Cybersecurity in Digital Banking: Risks, Remedies & Recommended Strategies

Ademola E. Elubode*

Abstract

In the modern financial landscape, digital banking has revolutionised the way individuals and businesses manage their finances. However, this digital transformation has also introduced significant security concerns that must be addressed to ensure financial data's integrity, confidentiality, and availability. This paper explores the multifaceted security challenges associated with digital banking, including cyber threats such as phishing, malware, and data breaches. The paper examines existing security measures and legal frameworks designed to protect digital banking systems. Additionally, the paper identifies key vulnerabilities and evaluates the effectiveness of current solutions. By analysing case studies and real-world incidents, the paper offers insights into best practices and innovative approaches to enhance digital banking security. The paper concludes that as cybercrime advances, banks must upgrade from outdated systems to more modern, secure infrastructure to effectively combat emerging threats. This migration requires a comprehensive overhaul, not just superficial upgrades, to strengthen cybersecurity and protect financial assets.

Keywords: cybersecurity, vulnerabilities, phishing, digital banking, malware

1. Introduction

Digital banking, often referred to as online banking, provides a convenient way for individuals and businesses to manage their financial activities through digital platforms such as mobile applications, websites, and automated teller machines (ATMs). This significant transition towards digital banking has revolutionised the traditional banking landscape over the past few decades. It has not only enhanced accessibility and efficiency but has also fundamentally altered the way people interact with their finances. Customers can now execute a wide range of transactions—such

as checking account balances, transferring funds, paying bills, and applying for loans—at any time and from virtually anywhere, marking a notable shift in the banking experience.[1]

Digital banking began in the late 20th century when banks started using technology for services like ATMs and electronic fund transfers (EFT). In the 1990s, as the Internet became more popular, banks created online platforms. These platforms let customers handle transactions, check account balances, and access other services from home. The rise of smartphones in the 2000s made digital banking even more popular. Mobile banking apps offered users greater convenience and easier access to their finances.[2]

Digital banking has revolutionised the financial ecosystem, offering numerous benefits that enhance user experience. Firstly, it provides 24/7 access to banking services from anywhere in the world, significantly improving convenience and customer satisfaction. Additionally, the automation of banking processes reduces the necessity for physical branches and staff, leading to cost savings for banks and faster transactions for customers. Importantly, digital banking promotes financial inclusion, making services accessible to underserved populations in remote areas, thereby bridging socio-economic gaps. While it presents new security challenges, advanced measures such as encryption and multi-factor authentication help protect customer data. Finally, the competitive landscape of digital banking fosters innovation among fintech startups and traditional banks, driving the development of new technologies and reducing reliance on paper, which contributes to environmental sustainability.[3]

The digital banking sector faces significant security concerns that threaten the integrity and confidentiality of financial data, largely due to the growing sophistication of cybercriminals. Phishing attacks remain prevalent, tricking individuals into revealing sensitive information through deceptive emails and websites. Additionally, malware and ransomware can compromise

* LL. B (Hons) B.L LL.M (Ife), Lecturer, Department of Private and Property Law, Faculty of Law, Elizade University, Ilara-Mokin, Ondo State. E-mail: ademola.elubode@elizadeuniversity.edu.ng; +2348084628449.

[1] Alice Ivey, 'A Brief History of Digital Banking', https://cointelegraph.com/news/a-brief-history-of-digital-banking?form=MG0AV3 accessed 6th January 2025.

[2] https://www.profinch.com/evolution-of-digital-banking-system/?form=MG0AV3 accessed 6th January 2025.

[3] C. Horton, and E. Aldrich, '5 Benefits of Digital Banking', https://www.forbes.com/advisor/banking/benefits-of-digital-banking/?form=MG0AV3 accessed 6th January 2025.

banking systems, leading to severe data breaches and financial losses.[4] Insider threats pose risks as well, as employees with access to sensitive information may inadvertently or intentionally compromise security. The shift to remote work has introduced further vulnerabilities, making it essential for institutions to enhance their protective measures. A comprehensive strategy that includes robust cybersecurity practices and continuous monitoring is crucial for safeguarding digital banking operations.[5] All these security concerns are the main focus of this paper.

2. Meaning of Cybersecurity

The term "cybersecurity" encompasses a comprehensive arrangement of technologies, protocols, and methodologies designed to safeguard digital systems against a wide variety of threats. These threats include attacks such as hacking, the spread of malware and viruses, data breaches, and unauthorised access to networks, devices, applications, and sensitive information.[6] In today's digital age, banks handle vast quantities of confidential information, including customer financial data, personal identification details, and extensive transaction records. The implementation of robust cybersecurity measures is essential to safeguard this valuable data and various forms of cybercrime.[7]

In the banking sector, the paramount objective of cybersecurity is the protection of users' assets and personal information. However, the scope of cybersecurity in banking extends beyond just protecting customer data; it involves securing the entire digital ecosystem of a bank, which includes everything from online banking platforms and mobile applications to internal databases and payment processing systems. Effective cybersecurity measures are designed to prevent unauthorised access, detect data leaks, and counteract malicious attacks that could jeopardise both customer information and the bank's operational integrity.[8]

---

[4] Claire dela Luna, 'Cyber Security in Banking: Threats, Solutions & Best Practices', https://www.esecurityplanet.com/cloud/cyber-security-in-banking/?form=MG0AV3 accessed 6th January 2025.

