CANDELP

COMMERCIAL & ENERGY LAW PRACTICE

CYBERATTACKS AND CONTRACTUAL LIABILITY IN NIGERIA:

RISKS, RESPONSIBILITIES, AND LEGAL PREPAREDNESS

INTRODUCTION

The increasing frequency and sophistication of cyberattacks have fundamentally altered the risk landscape for businesses, financial institutions, and governments worldwide. In 2024, the global average cost of a data breach reached $4.88 million, reflecting a steady upward trend that shows no sign of abating.[1] Global cybercrime costs reached an estimated $9.22 trillion in 2024 and are projected to climb to $13.82 trillion by 2028, figures that underscore the systemic and accelerating nature of the threat and its capacity to destabilise entire economies.[2]

Nigeria is not insulated from these developments. In the first quarter of 2025 alone, Nigeria recorded over 119,000 compromised user accounts from data breaches[3]. Financial institutions have collectively lost over ₦1.1 trillion to cyberattacks over a seven-year period.[4] The Central Bank of Nigeria's Financial Stability Report 2024 revealed a 45% surge in financial fraud cases, with 70% of losses linked to digital channels, while the Nigeria Inter Bank Settlement System reported that financial institutions lost ₦52.26 billion to fraud in 2024, representing a 196% increase over the preceding five years.[5] In 2024, a Federal High Court ordered the freezing of over 800 bank accounts following the compromise of Hope Payment Service Bank's systems and the unlawful transfer of approximately ₦10 billion.[6] The Nigeria Data Protection Commission imposed a ₦555.8 million fine on Fidelity Bank Plc for data protection violations arising from non-compliant third-party processors.[7]

These incidents raise fundamental legal questions that Nigerian law is only beginning to grapple with. When a cyberattack causes a party to fail in the performance of its contractual obligations, how does the law allocate responsibility? Which party bears the loss? Do existing contractual mechanisms adequately address the risk? These questions carry significant practical implications for Nigeria's rapidly expanding digital economy, driven by fintech platforms, electronic payment systems, and digital service delivery.

This article examines the intersection of cybersecurity and contractual liability within the Nigerian legal context. It analyses the applicable legislative framework, evaluates key contractual mechanisms for allocating cyber risk, draws comparative insights from other jurisdictions, and concludes with recommendations for legal and commercial preparedness. The central argument is that cyber risk is a foreseeable and manageable legal risk that must be addressed at the contracting table, not left to chance.

EXPLAINING CYBER LIABILITY

2.1. UNDERSTANDING CYBERATTACKS

A cyberattack is any deliberate and unauthorised attempt to access, damage, disrupt, destroy, or steal data, systems, or digital infrastructure. The most prevalent forms relevant to commercial and contractual contexts are:

1. Hacking and unauthorised system access - involves intrusion into computer systems without the owner's authorisation, exploiting technical vulnerabilities or weak security controls. This was illustrated by the 2024 incident in which hackers gained unauthorised access to the systems of Hope Payment Service Bank and transferred approximately ₦10 billion, triggering a Federal High Court order freezing over 800 identified accounts in suit number FHC/ABJ/CS/1358/2024 before Justice James Omotosho.[8]
2. Ransomware - is malicious software that encrypts a victim's data or locks system access until a ransom is paid. According to the Sophos State of Ransomware 2024 report, 59% of organisations surveyed globally reported being hit by a ransomware attack in the preceding year.[9] Even where victims decline to pay, the average cost of recovery reached $5.08 million in 2025. In Nigeria, Princeps Credit Systems Limited suffered a ransomware attack by the threat group "Killsec" in 2025, demonstrating that such attacks now reach businesses of all sizes.[10]
3. Data Breaches - involve the unauthorised access or exfiltration of confidential or personal data, whether through external attacks, insider threats, or third-party negligence. The NDPA 2023 requires breach notification to the Nigeria Data Protection Commission (NDPC) within 72 hours. The ₦555.8 million fine imposed on Fidelity Bank Plc in 2024 demonstrates that the consequences extend well beyond reputational damage.[11]
4. Phishing and Social Engineering - manipulates individuals into disclosing credentials or transferring funds. According to the Verizon 2024 Data Breach Investigations Report, phishing accounts for 15% of all data breaches globally and remains a leading initial access vector for Business Email Compromise.[12]

Distributed Denial of Service (DDoS) Attacks - overwhelm systems with excessive traffic, disabling platforms and payment gateways, preventing parties from performing their contractual obligations during the disruption.

