TEMPLARS
NIGERIA | GHANA

14 April 2026

Key contacts

Ronke Sokefun
Partner,
Corporate
and Commercial
ronke.sokefun
@templars-law.com

Francis Jarigo
Associate,
Corporate
and Commercial
francis.jarigo
@templars-law.com

Onyinye Omenugha
Associate,
Corporate
and Commercial
onyinye.omenugha
@templars-law.com

TEMPLARS ThoughtLab

Cybersecurity Failures and Board Liability:

What Directors and Executives Must Know

Introduction

In today's digitally driven economy, cyberattacks[1] have evolved from peripheral risks into existential corporate concerns. Such incidents do far more than disrupt systems: they erode shareholder value, trigger multi-jurisdictional regulatory investigations, and increasingly expose directors to personal litigation, reputational damage, and potential disqualification from office. Digital security has accordingly become a paramount boardroom priority, with affected parties and stakeholders directing scrutiny at the board itself by demanding answers on oversight failures, risk management lapses, and due diligence deficiencies.

A critical question often is, when a cyber incident occurs in an organisation, who bears liability for such a breach? Is it the organisation? Its executives? Or the hackers who are often unknown and undetectable? While the organisation would often bear the economic loss from such an attack, it is noteworthy that its executives can also be exposed to regulatory fines or penalty under Nigerian law for inadequate preventive measures. Board executives and directors are therefore no longer passive recipients of cyber risk: they are expected to exercise active oversight of the systems, policies, and controls designed to safeguard their organisations.

Premised on this backdrop, this article examines the liability of board executives for cyberattacks or cybersecurity failures under Nigerian law, the responsibility on senior management to ensure that adequate cybersecurity measures are implemented and maintained in organisations, and the legal exposure the are likely to face when cyber incidents occur. The article also offers risk mitigation tips or measures that may be adopted by board executives and/or businesses to minimise or avoid liability from cyberattacks or cybersecurity breaches.

[1] For the purposes of this article, "cyberattack" refers to any deliberate, unauthorised attempt to access, disrupt, damage, or otherwise compromise computer systems, networks, or digital infrastructure, whether by external threat actors or malicious insiders.

Can Board Executives Be Liable for Cybersecurity Failures in Nigeria? And in What Instances?

Board executives can be held liable for cybersecurity failures in Nigeria. However, their liability depends on how the failure occurred and whether the executives were negligent, complicit or failed in their legal duties. Their liability can arise under the following legal framework:

a. **The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (as amended**) (**Cybercrimes Act**), which is Nigeria's primary legislation for combating cybercrimes creates a framework that directly mandates cybersecurity controls by criminalising unsafe practices and requiring organisations to put protective measures in place. Where a corporate body commits an offence under the Act and it is shown to have been committed with the consent, connivance, or attributable neglect of a director, manager, secretary, or similar officer, that individual, alongside the company, will be liable to prosecution and punishment.[2]

b. **The Nigeria Data Protection Act (NDPA) 2023,** in addition to directly requiring organisations (data controllers and processors[3]) to implement robust security measures as part of their statutory duties, provides legal basis that could warrant personal liability of an organisation's leadership where the organisation contravenes its provisions[4]. Under the NDPA, data controllers and processors are legally obligated to implement appropriate technical and administrative security measures to safeguard personal data against unauthorised access, accidental loss, destruction, disclosure, alteration, misuse, or similar harms that could result from a breach[5]. Therefore, where breaches occur in circumstances suggesting neglect, failure of oversight, or inadequate governance structures, board executives of the affected organisations are likely to face civil liability or regulatory sanction[6], as would the organisation.

c. **The CBN Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Banks (PSBs), 2024 (the "Framework")**, represents the minimum requirements to be put in place by all DMBs and PSBs in their respective cybersecurity structures. The Framework specifically provides for Cybersecurity Governance and Oversight, which sets the agenda and boundaries for cybersecurity management and controls. The Framework requires the Board and Senior Management of all supervised financial institutions[7] to comply with all relevant statutes and regulatory requirements on cybersecurity including the Cybercrimes Act, NDPA, and other relevant laws[8]. Non-compliance with the provisions of the framework attracts financial penalties of not less than ₦2,000,000 (Two Million Naira) on the officers (board executives) of the erring entity and an additional penalty of ₦50,000 (Fifty Thousand Naira) for each day of continued default.[9]