[5] GuardRails, 'The Top 10 Cybersecurity Threats to Digital Banking and How to Guard Against Them', https://www.guardrails.io/blog/the-top-ten-cyber-security-threats-to-digital-banking-and-how-to-guard-against-them/?form=MG0AV3 accessed 6th January 2025.

[6] See Claire dela Luna, (n4) supra.

[7] *Ibid.*

[8] V. Sharma, 'Cybersecurity in Banking: Importance, Threats, Challenges', https://www.knowledgehut.com/blog/security/cyber-security-in-banking accessed 6th January 2025.

As the world increasingly shifts towards cashless transactions, the volume of online activities continues to rise. Individuals are now relying on digital payment methods, such as debit and credit cards, for a wide range of financial transactions. This growing dependence on digital finance necessitates robust cybersecurity measures to ensure that sensitive transaction data and user information are shielded from potential cyber threats. Effective cybersecurity not only protects consumer assets but also helps maintain trust in the financial system as a whole.[9]

2.1 Importance of Cybersecurity in Digital Banking

The banking industry has placed an increased emphasis on cybersecurity due to the critical importance of building and maintaining credibility and trust with customers. As financial institutions handle vast amounts of sensitive personal and financial information, the need for robust cybersecurity measures has never been more paramount. A breach in security can lead to devastating consequences, not only in terms of financial loss but also in the erosion of customer confidence.[10] Let us take a look at some of the factors that underscore the significance of cybersecurity in the banking sector:

2.1.1 Safeguarding Confidential Information

Financial institutions, particularly banks, are custodians of a vast amount of sensitive information. This includes intricate details such as account numbers, biometric verification numbers (BVN), national identification numbers (NIN), Social Security numbers, and various forms of personal identification. The importance of implementing robust cybersecurity measures cannot be overstated, as these protocols are crucial to protect this sensitive data from unauthorised access and potential exploitation, ensuring the privacy and security of individuals' financial and personal information.[11]

2.1.2 Regulatory Compliance

---

[9] *Ibid.*

[10] See V. Sharma, (n8) supra.

[11] See Claire dela Luna, (n4) supra.

The banking industry operates under a comprehensive framework of regulations designed to safeguard data protection and privacy. These regulations, which include provisions from the CBN Risk-based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Banks (PSBs) 2023 and the Nigerian Data Protection Act (NDPA), impose stringent requirements on how financial institutions handle sensitive customer information.[12] Non-compliance with these regulations can lead to severe consequences, including substantial financial penalties and legal action from regulatory bodies.[13] Such repercussions not only impact the financial standing of the institutions but also damage their reputations and erode customer trust. This reality underscores the critical importance of adopting robust cybersecurity practices to protect against data breaches, ensure regulatory compliance, and maintain the integrity of customer information in an increasingly digital banking landscape. Implementing effective security measures is, therefore, not just a legal obligation but a vital component of responsible banking operations.

2.1.3 Prevention of Financial Loss

Cyberattacks pose significant financial threats to organisations, particularly in the banking sector, where the stakes are often higher. These attacks can lead to direct financial losses, such as the theft of funds from accounts or financial systems. In addition to these immediate losses, banks must also contend with substantial costs associated with incident response and recovery efforts. This includes expenses for forensic analysis to determine the scope of the breach, implementing remedial measures to secure systems, and potentially compensating affected customers.[14]

Moreover, the reputational damage that results from a cyberattack can lead to a loss of trust among clients, further impacting the bank's financial stability and customer base. By making proactive investments in robust cybersecurity measures, such as advanced security protocols, employee training, and ongoing risk assessments, banks can significantly mitigate the risk of these financial

---

[12] See Regulation 1.0 of the CBN Risk-Based Cybersecurity Framework And Guidelines For Deposit Money Banks And Payment Service Banks 2023.

[13] *Ibid.*

[14] See V. Sharma, (n8) supra.

losses. This not only protects their assets but also safeguards their overall profitability and long-term viability in a highly competitive industry.[15]

There have been reported cases of cybersecurity attacks on Nigerian banks. For instance, in October 2024, scammers hacked Hope Payment Service Bank and stole ₦10 billion. The Federal High Court in Abuja ordered the freezing of 818 bank accounts suspected to have received the proceeds of this cyberattack.[16] This incident highlights the importance of robust cybersecurity measures in the banking sector to protect against such threats.

2.1.4 Preservation of Reputation

Trust is an essential foundation of the banking relationship between institutions and their clients. When customers choose a bank, they do so with the expectation that their financial information and assets will be safeguarded with the utmost care.[17] However, a significant security breach can severely undermine this trust, often resulting in considerable damage to the bank's reputation. When a significant security breach occurs, it can severely tarnish a bank's reputation, causing customers to lose faith and potentially switch to competitors. Consequently, banks may face not only the immediate loss of business but also long-term implications, including decreased customer loyalty and difficulties in attracting new clients.

To combat these challenges, banks must maintain a robust security posture. This involves implementing advanced security measures, continually assessing vulnerabilities, and educating both staff and customers about best practices in cybersecurity. By prioritising these efforts, banks can reinforce public confidence in their operations and demonstrate their commitment to protecting clients' sensitive information.[18] Ultimately, a strong security framework mitigates risks associated with breaches and strengthens the institution's overall reputation in the eyes of its customers and the broader community.

