TEMPLARS
NIGERIA | GHANA

26 February 2025

Key contacts

Emmanuel Gbahabo
Partner and Head,
Investigations, White Collar, & Compliance and Dispute Resolution
Emmanuel.gbahabo@templars-law.com

Onyedikachi Uneke
Associate,
Corporate & Commercial
onyedikachi.uneke@templars-law.com

TEMPLARS ThoughtLab

Cybersecurity Incident Response and Crisis Management Framework in Nigeria

Introduction

Nigeria's digital economy has experienced rapid growth with the rise of internet banking, mobile payments, and e-commerce. However, this progress has also brought about significant cybersecurity challenges, posing risks to business operations, data integrity, and customer trust. Businesses now face a surge in cybercrimes such as internet fraud, ransomware attacks, hacking, and privacy breaches which threaten both financial stability and brand reputation.

This article explores Nigeria's cybersecurity landscape with a focus on incident response mechanisms and crisis management frameworks tailored for businesses. It underscores the importance of adopting strategies that combine advanced technological solutions, effective policies, and stakeholder collaboration to enhance organizational resilience against cyber threats.

Overview of Cybersecurity Challenges in Nigeria

Nigeria's rapidly advancing digital landscape poses significant cybersecurity challenges that threaten the resilience of its economy and societal infrastructure. The increasing reliance on technology across various sectors enhances their vulnerability, as many businesses lack the resources and expertise to implement effective cybersecurity measures. According to the Central Bank of Nigeria (CBN), a staggering 70% of attempted or successful fraud/forgery cases in the Nigerian banking system stem from electronic channels. Perpetrators increasingly exploit the proliferation of online transactions, e-commerce platforms, and electronic messaging systems to engage in illicit activities[1]. According to reports from the Nigerian Communications Commission (NCC), cybercrime costs Nigeria approximately $500 million annually. Key drivers of this cybersecurity threat include low cybersecurity awareness, inadequate infrastructure and weak regulatory enforcement. The rise in cyber threats, ranging from data breaches to ransomware

[1] ThisDay, 'Beyond amending the Cybercrime Act' Available at: https://www.thisdaylive.com/index.php/2024/03/05/beyond-amending-the-cybercrime-act (accessed on January 8,2025).

attacks, underscores the need for a robust incident response strategy. The transnational nature of cybercrime complicates the security landscape, making Nigeria an attractive target for malicious actors seeking to exploit its burgeoning internet user base[2]. These circumstances demand not only innovation in response strategies but also a comprehensive framework for cybersecurity crisis management.

Hacking
(Unauthorized Access)
Up to 7 years imprisonment
or N7 million fine

Phishing
(Impersonation & Fraudulent Communications)
3 years imprisonment
or N1 million fine

Malware Attacks
(Viruses, Ransomware, Spyware)
3 years imprisonment or
N1 million fine

Legal Framework for Cybersecurity Incidents Monitoring, Detection, Prevention, Mitigation and Management in Nigeria

The increasing reliance on digital infrastructure in Nigeria has heightened the need for a robust legal framework to address cybersecurity challenges. As cyber threats evolve, organizations and individuals face risks ranging from data breaches to critical infrastructure attacks. To safeguard national security, economic stability, and individual privacy, Nigeria has implemented legal measures that govern the monitoring, detection, prevention, mitigation, and management of cyber incidents. Notably, the Cybercrimes (Prohibition and Prevention etc.) (Amendment) Act 2024 (the "Cybercrimes Act") is instrumental in the fight against cybersecurity in Nigeria. The following activities which constitute offences under the Cybercrimes Act:

a. **Hacking (i.e. unauthorised access)**

Under Section 6(2) of the Cybercrimes Act, it is an offence where any person who, with the intent to commit an offence obtains computer data, secure access to any program, commercial or industrial secrets or classified information without authorisation. The maximum penalty for this offence in Nigeria is imprisonment for a term of not more than seven years, a fine of not more than ₦7 million, or both such fine and imprisonment.[3]

b. **Phishing**

It is an offence for anyone to attempt to obtain sensitive information such as usernames, passwords, or credit card details by masquerading as a trustworthy entity in electronic