2.2. THE LEGAL DIMENSION OF CYBER LIABILITY

Cyber liability refers to the legal responsibility arising when a cyberattack causes loss or prevents the performance of an obligation. This liability may be contractual, tortious, or regulatory, and frequently all three simultaneously. A single ransomware attack on a logistics company may constitute a breach of its service level agreement, a failure to comply with data processing obligations under the NDPA 2023, and exposure to negligence claims from affected third parties.

The threat is particularly acute for smaller organisations. According to the Verizon 2025 Data Breach Investigations Report, 88% of all ransomware incidents globally involve small and medium enterprises (SMEs), organisations that are disproportionately underprepared in terms of cybersecurity infrastructure and legal readiness.[13]

NIGERIAN LEGAL FRAMEWORK

3.1. OVERVIEW

Nigeria's cybersecurity legal framework combines criminal legislation, data protection law, sector specific regulation, and general contract law principles inherited from the common law tradition. While it has evolved considerably, significant gaps remain, particularly in civil contractual liability.

3.2. THE CYBERCRIMES (PROHIBITION, PREVENTION, ETC.) ACT 2015 AS AMENDED IN 2024

The Cybercrimes Act 2015 remains Nigeria's primary instrument for combating cybercrime, criminalising hacking, computer fraud, identity theft, electronic forgery, and interference with critical infrastructure.[14] On February 28, 2024, the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024 was signed into law, introducing twelve targeted reforms. Most significantly, the Amendment Act shortened the mandatory incident reporting timeline from 7 days to 72 hours. Under Section 21(3), failure to report to the relevant sectoral Computer Emergency Response Team within 72 hours attracts denial of internet services and a mandatory fine of ₦2 million into the National Cyber Security Fund.[15] The Amendment Act also expanded the scope of payment technology offences to cover mobile money and contactless payments, [16]and introduced a 0.5% National Cybersecurity Levy on electronic transactions. While the 2015 Cybercrimes Act remains in force, the implementation of the 2024 Amendment Act was suspended by the House of Representatives in May 2024 pending further legislative review.

From a contractual standpoint, the Cybercrimes Act is primarily a criminal statute. It does not regulate the allocation of civil liability between contracting parties arising from a cyber disruption. Those questions remain governed by general contract and tort law principles.[17]

3.3. THE NIGERIA DATA PROTECTION ACT 2023 (NDPA)

The NDPA, signed into law on June 12, 2023, established the Nigeria Data Protection Commission (NDPC) as Nigeria's primary data protection authority.[18] The NDPA requires data controllers and processors to formalise their relationships through written Data Processing Agreements, flow down security obligations to sub-processors, and notify the NDPC within 72 hours of a high-risk breach.[19] Failure to comply attracts substantial regulatory consequences, as the Fidelity Bank fine illustrates.

In March 2025, the NDPC issued the General Application and Implementation Directive (GAID) 2025, effective September 2025, providing detailed operational guidance on compliance, including data breach procedures, Data Protection Officer appointments, and registration requirements.[20] Together, the NDPA and GAID constitute the primary data protection compliance framework governing contractual data processing relationships in Nigeria.

3.4. NIGERIAN CONTRACT LAW AND THE CHALLENGE OF CYBER DISRUPTION

Two common law doctrines are most relevant when a cyberattack disrupts contractual performance: force majeure and frustration. However, a balanced analysis requires that the counterarguments to these defenses be examined with equal rigour.