---

[15] *Ibid.*

[16] Pasca Oparada, 'Scammers Hack Nigerian Bank, Steal N10 Billion, 818 Accounts Identified as, Other Banks Upgrade', (Legit.ng, 17th October 2024) <https://www.legit.ng/business-economy/money/1619636-scammers-hacks-nigerian-bank-steal-n10-billion-818-accounts-frozen-zenith-upgrade/> accessed 6th January 2025.

[17] See V. Sharma, (n8) supra.

[18] *Ibid.*

2.1.5 Evolving Threat Landscape

As technology and digital banking services continue to advance at a rapid pace, the strategies employed by cybercriminals are also becoming increasingly sophisticated. This evolution poses significant challenges for financial institutions, as they must remain vigilant and agile in the face of emerging threats.[19] Firms must regularly assess and update their security protocols to address a variety of vulnerabilities that can arise from new technological developments. This includes implementing advanced encryption methods, utilising artificial intelligence for threat detection, and ensuring compliance with the latest regulatory standards.

It is important to note that there have been recent changes in the Nigerian core banking platform.[20] In October 2024, several Nigerian banks, including GTBank,[21] Zenith Bank[22] and First Bank (which clarified that their recent upgrade was focused on their supplier platform and not their customer-facing digital banking system)[23] migrated to new core banking systems to enhance their service delivery and system efficiency. For instance, Sterling Bank switched to a new core banking system called SeaBaaS on September 10, 2024.[24] These changes were driven by the need to improve customer experience, increase operational efficiency, and enhance security against cyber threats.

3. Cybersecurity Frameworks for Banks in Nigeria

---

[19] *Ibid.*

[20] A core banking application is an essential software solution that banks utilise to efficiently manage their fundamental operations which includes overseeing customer account management, processing various financial transactions, and implementing effective risk management strategies. By centralising these critical processes, the application enables banks to provide seamless services to their customers, ensuring accuracy, security, and compliance across all banking activities.

[21] Which switched to the Finacle core banking platform, developed by Infosys.

[22] Which migrated to Oracle's Flexcube.

[23] Dave Ibemere, 'First Bank Clarifies System Migration, Assures Customers of Uninterrupted Banking Service', (Legit.ng 25th October 2024) < https://www.legit.ng/business-economy/money/1621381-first-bank-clarifies-system-upgrade-report-assures-smooth-banking-service/> accessed 7th January 2025.

[24] Tola Owoyele, 'GTB, Zenith… Why Nigerian Banks Are Migrating to New Core Banking Systems', (Foundation for Investigative Journalism, 14th October 2024) < https://fij.ng/article/gtb-zenith-why-nigerian-banks-are-migrating-to-new-core-banking-systems/> accessed 7th January 2025.

3.1 CBN Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks 2023[25]

The Nigerian financial system has grown rapidly in recent years, leading to more products, services, institutions, and stakeholders. To build public trust in the financial system, banks must operate in a safe and secure environment. Financial institutions use technology to speed up the flow of money and provide services to their customers. They need to manage their technology systems to protect the confidentiality, integrity, and availability of information. This helps to avoid financial losses and reduce damage to their reputation.

Cybersecurity threats are becoming more complex and happen more often. Common threats include phishing, ransomware, and Distributed Denial-of-Service (DDoS) attacks. As a result, financial institutions must actively protect their important information to stay strong against these ongoing threats. The rise of new technology used by financial institutions to serve customers has also increased their risk of being attacked.

India's banks experienced 248 successful data breaches from June 2018 to March 2022, as reported to Parliament on August 2. These breaches primarily involved the leakage of card details and the theft of both business and non-business information. Public sector banks reported 41 breaches, while private sector banks accounted for 205, and foreign banks faced two incidents. In response to concerns about data security in the banking and insurance sectors, the Union Minister of State for Finance, Bhagwat Karad, highlighted that the Reserve Bank of India (RBI) has issued guidelines for a Cyber Security Framework for Scheduled Commercial Banks. These guidelines require banks to implement cybersecurity measures and IT controls to prevent data leakage.[26]

---

[25] https://www.cbn.gov.ng/Out/2024/BSD/EXPOSURE%20DRAFT%20OF%20THE%20RISK-BASED%20CYBERSECURITY%20FRAMEWORK%20AND%20GUIDELINES%20FOR%20DEPOSIT%20MONEY%20BANKS%20AND%20PAYMENT%20SERVICE%20BANKS.pdf?form=MG0AV3 accessed 6th January 2025.

[26] https://www.moneycontrol.com/news/business/banks/indian-banks-reported-248-data-breaches-in-last-four-years-says-government-8940891.html accessed 6th January 2025.

The Central Bank of Nigeria (CBN) has released this framework to help banks and payment service providers improve their cybersecurity. This framework outlines the basic cybersecurity controls that should be in place. It aims to guide the implementation of cybersecurity programs to make these institutions more resilient against cyber threats. This framework provides comprehensive guidelines for managing cybersecurity risks in digital banking. It includes responsibilities for the board of directors, senior management, and the Chief Information Security Officer (CISO), as well as requirements for vulnerability identification, third-party risk management, and cybersecurity maturity assessment.[27]

The framework uses a risk-based approach to manage cybersecurity risks. It has seven main parts:

1. Cybersecurity Governance and Oversight
2. Cybersecurity Risk Management System
3. Enhancing Cybersecurity Resilience
4. Emerging Technologies
5. Metrics, Monitoring & Reporting
6. Compliance with Statutory & Regulatory Requirements
7. Enforcement[28]

This new framework replaces the previous version issued in October 2018 and addresses gaps that have developed over time. It also takes into account recent laws and regulations, such as the Banks and Other Financial Institutions Act (BOFIA 2020) and the Nigerian Data Protection Act (NDPA 2023).[29]

The CBN Risk-based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Banks (PSBs) 2023 applies to commercial banks, merchant banks, non-interest banks, and payment service banks that the Banking Supervision Department of the CBN oversees. Together, these are referred to as Supervised Financial Institutions (SFIs).

