition of security intelligence. Thus, Security intelligence is defined by John et al. (2016) as “indirect and directed attacks on an organization.” However, the process of obtaining, evaluating, and disseminating data and information across an organization is often referred to as security intelligence (Jeff, 2020). Security intelligence, according to Awwal and Abiodun (2021), is any plan for effective security that includes the acquisition of timely and accurate intelligence about the target, particularly the organization, as well as individuals that pose a threat to such a target’s tactics and motives.

Sumo (2021) defines the term as the real-time gathering, standardization, and analysis of data created by users, applications, and infrastructure that has an impact on an enterprise’s IT security and risk posture as pertinent, emphasizing the need not only to collect Information Security-related data but also to consistently stay ahead of intruders. Security intelligence was defined in Raji’s dissertation (2022) as a pivot tactic to reduce the risk that fuses external and internal threats, as well as business insights across an entire organization, the process by which data and information are collected, analyzed, and disseminated throughout the organization.

Security intelligence methods

Several technologies have contributed to the evolution of security intelligence. In short, security intelligence expands on log management’s data collection capabilities and compliance benefits, Security information and event management
(SIEM), correlation, normalization, and analysis capabilities, NBAD’s network visibility and advanced threat detection capabilities, risk management’s ability to reduce breaches and ensure compliance, and network traffic’s visibility and advanced threat detection capabilities, as well as network forensics’ application content insight (John, 2011). Gathering security intelligence involves a collection of interconnected actions, technologies, and instruments that work together to achieve the desired outcome. IT firms that collect sensitive data through web apps are subject to stringent regulatory compliance requirements, and security intelligence can assist them in meeting those requirements. However, it is the process of gathering security intelligence that feeds into other downstream Security Operations processes that contribute to the security of the IT infrastructure against cyber-attacks (John et al., 2016). Jeff (2020) highlighted four processes in security intelligence:

i. A collaborative process and framework.
ii. 360-degree visibility.
iii. Extensive automation and integration.
iv. Alignment with the organization and security cases.

Security intelligence provides insight into threats before they occur. Cyber threats come in a variety of shapes and sizes. Some of these are undoubtedly cybercriminals attempting to breach your network via the firewall. This category includes threat actors operating on the open and dark webs, as well as your employees and business partners. Some people use social media and third-party websites to destroy your brand without ever interacting with your network. By the time you notice signs of these attacks on your network, it’s probably too late. To avoid damage, you need a warning of potential threats, along with actionable facts to:

a) Eliminate your most suspicious vulnerabilities before they are exploited.
b) Detect probes an attack at the earliest possible moment and respond effectively right away.
c) Understand the tactics, techniques, and procedures (TTP) of likely attackers and put effective defenses in place.
d) Identify and correct your business partners’ security weaknesses, especially those that have access to your network.
e) Detect data leaks and impersonations of your corporate brand (Jeff, 2020).

The main threat to an organization’s assets comes from within the organization, which is always a concern for the management and security manager. However, gathering information from existing corporate databases makes gathering security intelligence for an inside danger within a company much easier. Internal hazards are frequently easier to manage than external dangers. Obtaining security intelligence on external threats is more difficult and time-consuming, and it necessitates a bigger investment of resources.

Security intelligence, on the other hand, will enable a security manager to combat theft, industrial espionage, and sabotage. As a result, using knowledge systems will provide complete threat reporting and improve the security manager’s ability to respond to external threats (John et al., 2016). Direction, collection, processing, analysis, dissemination, and feedback are the six phases that make up the threat intelligence lifecycle, according to Giuseppe, Damian, and Willem-Jan (2021).

Figure 1 explains the threat intelligence cycle according to Giuseppe, Damian, and Willem-Jan (2021). The cycle is divided into four parts starting with the Direction, Collection, Processing/Analysis, and Dissemination.

The Direction stage is where requests are made to test the threat intelligence for possible dangers, which would give knowledge and the possible influences of intruders’ procedure, closeness also priorities about what to protect meaning “for instance stopping the arms trafficking to protect civilians’ life” and lastly the information assets and business processes that need to be protected (Giuseppe, Damian & Willem-Jan, 2021).
The collection is the process of information gathering: open-source scanning news, blogs, markets, crawling and scraping forums, websites, and any other relevant source, infiltrating closed sources such as dark web forums (Giuseppe, Damian & Willem-Jan, 2021).