1. Force Majeure must be expressly provided for in a Nigerian contract before a party can rely on it. In Globe Spinning Mills (Nig.) Plc v. Reliance Textile Industries Ltd, the Court of Appeal held that a force majeure clause excuses performance on the occurrence of specified events beyond the parties' control.[21] Since cyberattacks are now widely regarded as foreseeable commercial risks, a party seeking to rely on force majeure must demonstrate that it took all reasonable preventative measures, including implementing a documented cybersecurity plan.[22]

A force majeure defence based on a cyberattack may fail where the event is not truly beyond the affected party's control. Courts may find that inadequate cybersecurity measures, such as failure to patch vulnerabilities or implement basic controls, contributed to the disruption, thereby undermining reliance on force majeure.

Second, and perhaps more fundamentally, a counterparty may argue that cyberattacks are so prevalent and well-documented that they constitute an ordinary operational risk that any commercially reasonable business should have anticipated and planned for. Courts recognise the duty to protect data where the defendant knew or ought to have known of the substantial risk,[23] This may cause the courts to view cyberattacks not as an unforeseeable catastrophe but as a predictable business risk (to be addressed through investment in security infrastructure, cyber insurance, etc.), and ignoring this signals negligence rather than grounds for excusing performance.

2. Frustration operates where a supervening event renders performance impossible or radically different from what was contemplated, without default on either side. In Nwaolisah v. Nwabufoh, the Supreme Court held that frustration arises where a contractual obligation has become incapable of being performed because the circumstances render it radically different from what was undertaken.[24] Unlike force majeure, frustration discharges the contract entirely, a consequence courts apply reluctantly. Its application to cyberattacks remains largely uncharted in Nigerian jurisprudence.

However, the doctrine of frustration will not apply where a cyberattack results from the affected party's own inadequate security, as the event cannot be said to occur without fault. In such cases, the disruption is attributable to a failure to meet the expected standard of care, exposing the party to liability (negligence or breach of contract).

There is also a growing international consensus toward stricter accountability, with directors increasingly exposed to liability for cybersecurity failures. Nigerian courts, when confronted with such cases, will balance the need to excuse genuine victims of sophisticated attacks against the need to hold accountable those whose inadequate security enabled the breach.[25]

3.5. GAPS IN JUDICIAL GUIDANCE AND STATUTORY CLARITY

The most significant challenge in Nigeria's legal framework is not the absence of legislation but the absence of judicial interpretation. Nigerian courts have yet to develop substantial case law on the civil liability consequences of cyberattacks, define the standard of cybersecurity care expected of contracting parties, or apportion liability between a business and its technology provider following a breach. Neither the Cybercrimes Act nor the NDPA directly addresses the civil contractual consequences of a cyber event. These are questions Nigerian courts will increasingly be required to address as the volume of cyber disputes grows.

OPPORTUNITIES FOR LEGAL AND BUSINESS PREPAREDNESS

The current landscape presents a substantial opportunity for businesses and legal practitioners to proactively manage cyber risk through carefully crafted contractual arrangements and institutional frameworks. Cyber risk is a legal and commercial risk that must be addressed at the contracting table.

4.1. PROACTIVE CYBER RISK MANAGEMENT THROUGH CONTRACTS

A well drafted commercial agreement can allocate risk between parties, establish standards of care, create notification obligations, and determine the consequences of a cyber incident before one occurs. Nigerian businesses entering into technology service agreements, cloud computing contracts, data processing arrangements, fintech partnerships, and supply chain agreements must treat cybersecurity provisions as substantive commercial terms, not boilerplate additions.

4.2. KEY CONTRACTUAL CLAUSES FOR CYBER RISK ALLOCATION

4.2.1. FORCE MAJEURE CLAUSES

Force majeure provisions should expressly enumerate cyberattacks, ransomware events, third-party cloud outages, and critical software vulnerabilities as qualifying events, accompanied by clear notice requirements, mitigation obligations, and termination rights activating after a defined disruption period, typically 60 to 120 days. [26]

4.2.2. CYBERSECURITY WARRANTIES

Contracts involving data handling should include express warranties requiring compliance with recognised standards such as ISO 27001 or the NIST Cybersecurity Framework, supplemented by regular audit requirements. Vague formulations such as "commercially reasonable security" offer little practical protection in litigation and should be avoided.[27]

4.2.3. INDEMNITY CLAUSES

Indemnity clauses should require the party responsible for a security breach to indemnify the innocent party against all losses, regulatory fines, investigation costs, and third-party claims. Indemnities should not be limited to gross negligence or wilful misconduct, particularly where sensitive data is involved.