4. Major Cybersecurity Risks Encountered by Financial Institutions

[27] See (n12) supra.
[28] See (n24) supra.
[29] See Regulations 1-6 generally.

The banking industry faces ongoing cyber threats as hackers continually improve their methods to take advantage of weaknesses. Banks hold large amounts of sensitive financial data and customer information, making them prime targets for cybercriminals.[30] In this paper, we will look at the major cybersecurity threats in the banking sector in Nigeria, highlighting real-world incidents and current trends.

4.1 Phishing Attacks

Phishing continues to be one of the most widespread and concerning threats faced by the banking industry. Cybercriminals employ a variety of tactics, including fraudulent emails, deceptive text messages, and counterfeit websites that mimic legitimate banking platforms, all designed to mislead customers and employees into divulging sensitive information. This can include account numbers, passwords, Social Security numbers, and other personal details. Once cybercriminals successfully obtain this information, they can execute a range of malicious activities, such as siphoning funds, committing identity theft, or breaching the bank's internal systems, leading to potentially catastrophic consequences for both individuals and institutions. Between 2018 and 2022, the FBI received 3.26 million complaints about cyberattacks, leading to reported losses of $27.6 billion. In 2022, the U.S. recorded 800,944 cybercrimes. This number is expected to keep rising.[31]

In 2022, phishing attacks accounted for a significant 41 per cent of all cybercrimes, highlighting their prevalence and impact in the digital landscape. The introduction of ChatGPT in late 2022 marked a pivotal shift in the nature of these attacks, as cybercriminals began leveraging generative AI tools to enhance their strategies. This technological advancement has led to a dramatic improvement in the quality of phishing communications. Gone are the days of poorly written emails riddled with grammatical errors, awkward phrasing, and excessive use of colourful capital letters aimed at capturing attention.[32] Instead, the new generation of phishing attempts features

---

[30] A. Wilson, 'Cybersecurity in Banking: Importance, Threats, Challenges, and Evolution', https://www.imscloudservices.com/knowledge-base/security-articles/cybersecurityin-banking/ accessed 9th January 2025.

[31] E. Judd, 'Seven Cybersecurity Threats for Banks in 2024—and Some Smart Precautions', https://bankingjournal.aba.com/2024/02/seven-cybersecurity-threats-for-banks-in-2024-and-some-smart-precautions/ accessed 9th January 2025.

[32] *Ibid.*

polished, professional-looking messages that are much more convincing and proficiently crafted. As a result, individuals and organisations are facing increasingly sophisticated and deceptive threats, making it more challenging to discern legitimate communications from malicious ones. This evolution underscores the urgent need for heightened awareness and advanced cybersecurity measures to combat the growing sophistication of phishing attacks in our digital interactions.

In 2024,[33] law enforcement agencies successfully dismantled a highly sophisticated phishing network that had been targeting thousands of Australians, with a particular focus on customers from major banks in the country. This intricate scam involved sending out thousands of fraudulent emails that expertly imitated official bank communications, making it difficult for victims to discern the difference between authentic messages and those crafted by scammers. Many unsuspecting recipients fell prey to the ruse, unwittingly providing their login credentials and other sensitive information in response to these deceptive communications.[34]

The fallout from this widespread attack was significant, resulting in substantial financial losses for the affected individuals and raising alarm across the banking sector. The incident not only emphasised the urgent need for heightened vigilance among banking customers but also served as a stark reminder of the persistent and evolving threat of phishing scams in the digital age.[35] In response to this scenario, banks and financial institutions are urged to implement more robust security measures, educate their customers about recognising phishing attempts, and continuously update their protocols to combat these evolving threats.

4.2 Spoofing

Spoofing is a form of cyber-attack that is closely related to phishing, but it often employs more sophisticated techniques to deceive individuals. There are several distinct types of spoofing

---

[33] H. Cohen, and A. McDonald, 'Adrian Katong ran a One-Stop Shop for Phishing Scams. Here's How He Was Tracked Down', https://www.abc.net.au/news/2024-08-01/adrian-katong-phishing-scams-network-bulletproftlink-malaysia/104118036 accessed 9th January 2025.

[34] Myantispyware Team, 'Payment of US$8,600,000 to Your Bank Account Email Scam: What You Need to Know', https://www.myantispyware.com/2025/01/08/payment-of-us8600000-to-your-bank-account-email-scam-what-you-need-to-know/ accessed 10th January 2025.