[2] Nweze-Iloekwe, Nnesochi. 2022. "The Legal and Regulatory Aspect of International Cybercrime and Cybersecurity: Limits and Challenges". GGU Law Digital Commons. doi: https://core.ac.uk/download/524150762.pdf (accessed on January 8, 2025).
[3]Additionally, Section 12 of the Cybercrimes Act makes it an offence for any person, without authorization, to intentionally intercept, by technical means, non-public transmissions of computer data, content, or traffic data. This includes electromagnetic emissions or signals from a computer, computer system, or network carrying or emitting signals to or from a computer, computer system, or connected system or network. The penalty for this offence is imprisonment for a term of not more than two years or a fine of not more than ₦5 million, or both such fine and imprisonment; Section 13 of the Cybercrimes Act makes it an offence for any person to knowingly access any computer or network and input, alter, delete, or suppress any data, resulting in inauthentic data, with the intention that such data will be considered or acted upon as authentic or genuine, regardless of whether the data is directly readable or intelligible. The penalty for this offence is imprisonment for a term of not less than three years or a fine of not less than ₦7 million, or both such fine and imprisonment.

communications. This includes using emails or instant messaging to impersonate, and deceive users to change their password, or disclosing their identity with the intent of later using this information to commit fraud.[4]

The maximum penalty for this offence is imprisonment for a term of three years, a fine of ₦1 million, or both. An example of prosecution of this offence happened on 21 August 2024, the Economic and Financial Crimes Commission ("EFCC") convicted four suspected fraudsters, following their arrest by the EFCC, for impersonation, phishing and hacking of email accounts[5].

c. **Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)**

Section 32 (3) of the Cybercrimes Act makes it an offence for any person to engage in the malicious or deliberate spread of viruses or any malware that causes damage to critical information in public, private or financial institution's computers.

The maximum penalty for this offence is imprisonment for a term of three years, a fine of ₦1 million, or both. An example of prosecution of this offence occurred on June 2022, a suspected fraudster was convicted by a High Court Judge in Lagos following prosecution by the EFCC.

Reporting Obligations

By virtue of Section 21 (1) of the Cybercrimes Act, any person or institution, who operates a computer system or a network, whether public or private, must immediately inform the National Computer Emergency Response Team ("CERT") Coordination Centre through their respective sectoral CERTs or sectoral Security Operations Centres ("SOC") of any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network, so that the National CERT can take the necessary measures to tackle the issues. In such cases, and in order to protect computer systems and networks, the National CERT Coordination Centre may propose the isolation of affected computer systems or network pending the resolution of the issues.

Section 40 (2) of the Nigeria Data Protection Act, 2023 ("NDPA") requires data controllers or processors, to notify the Nigeria Data Protection Commission ("NDPC") within 72 hours of becoming aware of a data breach incident. Non-compliance by data controllers and processors with this obligation attracts fines and possible criminal action against the defaulting data controller or processor. Under the NDPA, Data Controllers or Processors of Major Importance ("DCMIs/DPMIs")[6] that are found to have breached this provision may be subject to the payment of a fine of between the sum of ₦10 million or 2% of its annual gross revenue from the preceding financial year, whichever is greater. Similarly, other data controllers or processors not of major importance may be liable to pay a fine of whichever is greater between the sum of ₦2 million or 2% of their annual gross revenue from the preceding financial year.[7]

[4] Under Section 32 of the Cybercrimes Act.
[5] https://www.efcc.gov.ng/efcc/news-and-information/news-release/10327-abuja-court-jails-four-internet-fraudsters-in-abuja (accessed on January 8, 2025).
[6] The Guidance Notice issued by the NDPC on February 14, 2024 classifies DCMIs/DPMIs into 3 categories as follows: i) Major Data Processing-Ultra High Level: This includes commercial banks operating at the national or regional level, telecommunication companies, insurance companies, multinational companies, oil and gas companies, any organisation that processes personal data of over 5,000 data subjects in 6 months etc; ii) Major Data Processing-Extra High Level: This includes microfinance banks, higher institutions, hospitals providing tertiary or secondary medical services, mortgage banks any organisation that processes personal data of over 1,000 data subjects within 6 months etc and iii) Major Data Processing-Ordinary High Level: This includes small and medium-scale enterprises, primary and secondary schools; primary health centres, any organisation that processes personal data of over 200 data subjects within 6 months etc.
[7] Section 48 of the NDPA

In the same vein, Article 4.3 of the Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions 2022 requires a report of the cybersecurity self-assessment signed by the Chief Information Security Officer ("CISO") to be submitted every year on or before 31 March to the director and Other Financial Institutions Supervision Department of the CBN. Other Financial Institutions ("OFIs") are also required to promptly report all potential cyber-threats to their information assets, to the director.

Incident Response and Crisis Management Framework in Nigeria

Nigeria's reliance on digital infrastructure necessitates a strong cybersecurity incident response and crisis management framework. Rooted in the Cybercrimes Act, Nigeria's framework for incident response provides guidelines for reporting and managing cyber threats. Agencies like the Nigerian Computer Emergency Response Team (ngCERT) coordinate responses, facilitate real-time threat intelligence sharing, and promote crisis communication. Furthermore, the framework emphasizes the importance of preparedness measures which include cybersecurity awareness, capacity building, and incident response drills.