4.2.4. LIABILITY CAPS

In many technology vendor contracts, liability is capped at twelve months of fees paid under the agreement. Businesses may insist that data breaches and cyber incidents be carved out from general liability caps and subject to a separate, higher cap aligned to the vendor's cyber insurance policy.[28]

4.2.5. BREACH NOTIFICATION PROVISIONS

Notification clauses should cover both suspected and confirmed incidents, specify the form and recipient of notifications, and require the notifying party to cooperate fully with any investigation. Timely notification is critical to enabling compliance with the NDPA's 72-hour regulatory reporting obligation.[29]

4.3. CYBER RISK MANAGEMENT AND CORPORATE GOVERNANCE

Effective legal preparedness requires integrating cybersecurity into broader corporate governance frameworks. Boards should treat cyber risk as a standing item on the enterprise risk register, with legal, IT, and compliance teams collaborating to assess exposure across the organisation's contract portfolio. Regular cybersecurity audits, incident response exercises, and cyber insurance procurement are all essential components of an institutionalised approach to cyber risk management. A well-structured cyber insurance policy should cover first-party losses, including business interruption and data recovery costs, as well as third-party liability from regulatory investigations and individual claims, and should align with the organisation's contractual indemnity provisions to eliminate coverage gaps.[30]

CHALLENGES AND RISKS

5.1. CROSS-BORDER JURISDICTION AND ENFORCEMENT

One of the most formidable challenges in addressing cyber liability in Nigeria is the cross-border nature of cybercrime. Cyberattacks can be planned and executed from foreign jurisdictions, making identification, prosecution, and civil redress extremely difficult. The cross-border dimension of cybercrime presents a fundamental jurisdictional challenge, as offences once confined to a single territory now frequently implicate multiple nations when perpetrated through digital networks.[31]

Nigeria's Cybercrimes Act 2015, as amended, provides a framework for international cooperation, but enforcement remains constrained by institutional weaknesses, including inadequate technical expertise, fragmented interagency collaboration, and limited digital forensic capacity.[32] While notable progress was achieved through INTERPOL's Operation Red Card between November 2024 and February 2025, which resulted in the arrest of 306 suspects across seven African countries, including Nigeria and the seizure of 1,842 devices, these operations remain largely externally driven interventions rather than outcomes of domestic institutional capacity.[33] For businesses seeking contractual redress against foreign perpetrators, the practical prospects of enforcement remain limited.

5.2. INTERPRETATION DIFFICULTIES IN DIGITAL CONTRACTS

Nigerian courts are yet to develop clear interpretive standards for automated or digital contracts. As commercial transactions increasingly migrate to electronic platforms, questions arise regarding offer and acceptance in automated systems, the legal status of smart contracts, and the evidentiary weight of digital transaction records. While the Evidence Act 2011 provides for the admissibility of electronic evidence under Section 84, the judicial application of these provisions to complex digital contractual disputes is underdeveloped. Courts may struggle to determine, for example, at precisely what point a ransomware-induced system failure constitutes a breach of a cloud service agreement, or whether a temporary Distributed Denial of Service (DDoS) attack that disrupts a payment gateway triggers a force majeure or constitutes an actionable breach.

5.3 PRACTICAL RISKS FOR SMALL AND MEDIUM ENTERPRISES

Small and medium enterprises face disproportionate cyber risk with the least capacity to manage their legal consequences. Many SMEs operate without dedicated legal counsel, cybersecurity clauses in their commercial agreements, or cyber insurance. According to the NIBSS Fraud Report 2024, attempted fraud cases increased by 338% between 2023 and 2024, and fraud losses surged by 196% over five years, with the majority of victims being individuals and businesses without adequate institutional infrastructure to respond effectively.[34] The legal and financial consequences of a cyber incident for an underprepared SME can be catastrophic, particularly where contractual counterparties seek to hold them liable for data breaches or service failures caused by attacks on their systems.