[35] *Ibid.*

attacks, all of which leverage some element of impersonation to manipulate the victim. One prevalent method is domain spoofing, where an attacker creates a counterfeit version of a legitimate domain.[36] This fraudulent replication is crafted to look nearly identical to the actual domain, often fooling users into believing they are accessing a trustworthy website. By doing so, the attackers aim to trick individuals into submitting sensitive information, such as login credentials and personal data. This tactic hinges on the assumption that users may not scrutinise the web address closely enough to notice subtle differences that indicate the site is not genuine.[37]

An emerging spoofing technique that has gained attention in recent years is linked to facial recognition technology. With the increasing reliance on facial recognition for unlocking smartphones and accessing various applications, cybercriminals are actively seeking ways to exploit potential vulnerabilities in these systems. Recent research has shown that it is feasible for malicious actors to create highly realistic 3D facial models using images sourced from social media platforms.[38] By leveraging these models, they can potentially bypass security measures like Face ID, thus gaining unauthorised access to personal devices.

The implications of this technology extend beyond mere unauthorised access, as it opens the door to more sinister applications. For instance, cybercriminals could fabricate incriminating or embarrassing video content featuring high-profile individuals—celebrities, politicians, and business leaders—by using manipulated facial recognition data. Such deepfake videos could be employed for blackmail or extortion, as the affected individuals may feel pressured to pay to prevent the release of damaging footage. This represents a troubling intersection of technology and crime, highlighting the need for enhanced security measures and public awareness around the vulnerabilities associated with facial recognition systems.

Another common form of spoofing involves the manipulation of caller ID information. In this scenario, an attacker fabricates a financial institution's phone number to contact or text customers

---

[36] B. Lenaerts-Bergmans, 'What is a Spoofing Attack?', https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/spoofing-attack/ accessed 9th January 2025.

[37] *Ibid.*

[38] Anbarjafari et al., '3D Face Reconstruction with Region Based Best Fit Blending Using Mobile Phone for Virtual Reality Based Social Media', https://arxiv.org/pdf/1801.01089 accessed 10th January 2025.

directly. When this spoofed number reaches a customer's phone, it appears as though the legitimate bank is reaching out, which can lead to confusion and concern for the victim. This type of attack can be particularly insidious, as the correct caller ID displayed on the customer's device can mask the true nature of the communication.[39] On the other hand, in a Man-in-the-Middle (MitM) attack, an adversary might establish a rogue Wi-Fi access point that resembles a trustworthy network. Once users connect to this fake network, the attacker can intercept and monitor their web activity, enabling them to collect personal information such as login credentials and credit card numbers.[40]

This practice has been notably prevalent in countries like Nigeria, where scammers have been known to call unsuspecting bank customers. During these calls, they might instruct the victims to provide a particular code, claiming that it was sent to their phones for necessary updates to their accounts. Such tactics exploit trust and urgency, making it challenging for individuals to discern a real communication from a fraudulent one.[41]

To mitigate the risks associated with these forms of spoofing, implementing seamless multi-factor authentication can prove highly effective. In other words, you can help prevent attacks by banning bad passwords, blocking old authentication methods, and training employees about phishing. One of the best things you can do is turn on Multi-Factor Authentication (MFA), which adds an extra layer of security that makes it very hard for attackers to access accounts. It blocks over 99.9 percent of account compromise attacks. With MFA, knowing or cracking the password alone is not enough to gain access.[42] Even if someone gets your password, the second authentication method can stop them from accessing your account. Online services use MFA to confirm who you are and keep your information safe from hackers. By asking for extra verification, like a PIN, a text confirmation, or a fingerprint, they greatly improve the security of your account. By adding an

---

[39] https://www.comptia.org/content/articles/what-is-spoofing accessed 9th January 2025.

[40] See B. Lenaerts-Bergmans, (n35) supra.

[41] Dave Ibemere, 'Fraud Alert: First Bank, Access, GTB, UBA Expose Tricks, Advise Customers To Protect Bank Accounts', (Legit.ng 14th February 2024) https://www.legit.ng/business-economy/money/1570866-access-gtb-bank-sends-scam-alarm-messages-customers/ accessed 10th January 2025.

[42] Melanie Maynes, 'One Simple Action You Can Take to Prevent 99.9 Percent of Attacks on Your Accounts', https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/ accessed 10th January 2025.

additional layer of verification beyond just a password, organisations can significantly enhance their security posture and reduce the likelihood that users will fall prey to these deceptive tactics.[43]

4.3 Malware & Ransomware

Malware, which encompasses a range of malicious software types, poses a significant threat to the banking sector, with ransomware being one of the most concerning varieties. Malware can infiltrate bank systems through various means, such as phishing emails, malicious downloads, or vulnerabilities in software. Once inside, it can steal sensitive data, compromise system integrity, or even cause widespread operational failures that disrupt banking services.[44]

Ransomware, in particular, operates by encrypting a victim's data or locking them out of their systems, rendering them inoperable. Attackers then demand a ransom, typically paid in cryptocurrencies, in exchange for a decryption key or to restore system access.[45] This scenario can be compared to a virtual kidnapping, where the attackers hold the bank's operational capabilities hostage until their demands are met. One of the most infamous incidents involving ransomware was the WannaCry[46] attack in May 2017. This global cyberattack rapidly spread across networks, infecting hundreds of thousands of computers in over 150 countries, including numerous financial institutions. The WannaCry malware exploited a vulnerability in Microsoft Windows, which had not been adequately patched in many systems.

Nigeria successfully avoided the worst impacts of the WannaCry cyberattack. According to various reports from that period, the country did not experience any significant incidents related

---

[43] *Ibid.*

[44] A. Wilson, (n30) supra.

[45] https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/ accessed 10th January 2025.