The processing stage is where all the collected data are formatted, filtered for false and redundant information, and made usable by the organization (Giuseppe, Damian & Willem-Jan, 2021).

Analysis is the process of converting processed data into intelligence that can be used to make decisions. Decisions may include the prospect of further investigation of possible danger, as well as essential action to halt an attack, depending on the circumstances (Giuseppe, Damian & Willem-Jan, 2021). The dissemination stage involves getting the finished intelligence output to the places it needs to go (Giuseppe, Damian & Willem-Jan, 2021).

Meanwhile, Mark, Robert, Miyamoto, and Jason Martin (2015) stated the Security analytics process presented in Figure 2 below.

Explanatory analysis (or retrospective analysis) is frequently used in security intelligence to figure out what transpired so that methods can be used in the event of a security breach and reduce vulnerability. The main purpose of the concept is to predict actions that adversaries can take in order to put in place defensive measures to stop them. Experiencing the same thing, like a continuously conveyed denial of service (DOS) or a live invasion, the predictive examination might appear to be more significant. You’ll have the option to zero in on your endeavors on shutting knowledge holes and setting up early advance notice sensors assuming you comprehend gaps in your insight. These sensors are usually a mix of devices, such as seller advisory (e.g., Security Information and Event Management SIEM) and security investigative techniques (Sol, 2015). Security intelligence technologies, including SIEM systems and big data in security mechanisms, are critical for managing the risks of rising hacking and insider breaches. These strategies make it conceivable to utilize the progression of information to identify examples of use and access that sound inaccessible. SIEM arrangements monitor both ongoing occasions and a pile of authentic information to detect uncommon examples of conduct, qualify likely dangers to lessen misleading up-sides, and tell organizations when essential. Be that as it may, a SIEM arrangement can be ignorant concerning potential dangers to your safeguarded information (Sol, 2015). When you accept your security intelligence, you have two options: act or sit idle. You’d believe that making a move to address your danger would be the clearest decision, however, security intelligence can be troublesome in light of the fact that things aren’t dependably as “highly contrasting” as we’d need (Raji, 2022).

**Methods**

**Study design**

The paper adopted a descriptive survey. The survey design systematically collected data and as a result, the researcher theoretically assesses cybercrime threats in corporate bodies and the role that security intelligence could adopt as a measure to counter. The data was presented formally to staff and customers of Leadway Assurance Lagos, Nigeria, on the 7th of February 2022, and was collected on the 21st of February 2022.
Study population
The research population was drawn from the financial institution Leadway Assurance Lagos State, which operates an internet database communication internally with its customers and clients because they are prone to cybercrime. This study recruited 100 respondents, who include staff from each department and their customers. This paper employed the purposive random sampling technique and it was used to recruit 5 participants in each department of the institution with knowledge of the subject matter. The technique sampled 50 staff with 2 years and above experience in all departments of the organization and 50 customers of the organization. The recruitment of staff and customers was conducted physically through an introduction letter and interactions with the staff met in different departments.

Data collection
The sources of data collection are primary and secondary sources. The primary source was the questionnaire with close-ended questions used to arrive at figures to be calculated mathematically while the secondary data contained published books, newspapers and journals related to the paper. This paper used quantitative research that aimed at producing the best available data, process, and performance to aid understanding of the theme in this study. Preliminary testing was carried out with staff from each department to assess their response to the questions and, as a result, some questions were modified before the final administration of the questionnaire through an online link. A copy of the questionnaire can be found under Extended data (Afolabi & Raji, 2022).

A suitable design was structured, a two-point and four-point Likert scale for each variable. A two-point scale of Yes or No and a four-point scale of strongly agree (4), agree (3), disagree (2), and strongly disagree (1). An online questionnaire was sent to participants which enabled us to collect data in a less expensive, time efficient and less pressurized manner, leaving respondents to answer in their own time. The questionnaire comprised 3 sections, the first section assessed the level of cybercrime in financial institutions. The second section viewed the nature of the cybercrime, while the third section assessed the level of knowledge or awareness respondents have about security intelligence. The platform used was Google Forms. The location of respondents is Lagos, Nigeria and participants took less than 7 minutes to complete the questionnaire.

Data analysis
The data collected from the field was analyzed using frequency counts, percentages, and charts for the demographic variables while the inferential aspect was analyzed using the Chi-square test of independence. Furthermore, the paper used SPSS (Statistical Package for the Social Sciences) version 21 for the analysis.