---

[2] Section 29(2) of the Cybercrimes Act, 2015
[3] Section 65 of the NDPA defines: a data controller means as "an individual, private entity, public commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data". It further defines a data processor "an individual, private entity, public authority, or any other body, who processes personal data on behalf of or at the direction of a data controller or another data processor".
[4] Section 53 (1) of the NDPA.
[5] Section 39 of the NDPA 2023
[6] *Ibid*
[7] Including commercial banks, merchant banks, non-interest banks, microfinance banks, primary mortgage banks, payment service banks, development finance institutions, discount houses, finance companies, and bureaux-de-change | CBN website: https://www.cbn.gov.ng/supervision/finstitutions.html#:~:text=The%20Central%20Bank%20of%20Nigeria,Payments%20System%20Supervision> accessed 13 March 2026.
[8] Clause 6.0 (1) of the CBN Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Banks (PSBs), 2024
[9] Clause 6.0(3) of the framework references the provisions of the Banking and Other Financial Institutions Act, 2020, mandating all banks and other regulated entities to strictly comply with the cybersecurity regulations and guidelines made by the CBN. Specifically, section 68 (3) of the Act provides that any officer of a bank, specialised bank or other financial institution who, through an action or omission, fails to comply

Naira) on the officers (board executives) of the erring entity and an additional penalty of ₦50,000 (Fifty Thousand Naira) for each day of continued default.[10]

d. **Companies and Allied Matters Act, 2020 (CAMA):** under CAMA[11], directors[12] owe fiduciary duties to the members of the company, to act in good faith and exercise reasonable care and diligence in managing the affairs of the company[13]. In the event a cyber breach occurs, regulators, and shareholders may scrutinise whether the board of directors exercised reasonable oversight, such as ensuring adequate security controls. If directors ignored the implementation of basic technical and administrative measures, they may face allegations that they breached their duty of care. By contrast, directors that show oversight and documented cyber risk governance are better positioned to show that they fulfilled their fiduciary obligations even when a breach occurs[14].

e. **Common Law Duty of Care/Tort of Negligence:** Nigerian courts have generally approached cyber-related losses through the lens of duty of care and contractual responsibility, rather than treating hacker intervention as a complete defence. In *Old Generation Bank v. 54 Banks*[15] for instance, the Federal High Court ordered 54 (fifty-four) different banks[16] to return approximately ₦9.3 billion that was fraudulently transferred from an unnamed, old generation bank account by hackers.

f. **Liability under Contract/Contractual Responsibility:** where cybersecurity related contracts entered into between an organisation and a contractual counter party enables such a party to sustain a claim against the organisation and its executives in the event of a cyber-attack or cybersecurity breach that occasions damage or harm to such a party, then the organisation and its executives would be liable.

Essentially, the current legal regime requires boardroom executives to prioritise and ensure that their cybersecurity architecture is robust to prevent cyberattacks or risk facing liability. As noted earlier, besides the financial losses that an organisation will suffer in the event of a cyberattack, board executives, especially those at the leadership level may be personally liable. Executives and board members are no longer passive observers of cybersecurity risk; they are active legal bearers of responsibility.

---

with the section shall be liable to a penalty of not less than ₦2,000,000 and an additional penalty of ₦50,000 for each day during which such offence continues.

[10] Clause 6.0(3) of the framework references the provisions of the Banking and Other Financial Institutions Act, 2020, mandating all banks and other regulated entities to strictly comply with the cybersecurity regulations and guidelines made by the CBN. Specifically, section 68 (3) of the Act provides that any officer of a bank, specialised bank or other financial institution who, through an action or omission, fails to comply with the section shall be liable to a penalty of not less than ₦2,000,000 and an additional penalty of ₦50,000 for each day during which such offence continues.

[11] Section 305 of CAMA

[12] All directors including Executive Directors, Non-Executive Directors, and Independent Non-Executive Directors.