[46] The WannaCry ransomware attack on May 12, 2017, affected over 200,000 computers in more than 150 countries, targeting notable organisations like FedEx and the UK's National Health Service. The attack was temporarily neutralised when a security researcher discovered a "kill switch," but many computers remained encrypted until the ransom was paid or the encryption reversed. WannaCry exploited a vulnerability known as "EternalBlue," developed by the US National Security Agency and later leaked by the group Shadow Brokers. This exploit primarily affected older, unpatched versions of Microsoft Windows, which allowed the ransomware to spread rapidly.

to WannaCry, which is a type of ransomware that affected many other nations. This indicates that Nigeria was largely unscathed during this widespread attack.[47]

As a result of this attack, several banks faced dire consequences, including forced payments of exorbitant ransoms to regain access to their vital data. Others suffered extensive service disruptions, leading to a loss of customer trust, significant financial losses, and costly recovery efforts as systems needed to be restored and secured against future threats. The WannaCry incident underscored the urgency for banks to strengthen their cybersecurity measures and develop robust response strategies to protect against the evolving landscape of cyber threats.[48]

4.4 Insider Threats

Not all threats to a bank's security come from outside its premises; a considerable and often underestimated risk resides within the organisation itself, known as insider threats. These threats can emerge from a variety of individuals, such as unhappy employees seeking revenge, contractors with access to sensitive information, or third-party vendors involved in the bank's operations. Insiders possess a level of access that allows them to interact with critical systems and sensitive data, making it possible for them to unintentionally or deliberately compromise security measures, leading to potential data leaks or unauthorised access methods that can be exploited by external attackers.[49]

A striking illustration of the dangers of insider threats unfolded in 2019 when Capital One, one of the largest financial institutions in the United States, became the target of a significant data breach. The breach was carried out by Paige Thompson, a former employee of Amazon Web Services, who discovered and maliciously exploited a security vulnerability in Capital One's cloud infrastructure. Armed with her knowledge of cloud technologies, Thompson gained unauthorised

---

[47] Zakariyya Adaramola, 'How Nigeria Escaped 'WannaCry' Cyber-Attack', (Daily Trust, 21st May 2017) https://dailytrust.com/how-nigeria-escaped-wannacry-cyber-attack/ accessed 10th January 2025.

[48] D. Dahlberg, 'How the Impact of WannaCry Ransomware Was Felt Around the World', https://www.bitsight.com/blog/assessing-the-global-impact-of-wannacry-ransomware accessed 10th January 2025.

[49] See Claire dela Luna, (n4) supra.

access to a staggering volume of sensitive customer information, affecting over 100 million people.[50]

The compromised data was deeply personal and included critical details such as Social Security numbers, credit scores, bank account information, and even transaction history. The fallout from this breach was extensive and severe, not only jeopardising the financial security of millions of customers but also shaking public trust in Capital One. It led to a cascade of legal actions, as various regulatory bodies intervened to hold the bank accountable for its cybersecurity shortcomings and the ineffective safeguards it had in place to protect customer data from both insider and outsider threats.[51]

In the wake of this incident, Capital One faced significant financial repercussions, including hefty fines that served as a wake-up call to the banking industry as a whole. The breach starkly illustrated the critical need for stringent access controls, comprehensive employee training programs emphasising cybersecurity awareness, and robust monitoring systems designed to detect suspicious activity within the organisation. It underscored the necessity for banks to cultivate a proactive security posture to effectively mitigate the risks posed by insider threats and to ensure the protection of sensitive client information in an increasingly interconnected digital landscape.

4.5 Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) attacks represent a significant threat to financial institutions, particularly banks. These malicious attacks involve overwhelming a bank's online services with a flood of internet traffic. As a result, the affected systems can become severely overwhelmed, leading to slowdowns or complete crashes. This renders critical services, such as online banking and payment processing, unavailable to customers and businesses alike. The implications of such

---

[50] Emma Roth, 'Former Amazon Employee Convicted Over 2019 Capital One Hack/Paige Thompson Was Found Guilty On Seven Counts Of Wire And Computer Fraud', (The Verge, 18th June 2022) https://www.theverge.com/2022/6/18/23173727/former-amazon-employee-convicted-over-2019-capital-one-hack-paige-thompson accessed 10th January 2025.

[51] R.D. Fairbank, 'Information on the Capital One Cyber Incident', https://www.capitalone.com/digital/facts2019/ accessed 10th January 2025.

attacks can be devastating, as they disrupt business operations, create immense frustration among customers, and expose the bank's systems to further vulnerabilities that could be exploited.[52]

There have been DDoS attacks on banks in Nigeria. For example, there was an attempt to hack into Guaranty Trust Bank's website, raising concerns about how secure Nigerian banks are against cyber threats.[53] The increase in DDoS attacks has led banks to work with cybersecurity firms to strengthen their defences. These incidents show that banks need better security measures to protect against such attacks.