Results
Operational questions
i. How often has cybercrime occurred in financial institutions in Nigeria?

Table 1 states all the questions assessing the rate of cybercrime occurrence and it revealed the rate of cybercrime in financial institutions in Nigeria. The table showed that 32% strongly agreed, 21% agreed, 17% disagreed and 30% strongly disagreed that financial institutions are vulnerable to internal and external threats from cybercrime. In order to make a comprehensive deduction out of 100% of the population, 53% of the respondents concur that the company is vulnerable to internal and external threats from cybercrime while 47% oppose that the company is vulnerable to internal and external threats from cybercrime. The full dataset can be found under Underlying data (Afolabi & Raji, 2022).

Cybercrime attacks can occur in diverse ways towards different people in different places. Thus, out of the respondents, 59% strongly agreed, 12% agreed, 9% disagreed and 20 strongly disagreed that cybercriminals have targeted more than one person at a time making the company’s customers and clients vulnerable to cybercrime threats. The deduction over 100% is that 71% of the respondents conceded that cybercriminals can target more than one person at a time while 29% are contradictory.

Commercial activities can be affected if attacked by cybercriminals. Thus, 68% of the respondents did not agree that customers in financial institutions experience electronic crime that has affected commercial activities.
However, in order to reveal the rate of cybercrime activities within the span of 2015-2020, respondents were asked if there was a rise in cybercrime activities on corporate bodies and 68% acknowledged that between 2015-2020 there would be a rise in cybercrime activities on corporate entities in Nigeria while 32% diverge.

ii. What type of cybercrime attacks are experienced on financial institutions in Nigeria?

Table 2 revealed the type of cybercrime attacks experienced on financial institutions in Nigeria.

Respondents were asked if they admit that the top 5 cybercrimes affecting financial institutions’ business and individuals’ data are phishing scams, website spoofing, piracy, ransomware, and hacking. Thus, 97% of the respondents concur but 3.0% believed otherwise. Furthermore, phishing scams were acceded by respondents with 84% being the most used method to perform cybercrime activities on financial institutions while 16.0% of the respondents disputed. Customers and staff were asked if they have experienced website spoofing as a method to perform cybercrime activities on them, 65% of the respondents dissented while 35% agree. Piracy has to be a cybercrime attack that has less occurrence in financial institutions, 59% of the respondents disagreed that the financial institution’s document or data has not in any way been pirated while 41% agreed.

iii. Can Security Intelligence be used to checkmate these attacks?

Table 3 revealed the Security intelligence awareness among staff and customers and if it can checkmate these cyber-attacks on the financial institutions. The table further revealed that 34% and 18% of the staff and customers agreed that Security threat data or information that has been collected, analyzed, should be disseminated to staff and customers to reduce cybercrime in the company respectively while 16% and 32% of the staff and customers’ respondents disagree respectively.

<table>
<thead>
<tr>
<th>Table 1. Level of cybercrime.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Questions</td>
</tr>
<tr>
<td>Are financial institutions vulnerable to internal and external threats from cybercrime?</td>
</tr>
<tr>
<td>Cybercriminals have targeted more than one person at a time making customers and clients vulnerable to cybercrime threats. Do you agree?</td>
</tr>
<tr>
<td>Do customers in financial institutions experience electronic crime that has affected commercial activities?</td>
</tr>
<tr>
<td>Between 2015 and 2020 there was a rise in cybercrime activities on corporate entities in Nigeria. Do you agree?</td>
</tr>
</tbody>
</table>

Source: Authors’ Field Survey (2022).

<table>
<thead>
<tr>
<th>Table 2. Nature of cybercrime.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Questions</td>
</tr>
<tr>
<td>The top 5 cybercrimes affecting financial institutions’ business and individuals’ data are phishing scams, website spoofing, piracy, ransomware, and hacking. Do you agree?</td>
</tr>
<tr>
<td>Are you aware that phishing scams have been the most used method to perform cybercrime activities on financial institutions?</td>
</tr>
<tr>
<td>Financial institutions have experienced website spoofing as a method to perform cybercrime activities. Do you agree?</td>
</tr>
<tr>
<td>Piracy is a crime, has the company’s document or data in any way been pirated?</td>
</tr>
</tbody>
</table>