COMPARATIVE INSIGHTS

6.1. UNITED KINGDOM

Nigeria and the United Kingdom share a common law foundation and, broadly, a similar legislative instinct in approaching cybersecurity through a combination of criminal law, data protection obligations, and sector-specific regulatory frameworks. However, the two jurisdictions diverge significantly in both the depth of their regulatory architecture and the maturity of their judicial engagement with cyber liability.

While Nigeria's cybersecurity regime emphasises criminal enforcement and data protection, the UK employs a more sophisticated, sector-specific regulatory model with enforceable standards and evolving legislative scope. This divergence is most evident in enforcement, where UK jurisprudence has established clear liability for cybersecurity failures in contrast to Nigeria's absence of comparable case law, leaving regulatory expectations less defined. In the UK case of Information Commissioner's Office (ICO) v. Advanced Computer Software Group Ltd and its Group Entities[35] the ICO fined Advanced £3.08 million for a ransomware breach caused by poor security, establishing for the first time that data processors can be held directly liable for cybersecurity failures

6.2. THE UNITED STATES

The United States demonstrates how high-volume cyber litigation can drive contractual and legislative evolution. Ransomware-related federal court complaints increased by over 600% between 2021 and 2023, with single incidents spawning hundreds of class action lawsuits. [36] The Merck and Co. v. Ace American Insurance Co. litigation arising from the NotPetya ransomware attack, which was eventually settled in January 2024 after establishing that standard war exclusion clauses did not automatically cover state-sponsored cyberattacks, has had significant implications on how cyber losses are treated under commercial insurance policies globally.[37] The US Securities and Exchange Commission's 2023 cybersecurity disclosure rules, requiring public companies to disclose material cyber incidents within four business days, further demonstrate the trajectory towards mandatory corporate cyber transparency that Nigeria's regulatory framework is beginning to follow.

6.3. SINGAPORE

Singapore represents perhaps the most instructive model for Nigeria, given its status as a leading digital economy with a clear, well-enforced cybersecurity legal framework. The Cybersecurity (Amendment) Act 2024, which commenced on October 31, 2025, expanded Singapore's regulatory scope in four specific and instructive ways that Nigeria would do well to study.

First, The reform extends cybersecurity regulation to third-party-owned critical infrastructure, recognising reliance on external vendors and imposing corresponding obligations, an approach particularly relevant to Nigeria, where such outsourcing often lacks equivalent security requirements.

Second, the Amendment Act introduced the concept of Systems of Temporary Cybersecurity Concern, allowing Singapore's Cyber Security Agency to impose targeted cybersecurity requirements on specific systems during high-risk periods, such as major international events or national emergencies, without subjecting those systems to permanent regulatory oversight. [38]

Third, it designated Major Foundational Digital Infrastructure service providers, specifically cloud computing services and data center facility services, as a regulated category subject to mandatory cybersecurity codes and incident reporting obligations. [39]

Fourth, expanded incident reporting obligations now require Critical Information Infrastructure owners in Singapore to notify the Cyber Security Agency within two hours of becoming aware of a suspected cyberattack, a significantly tighter standard than Nigeria's 72-hour threshold and one that reflects the speed at which cyber incidents can cascade across interconnected systems. [40]

Each of these specific reforms offers a clear blueprint for strengthening Nigeria's cybersecurity framework.

6.4 LESSONS FOR NIGERIA

The comparative analysis yields three clear lessons. First, effective cyber regulation requires not only criminal statutes but civil enforcement mechanisms that clearly allocate contractual liability. Second, regulatory bodies must be sufficiently empowered and resourced to investigate and sanction violations consistently and publicly. Third, judicial capacity in handling cyber-related commercial disputes must be deliberately developed through specialised training, practice directions, and the encouragement of reported decisions in this field.