In 2022, the landscape of cybersecurity threats to UK financial institutions intensified, with a marked increase in DDoS attacks targeting several major banks.[54] These coordinated assaults overwhelmed their online banking platforms, resulting in significant service outages. Thousands of customers found themselves unable to access their accounts for extended periods, often stretching into hours. This widespread disruption not only caused inconvenience but also generated considerable dissatisfaction, leading to reputational damage for the banks involved. The series of incidents served as a stark reminder of the ongoing and evolving threat that DDoS attacks pose to the banking sector, highlighting the critical need for robust cybersecurity measures to safeguard financial services against such vulnerabilities.[55]

4.6 Advanced Persistent Threats (APTs)

Advanced Persistent Threats (APTs) represent a highly sophisticated class of cyberattacks characterised by cybercriminals gaining unauthorised access to a bank's network and maintaining that access undetected for prolonged periods. These attackers take a stealthy approach, closely

---

[52] T. Walsh, and S. Winterfeld, 'DDoS Attacks on Financial Services Industry Up 154%, According to New FS-ISAC/Akamai Report', https://www.fsisac.com/newsroom/pr-akamai-ddos-report-2024 accessed 10th January 2025.

[53] Justice Okamgba, 'GTB Channels Attack Heightens Cybersecurity Concerns', (The Punch, 19th August 2024) https://punchng.com/gtb-channels-attack-heightens-cybersecurity-concerns/ accessed 10th January 2025.

[54] Editorial, 'DDoS Attacks on Financial Institutions: Risks, Consequences, and Prevention', (Fintech News, 29th November 2020) https://www.fintechnews.org/ddos-attacks-on-financial-institutions-risks-consequences-and-prevention/ accessed 10th January 2025.

[55] Editorial, 'UK Finance Suffers Surge in DDoS Attacks', (Finextra, 14th September 2022) https://www.finextra.com/newsarticle/40955/uk-finance-suffers-surge-in-ddos-attacks accessed 10th January 2025.

monitoring the bank's systems and gradually extracting sensitive data while compromising critical digital infrastructure. APTs are particularly aimed at larger financial institutions because these targets often possess extensive resources and valuable information, making them prime candidates for extensive disruption.[56]

The danger posed by APTs lies in their covert nature; they can remain undetected for months or even longer, which greatly enhances the threat they pose to the integrity and confidentiality of sensitive financial data. During this stealth phase, attackers can methodically harvest information, such as customer data, financial records, and intellectual property, all before the institution becomes aware of the breach.[57]

Nigerian banks have indeed faced Advanced Persistent Threat (APT) attacks, which are highly sophisticated and targeted cyber intrusions. A notable example occurred in 2016 when hackers targeted the Central Bank of Nigeria (CBN) in an APT attack.[58] The attackers attempted to steal a significant amount of money by manipulating the SWIFT payment system, a critical network used for international financial transactions. Fortunately, the attack was detected and thwarted before any funds were lost. However, this incident underscored the vulnerability of even the most secure financial institutions to advanced cyber threats, highlighting the need for continuous vigilance and robust cybersecurity measures.

A notable instance of an APT occurred in 2016 when Bangladesh's central bank became a target in a highly orchestrated cyberattack. In this incident, hackers managed to infiltrate the bank's systems and launched an audacious plan to siphon off nearly $1 billion by exploiting vulnerabilities in the SWIFT payment system, which is used globally for secure financial

---

[56] A. Wilson, (n30) supra.

[57] See Claire dela Luna, (n4) supra.

[58] Godfrey George, 'Bank Customers, Companies Lose Billions to Nigeria's Weak Cybersecurity', (The Punch, 2nd April 2023) https://punchng.com/bank-customers-companies-lose-billions-to-nigerias-weak-cybersecurity/ accessed 10th January 2025.

transactions.[59] Although a significant portion of the attempted theft was thwarted and most of the funds were recovered, the attackers successfully made off with $81 million.[60] This breach not only resulted in a substantial financial loss but also highlighted the vulnerabilities present even within some of the most secure financial institutions, underscoring the urgent need for enhanced cybersecurity measures in the financial sector.

4.7 Combating Cybersecurity Threats

To tackle cybersecurity threats, banks and financial institutions must use a combination of technology and best practices to improve their security measures.

4.7.1 Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) enhances security significantly by requiring multiple forms of verification before granting access to sensitive systems. It requires users to verify their identity in several ways, making it much harder for someone to hack into an account. These can include biometric verification such as fingerprint or facial recognition, one-time passcodes sent to a registered mobile device or email, or even hardware tokens.[61] By implementing MFA, banks can greatly reduce the likelihood of unauthorised access, as even if a password is compromised, the additional verification step acts as a vital barrier to protect sensitive information.

4.7.2. End-to-End Encryption (E2EE)

End-to-end encryption is a fundamental security measure that ensures that data remains confidential and secure throughout its entire journey. When information is transmitted, it is encrypted at the source and remains encrypted until it reaches its intended recipient. This means that even if cybercriminals manage to intercept the data while it is in transit, they would only encounter unreadable ciphertext.[62]

---

[59] R. Balu, 'Bangladesh Bank Cyber Heist: Incident Analysis', https://repository.gatech.edu/server/api/core/bitstreams/df3d1c19-47be-4738-a855-9c049b709d52/content accessed 10th January 2025.

[60] *Ibid.*

[61] M. Ibrahim, '10 Benefits of Multi-Factor Authentication (MFA)', https://supertokens.com/blog/benefits-of-multi-factor-authentication accessed 10th January 2025.

[62] https://www.aciworldwide.com/end-to-end-encryption accessed 10th January 2025.