Source: Authors’ Field Source (2022).
<table>
<thead>
<tr>
<th>Questions</th>
<th>Strongly agree</th>
<th>Agree</th>
<th>Disagree</th>
<th>Strongly disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Staff N (%)</td>
<td>Customers N (%)</td>
<td>Staff N (%)</td>
<td>Customers N (%)</td>
</tr>
<tr>
<td>Security threat data information collected and analyzed, should be</td>
<td>18(18.0)</td>
<td>18(18.0)</td>
<td>16(16.0)</td>
<td>0(0.0)</td>
</tr>
<tr>
<td>disseminated to reduce cybercrime in the company. Do you agree?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allowing the security functions in the organization to be proactive will</td>
<td>17(17.0)</td>
<td>16(16.0)</td>
<td>22(22.0)</td>
<td>0(0.0)</td>
</tr>
<tr>
<td>decrease the required time to respond to a risk or threat posed by</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cybercrime. Do you agree?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security intelligence comprises tools and applications, is SIEM a</td>
<td>18(18.0)</td>
<td>24(24.0)</td>
<td>1(1.0)</td>
<td>1(1.0)</td>
</tr>
<tr>
<td>security intelligence application tool?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does security intelligence focus on setting up early-warning sensors in</td>
<td>20(20.0)</td>
<td>19(19.0)</td>
<td>0(0.0)</td>
<td>2(2.0)</td>
</tr>
<tr>
<td>order to know the organization's landscape and address intelligence gaps?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Authors’ Field Source (2022).
The highest percentage 39% and 16% of staff and customers respectively, agreed that allowing the security functions in the organization to be proactive will decrease the required time in responding to a risk or threat posed by cybercrime while 11% and 34% of the respondents disagreed.

Staff and customers 42% and 17% respectively both agreed that Security intelligence comprises tools and applications and SIEM (security information and event management) is a security intelligence application tool respectively, while 8% and 33% disagreed.

Lastly, 39% of staff and 19% of customers agreed that security intelligence focuses on setting up early-warning sensors in order to know the organization’s landscape and address intelligence gaps while 11% of staff and 31% of customers disagreed respectively.

**Hypothesis testing**

**Table 4 revealed Hypothesis 1**

**H01:** Security Intelligence Intervention is independent of the nature of cybercrime among respondents.

**H11:** Security Intelligence Intervention is dependent on the nature of cybercrime among respondents.

**Decision:** Since both the p-value (0.454) is greater than Alpha-Value (0.05) and the $\chi^2$-Value (2.621*) is less than the tabulated Chi-Square value at 3 degrees of freedom, it is therefore concluded that security intelligence intervention is independent of the nature of cybercrime across both staff and customers.

**Table 5 revealed Hypothesis 2**

**H02:** The nature of the type of cybercrime is independent of the age group of respondents

**H12:** The nature of cybercrime is dependent on the age group of respondents

### Table 4. Security intelligence intervention is independent of the nature of cybercrime across both staff and customers.

<table>
<thead>
<tr>
<th>Nature of cybercrime among staff and customers</th>
<th>Yes (%)</th>
<th>No (%)</th>
<th>$\chi^2$-Value</th>
<th>Df</th>
<th>P-Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security intelligence</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>32(32.0)</td>
<td>8(8.0)</td>
<td>2.621*</td>
<td>3</td>
<td>.454</td>
</tr>
<tr>
<td>Agree</td>
<td>20(20.0)</td>
<td>3(3.0)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strongly agree</td>
<td>34(34.0)</td>
<td>3(3.0)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>86(86.0)</td>
<td>14(14.0)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Adjusted value.

### Table 5. The nature of cybercrime is independent of the age group of respondents.

<table>
<thead>
<tr>
<th>Age</th>
<th>Nature of cybercrime among Staff and customers</th>
<th>$\chi^2$-Value</th>
<th>Df</th>
<th>P-Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;=20</td>
<td>3(3.0)</td>
<td>3(3.0)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21-30</td>
<td>70(70.0)</td>
<td>9(9.0)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31-39</td>
<td>4(4.0)</td>
<td>0(0.0)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Above 40 yrs</td>
<td>9(9.0)</td>
<td>2(2.0)</td>
<td>7.716*</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>86(86.0)</td>
<td>14(14.0)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Adjusted value.
**Table 6. The nature of cybercrime among staff and customers is independent of sex.**

<table>
<thead>
<tr>
<th></th>
<th>Nature of cybercrime among Staff</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes (%)</td>
<td>No (%)</td>
<td>$\chi^2$-Value</td>
<td>Df</td>
</tr>
<tr>
<td><strong>Sex</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>48(48.0)</td>
<td>7(7.0)</td>
<td>.164$^a$</td>
<td>1</td>
</tr>
<tr>
<td>Female</td>
<td>38(38.0)</td>
<td>7(7.0)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>86(86.0)</td>
<td>14(14.0)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

$a$Adjusted value.