REGULATORY LANDSCAPE IN NIGERIA

7.1. EXISTING REGULATORY GUIDANCE

Beyond the Cybercrimes Act and the NDPA, Nigeria's cybersecurity regulatory landscape is shaped by a range of sector-specific instruments. The Central Bank of Nigeria's Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks establish sector-specific cybersecurity obligations for financial institutions, including requirements for incident response planning, vendor management, and board-level cybersecurity governance.[41] The Securities and Exchange Commission has issued guidelines addressing cybersecurity obligations for capital market operators. The Nigerian Communications Commission regulates cybersecurity obligations for telecommunications service providers. In June 2024, the President signed the Designation and Protection of Critical National Information Infrastructure Order, placing specified computer systems and networks under enhanced oversight by the Office of the National Security Adviser. [42]

7.2. GAPS IN CONTRACTUAL ALLOCATION OF CYBER RISKS

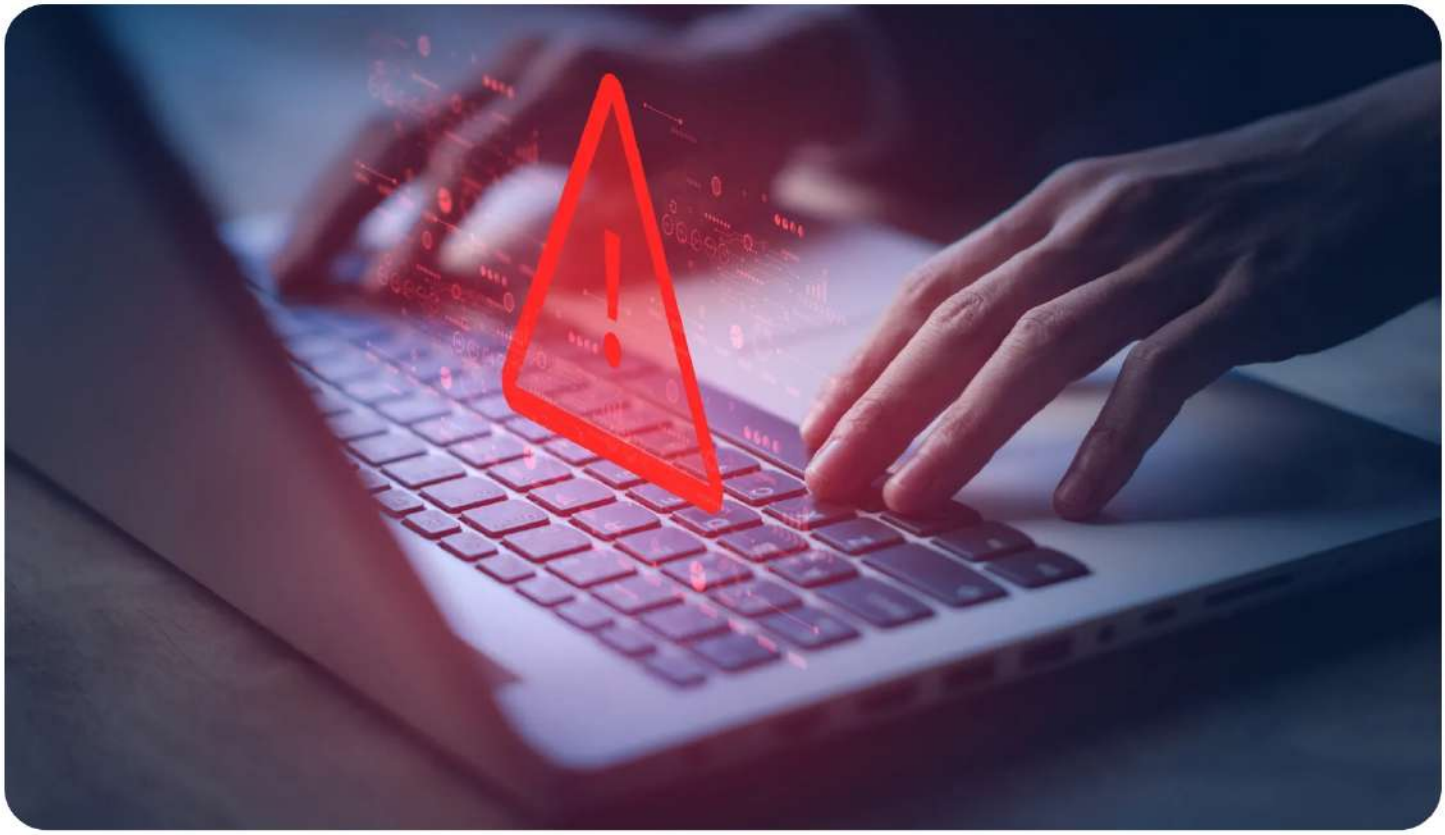
None of the existing regulatory instruments in Nigeria prescribes the specific contractual terms that businesses must include in their commercial agreements to manage cyber exposure, nor do they establish a statutory standard of contractual care for the protection of data processed under commercial arrangements beyond the Data Processing Agreement requirements of the NDPA. There is no regulatory guidance on the enforceability of liability caps in technology contracts where a data breach is involved, no prescribed minimum insurance requirements for technology service providers, and no mandatory audit or certification requirements for cloud service providers operating in Nigeria.