Crisis management extends beyond immediate containment to include post-incident recovery and resilience building. This involves conducting forensic investigations, updating security protocols, and implementing lessons learned to prevent future incidents. Nigeria's cybersecurity incident response and crisis management framework underscores the importance of a proactive, collaborative, and adaptive approach to navigating the complexities of the modern cyber threat landscape.

Strengthening Cybersecurity: Developing a Cyber Incident Response Plan and Effectively Managing Cyber Incidents in Nigeria

In today's digital world, understanding cyber incidents is critical to protecting organizational assets and maintaining operational resilience. With cyber threats evolving rapidly, organizations face unique challenges that demand a thorough understanding of potential risks. From data breaches to ransomware attacks, every cyber incident carries distinct implications, underscoring the need for robust incident response strategies. The following steps can serve as an effective guide to address, manage, and understand cyber incidents[8]:

a. Gaining Insights into Cyber Incidents

Mitigating cyber incidents requires a strategic, proactive approach to uncover system vulnerabilities that could lead to financial, reputational, and legal damages. Comprehensive incident impact assessments are essential for identifying vulnerabilities, evaluating potential outcomes, and prioritizing threats based on severity, ensuring effective resource allocation. To stay ahead of evolving threats, organizations must remain vigilant, continuously monitoring cyber risk trends and adapting response strategies. Additionally, addressing human error-a persistent vulnerability—through targeted employee training and awareness programs is vital. Building a culture of cybersecurity enhances resilience and significantly reduces the risk of successful attacks, positioning organizations to better withstand cyber threats.

b. The Value of a Strong Response Plan

A robust cybersecurity response plan is crucial for building resilience, reducing risks, and minimizing disruptions caused by cyber incidents. By clearly outlining roles, responsibilities, and communication channels, businesses and organizations can act swiftly and maintain stakeholder confidence during a crisis. To stay effective, these plans should be regularly reviewed and updated to incorporate new threats and lessons learned from past incidents. Incorporating established frameworks—such as the NIST Cybersecurity Framework, ISO/IEC 27001 for systematic management of sensitive information, COBIT for aligning IT with business goals, ENISA Cybersecurity Policies, and guidelines from the Center for Internet Security (CIS) for enhancing cybersecurity resilience and risk management. These frameworks provide a structured approach to managing all phases of incident response, from preparation to post-incident review.

c. Building a Resilient Incident Response Team

An effective incident response plan relies on a skilled, well-coordinated team, with clearly defined roles and regular training exercises to enhance collaboration and readiness. Simulations of real-world scenarios improve both technical skills and team dynamics under pressure. Involving key stakeholders in planning ensures alignment with organizational goals and proper resource allocation. Continuous improvement is achieved by measuring

https://novatiaconsulting.com/cyber-incident-response-planning-in-nigeria/ (accessed on January 8, 2025)

readiness through performance metrics and post-incident assessments, ensuring preparedness for evolving cyber threats.

d. **Having an effective Incident Response Policy**

An Incident Response Policy, aligned with global frameworks like ISO/IEC 27001, provides a structured approach to identifying, managing, and mitigating cyber incidents. In the same vein, regular policy updates are necessary to address evolving threats, fostering a culture of vigilance and compliance for a strong defensive posture.

e. **Learning from incidents and regular training and awareness programs**
Every cyber incident presents an opportunity for improvement. Post-incident analysis helps identify vulnerabilities and evaluate the effectiveness of responses, with lessons learned used to refine strategies and strengthen defences. Ongoing training and awareness programs are also vital in building a cybersecurity-conscious workforce. Tailored workshops and real-world scenarios empower employees to recognize threats and respond appropriately, while regular evaluations ensure the programs remain impactful and relevant

f. **Navigating Legal and Compliance Requirements**

Compliance with data protection regulations is a critical aspect of incident response. Organizations must establish mechanisms for timely breach notifications and adhere to regulatory obligations to avoid penalties and maintain trust. Integrating legal considerations into response plans ensures preparedness for both technical and compliance challenges.

g. **Leveraging Technology and Continuous Improvement**

Advanced technologies like threat intelligence tools and automated response systems improve incident detection and management by reducing reaction times and minimizing errors. Regular simulations and forensic analyses enhance preparedness, while continuous improvement through incident analysis and feedback-driven changes ensures adaptation to evolving threats. Performance metrics offer insights to refine strategies and strengthen resilience.