In other words, in end-to-end encryption (E2EE), a communication system creates two sets of cryptographic keys, one public and one private, for each user, a process known as asymmetric cryptography, where public keys encrypt data and private keys decrypt it. Public keys, shared with every user on the system, lock the data through large numerical values created by an algorithm, while private keys, unique to the owner and not shared, unlock the data secured by their paired public key. The actual encryption occurs at both endpoints at the device level, whether it is a mobile device, a point of sale device, or a personal computer.[63]

The E2EE process involves five steps: key generation, key exchange, encryption, transmission, and decryption. For example, if Tom wants to send Stella payment information, he encrypts it using Stella's public key, and the data remains encrypted while in transit and even when stored on a server. Hackers cannot access the information as they lack the unique private key needed to decrypt the data, and once the data reaches Stella's device, it is decrypted by her private key, allowing her to access the information. If Stella needs to respond to Tom, her message will be encrypted using Tom's public key.[64] For banks, employing robust encryption protocols to protect data both at rest (stored data) and in transit (data being transmitted) is essential to safeguarding customer information and maintaining regulatory compliance.

4.7.3. AI-Powered Threat Detection

Artificial Intelligence (AI) has emerged as a powerful tool in the field of cybersecurity, particularly when it comes to detecting and responding to threats swiftly and effectively. AI systems can process and analyse vast amounts of data in real-time, identifying unusual patterns or behaviours that may indicate a potential security breach. For instance, machine learning algorithms can recognise consistent user behaviours and flag any deviations, making them particularly useful in combating phishing attempts and fraudulent activities. By deploying AI-powered threat detection,

---

[63] *Ibid.*

[64] *Ibid.*

banks can enhance their cybersecurity posture, allowing for rapid identification and mitigation of threats before they can cause significant harm.[65]

4.7.4 Zero Trust Architecture

The Zero Trust Architecture represents a paradigm shift in cybersecurity, premised on the principle that no user, device, or network should be considered inherently trustworthy. This model mandates continuous verification at every level of access, meaning that every access request must be authenticated, authorised, and encrypted. Implementing a Zero Trust framework requires a comprehensive and strong network security architecture that controls and monitors all connections within the system. By doing so, banks can effectively prevent unauthorised access, minimise the risk of data breaches, and ensure that even in compromised environments, sensitive data remains protected.[66]

4.7.5 Security Incident and Event Management (SIEM) Systems

Security Incident and Event Management (SIEM) systems play a crucial role in the modern cybersecurity landscape, as they aggregate and analyse security data from various sources within an organisation. These systems provide real-time monitoring and alerting, allowing security teams to quickly identify and respond to potential threats.[67] By correlating events and logs from firewalls, intrusion detection systems, and other security tools, SIEM solutions enhance situational awareness and enable a more proactive approach to threat management. The timely alerts generated by SIEM systems can lead to quicker incident response times, effectively minimising damage and disruption from cyberattacks.

5. Conclusion and Recommendations

Cybercrime is becoming more advanced, which means banks need better security measures now more than ever. Many older banking systems, built years ago, struggle to handle today's

---

[65] W. Poole, 'The Role of AI in Evolving Cybersecurity Attacks', https://www.cyberdefensemagazine.com/the-role-of-ai-in-evolving-cybersecurity-attacks/ accessed 10th January 2025.

[66] S. Rose, and O. Borchert, and S. Mitchell, and S. Connelly, 'Zero Trust Architecture', https://doi.org/10.6028/NIST.SP.800-207 accessed 10th January 2025.

[67] https://www.ibm.com/think/topics/siem accessed 10th January 2025.

cybersecurity threats. These outdated systems often have weaknesses because they were not designed to support modern security standards. To effectively tackle the numerous cybersecurity challenges that modern banking faces, it is crucial for financial institutions to migrate to more advanced and cutting-edge technology systems. This migration is not just a cosmetic upgrade; it involves a comprehensive overhaul of existing infrastructure, allowing banks to significantly enhance their security frameworks.

It is therefore recommended that, by implementing robust encryption methods, banks can safeguard sensitive customer data against unauthorised access and breaches. Encryption transforms data into a format that can only be read by someone with the correct decryption key, making it much more difficult for cybercriminals to exploit vulnerabilities.

Also, the incorporation of multi-factor authentication (MFA) adds another layer of protection. MFA requires users to verify their identity through multiple forms of verification, such as passwords combined with biometric scans or temporary codes sent to mobile devices. This method significantly reduces the likelihood of unauthorised access, even if passwords are compromised.

Moreover, upgrading to advanced systems enables real-time threat detection capabilities. These systems utilise sophisticated algorithms and machine learning techniques to monitor transactions and user behaviour, allowing for the immediate identification of any discrepancies or unusual activities. This proactive approach not only helps in quickly mitigating potential threats but also enhances the institution's ability to respond and adapt to emerging security challenges.

Modern systems are designed with a focus on data protection and regulatory compliance, ensuring that customer information is safeguarded against unauthorised access and breaches. By adopting newer technologies, banks can enhance their ability to track, analyse, and respond to cybersecurity

incidents swiftly, ultimately preserving the trust and confidence of their customers in an increasingly digitised world.[68]

In summary, the importance of cybersecurity in the banking industry cannot be overstated. It is imperative for banks to prioritise cybersecurity not just as a reactive measure but as a proactive strategy to secure their operations, protect their customers, and sustain their reputation in an increasingly digitised financial landscape.

[68] C. Aguwa, 'Why Nigerian Banks are Migrating to a New Core Banking System', (Nigerian Fact, 15th October 2024) < https://nigerianfact.com/why-nigerian-banks-are-migrating-to-a-new-core-banking-system/> accessed 7th January 2025.