[13] Section 308 of CAMA

[14] A director may demonstrate the exercise of proper oversight by showing that appropriate cybersecurity policies and controls were duly implemented, that such policies were effectively complied with, and that the director acted with due care, skill, and diligence and did not act negligently.

[15] FHC/L/CS/629/2025

[16] And would have done same for their executives if it was part of the reliefs sought, and it was determined that the executives were complicit or acted negligently.

Measures That May be Implemented by Organisations to Mitigate or Prevent Liability

To mitigate risks, board executives and organisations can adopt the following:

a. **Compliance with Statutory Provisions/Responsibilities:** While compliance may not eliminate liability, it will materially reduce legal exposure and can mitigate or even defeat civil claims for damages depending on the facts. Therefore, board executives, and organisations must prioritise not just minimum compliance, but appropriate measures at every time.

b. **Internal Controls and Robust Cybersecurity Governance**: There is need for cybersecurity to be embedded into internal corporate governance structures of organisations, with board-level oversight and clear accountability for risk management. For instance, a company's strong governance framework should incorporate periodic risk assessments, investment in resilient cybersecurity systems, and alignment with best operational standards. Also, board executives should implement strict access control measures to ensure that employees can only have access to the data and systems necessary for their job functions, conduct regular audits of all network systems and monitor network traffic to detect any unusual or suspicious activities, perform thorough background checks on all employees , especially those who will have access to sensitive information or critical systems, and deploy advanced security software such as firewalls, intrusion detection systems and anti-malware tools to protect against cyber threats.

c. **Contractual Exemptions**: it is imperative that air-tight cybersecurity clauses limiting liability in situations of cyberbreaches are strategically included in onboarding agreements. So, in contracts with technology vendors for instance, service providers and partners can include tailored cybersecurity clauses that protect the organisation and its executives from cybersecurity related liability.

d. **Continuous Regulatory Engagement:** There is no doubt that regulators play a critical role in shaping expectations around cyber risk. Thus, board executives and organisations should regularly engage with legislative and regulatory developments, including updates on cybercrime and data protection laws, to ensure compliance.

e. **Cyber Insurance and Financial Hedging:** While cyber insurance will not substitute for strong controls, it can transfer certain financial exposures. Organisations should prioritise cyber insurance as it is an essential aspect of risk management. Furthermore, careful attention must be paid to the various policy requirements because coverage may be denied if minimum cybersecurity controls are not maintained[17].

f. **Continuous Training and Awareness at Leadership Level**: Cyber literacy has evolved into a core governance competency. Therefore, board executives are expected to possess a working understanding of cybersecurity risks sufficient to exercise meaningful oversight. Leadership should institutionalise periodic cybersecurity briefings to ensure that directors receive structured updates on emerging threat trends, sector-specific vulnerabilities, and the organisation's evolving risk posture.

[17]See TEMPLARS Publication on Cybersecurity Incident Response and Crisis Management Framework in Nigeria, available at: https://www.templars-law.com/app/uploads/2025/02/CYBERSECURITY-INCIDENT-RESPONSE-AND-CRISIS-MANAGEMENT-FRAMEWORK-IN-NIGERIA.pdf

Conclusion

The extant legal and regulatory framework indicates that cybersecurity has transitioned from a technical concern to a board-level governance imperative that could result in material liability to an organisation and its executives. In the corporate governance context, cyberattacks present material risks to enterprise value and impose upon boards of directors a duty to oversee cybersecurity risk management as part of their broader fiduciary obligations. Organisations and board executives that fail to establish, implement, and sustain resilient cybersecurity and data protection systems or take the necessary steps required to prevent a cybersecurity failure, will be exposed to regulatory sanctions, statutory penalties, restitution obligations, civil liabilities, and reputational damage. Consequently, boards and senior executives of organisations must treat cybersecurity compliance as a crucial obligation and a strategic priority that is required to safeguard organisations and strengthen long-term operational resilience.

Overall, organisations that adopt and enforce sound governance frameworks will not only reduce their exposure to cybersecurity related liability, but will by so doing, enhance investor confidence in their business, strengthen operational integrity, market presence, and reduce the risks of negative publicity.

If you require any further clarification, do not hesitate to contact us.