Role of Lawyers in Cyber Security

Businesses organizations should promptly involve their lawyers in incident response activities to ensure that they proactively comply with cybersecurity laws and regulations, and to assist with crafting clear policies and frameworks to prevent vulnerabilities and mitigate risks. The legal team can provide guidance on developing and executing effective incident response plans, ensuring timely reporting and adherence to legal obligations during cyber crises. Furthermore, lawyers can champion crisis management efforts by advocating for robust enforcement measures, collaborating with law enforcement, and equipping organizations with the tools and knowledge to withstand and recover from cyber threats.[9]

[9] Article 5 of the Nigeria Bar Association Cybersecurity Guideline, 2024 mandates lawyers and legal organizations to secure network configurations against unauthorized access and cyber threats. This includes implementing firewalls, intrusion detection systems, and secure protocols like VPNs for remote access.

Recommendations For Business Cybersecurity Resilience

To survive cyber incidents and build long-term resilience, businesses must take proactive steps to enhance their cybersecurity posture. Below are key measures organizations should implement to survive cyber incidents and build long-term resilience, businesses must take proactive steps to enhance their cybersecurity posture. Below are key measures organizations should implement:

a. **Stay Informed About Cyber Threats and Trends**

Businesses must consistently monitor the evolving cyber threat landscape, keeping up with trends such as ransomware attacks, phishing techniques, and newly discovered vulnerabilities. This includes subscribing to threat intelligence services, attending cybersecurity conferences, and engaging with industry groups.

b. **Develop a Comprehensive Cybersecurity Framework**

Organizations should adopt recognized frameworks like ISO/IEC 27001, NIST Cybersecurity Framework, and ENISA guidelines to structure their security policies and response plans effectively.

c. **Implement a Multi-Layered Defence Strategy**

Businesses should use multiple security layers, including firewalls, antivirus software, and intrusion detection systems, to protect against cyber threats. Relatedly, businesses should utilize endpoint security solutions to protect individual devices, ensuring that every access point within the network remains secure. A zero-trust security model should also be adopted, which requires continuous authentication and verification before granting access to sensitive systems, significantly reducing the risk of unauthorized breaches.

d. **Regularly Train Employees on Cybersecurity Awareness**

Since human error is a major cybersecurity risk, businesses must invest in continuous employee training to enhance security awareness. Training programs should also emphasize safe browsing habits, the importance of strong password management, and the use of password managers to store credentials securely. Additionally, clear incident reporting procedures should be established, ensuring that employees know how to report potential security threats immediately, minimizing the impact of cyber incidents before they escalate.

e. **Establish a Robust Incident Response Plan**

Businesses should incorporate a well-defined incident response plan which assigns clear roles and responsibilities and includes a crisis communication process to manage interactions with both internal stakeholders, such as employees and executives, and external parties, including customers, regulatory bodies, and the media. To guarantee its effectiveness, the incident response plan should be regularly tested through tabletop exercises and real-world simulations, allowing organizations to identify weaknesses and refine their response strategies proactively.

f. **Secure Critical Business and Customer Data After a Cyber Incident**

Following a cyber incident, businesses must take immediate action to secure critical data and prevent future breaches. Implementing strong encryption for stored and transmitted data ensures that any stolen information remains unusable to attackers. Multi-factor authentication (MFA) should be enforced across all systems to strengthen access controls and reduce the risk of unauthorized logins. Additionally, businesses must conduct a thorough data integrity assessment, identifying compromised assets and restoring affected systems using secure offline backups. Regular audits and post-incident forensic analysis should be performed to understand attack vectors and enhance security measures, ensuring long-term data protection and business continuity.

Conclusion

Navigating Nigeria's complex cybersecurity landscape requires a strategy that combines robust legal frameworks, advanced technological measures, and proactive stakeholder engagement. The way forward involves both public and private sectors working collaboratively to bolster incident response and crisis management efforts. Businesses must prioritize the strengthening of their digital infrastructure by investing in effective cybersecurity measures, regular workforce training, and continuous system updates to safeguard sensitive data and maintain stakeholder trust. This proactive approach not only ensures compliance with evolving legal requirements but also helps mitigate risks that can otherwise lead to significant financial losses and reputational damage.

Lawyers play a pivotal role in this ecosystem by guiding organizations through the intricacies of regulatory compliance, drafting and enforcing robust cybersecurity policies, and managing breach notifications and liability issues during cyber incidents. Their expertise ensures that companies not only adhere to stringent data protection laws but also effectively navigate the legal implications of cyber threats. Ultimately, these efforts matter to businesses because they underpin operational resilience, enhance customer confidence, and secure the foundation for sustainable growth in Nigeria's rapidly expanding digital economy.