**Decision:** Both the p-value (0.052) is greater than Alpha-Value (0.05) and the $\chi^2$-Value (7.716$^a$) is less than the tabulated Chi-Square value at 3 df of freedom. It is therefore concluded that the nature of cybercrime is independent of the age group. That is all age groups of both customers and staff tend to commit different types of cybercrime.

Table 6 revealed Hypothesis 3

**H$_{03}$:** The nature of cybercrime is independent of sex

**H$_{13}$:** The nature of cybercrime is dependent on sex

**Decision:** Both the p-value (0.685) is greater than Alpha-Value (0.05) and the $\chi^2$-Value (0.164$^a$) is less than the tabulated Chi-Square value at 1 degree of freedom. It is therefore concluded that the nature of cybercrime among staff and customers is independent of sex. That is both male and female customers and staff tend to commit different nature of cybercrime.

**Discussion**

This study carried out a quantitative collection of data using staff and customers of some financial institutions in Nigeria. The analysis of research questions reviewed three variables which are the level, nature of cybercrime on financial institutions in Nigeria, and security intelligence awareness/application. Thus, the study asked three questions which are the rate of cybercrime attacks, the kind of cybercrime attacks experienced, and the security intelligence awareness/applications that can be used to checkmate cybercrime.

Findings revealed that on a scale of 1 to 10 the financial institution Leadway Assurance experience a 5-scale rating. There is internal and external vulnerability which is a threat to the company. It was realized that customers experience fewer attacks in financial institutions, meaning customers are confident with their information on the company’s database. However, due to the rise in cybercrime activities in Nigeria and against corporate bodies, financial institutions in Nigeria need more security operational posture in order to be proactive and guard against cybercrime attacks. There are several types or nature of cybercrime attacks across the globe. Thus, findings reveal that the top five cybercrime attacks affecting financial institutions in Nigeria are phishing scams, website spoofing, piracy, ransomware, and hacking. Particularly, a phishing scam with 90% is prevalent and it is the most used mechanism to commit cybercrime, while website spoofing, piracy, and hacking are within 50%-60%.

If with the advent of IT infrastructure, tools and measures, there is still a prevalence of cyberattacks on corporate bodies in Nigeria, then more proactive innovation or techniques should be tested and if it works should be applied. Thus, findings reveal that security threat data or information that has been collected and analyzed should be disseminated to staff and customers which would bring awareness of the type of prevalent attack in the organization. Security intelligence was looked into and data explained that in a financial institution, setting up early-warning sensors in order to know the organizational landscape and intelligence gap is advised.

**Conclusions**

The level of cybercrime in financial institutions in Nigeria was found to be too high by the respondents. There is also a high level of perception of the nature of cybercrime. In addition, security intelligence explained that the collection of previous cybercrime attacks can be used for predictive analysis. It highlighted SIEM as a security intelligence tool that can be applied in an organization or financial institution. The paper states that security intelligence intervention is independent of the nature of cybercrime across both staff and customers and also the nature of cybercrime is independent of age group and sex. That is customers and staff of all age groups and sexes tend to commit cybercrimes of different natures.
Data availability

Underlying data

This project contains the following underlying data:

- Security_Intelligence_Data.xlsx

Extended data
This project contains the following extended data:

- RESEARCH_QUESTIONNAIRE_ON_SECURITY_INTEL_MANUSCRIPT.docx

Data are available under the terms of the Creative Commons Zero “No rights reserved” data waiver (CC0 1.0 Public domain dedication).

References


Publisher Full Text
Reference Source
Reference Source
Publisher Full Text
The benefits of publishing with F1000Research:

• Your article is published within days, with no editorial bias
• You can publish traditional articles, null/negative results, case reports, data notes and more
• The peer review process is transparent and collaborative
• Your article is indexed in PubMed after passing peer review
• Dedicated customer support at every stage

For pre-submission enquiries, contact research@f1000.com