Whether these gaps should be addressed through prescriptive regulation or left to contractual autonomy is itself a matter of genuine debate, and a candid analysis requires that both sides be examined.

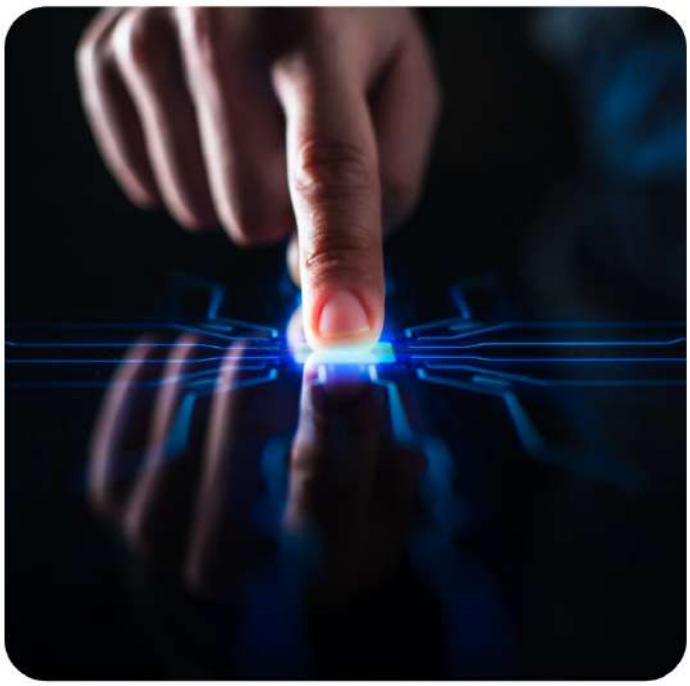
The case for regulatory intervention rests on the fact that market forces alone have not produced adequate contractual protection against cyber risk. Standard form technology contracts routinely contain liability caps that bear no relationship to the potential scale of a data breach, indemnity provisions that dissolve under scrutiny, and force majeure clauses that say nothing about ransomware. Where the parties to a commercial agreement have unequal bargaining power, as is frequently the case between a large technology vendor and a small or medium enterprise, the weaker party has little practical ability to negotiate meaningful cybersecurity protections. A regulatory floor, on this view, is not overreach. It is a correction of a market failure that is already causing measurable harm.

The case against prescriptive regulation is, however, equally compelling, and in the view of this author, ultimately more persuasive. Cybersecurity is a domain in which technology evolves at a pace that regulation structurally cannot match. A statutory instrument that prescribes specific contractual requirements, whether particular security standards, defined notification timelines, or mandatory audit mechanisms, risks being rendered obsolete before the ink is dry.[43] Prescriptive regulation also risks a one-size-fits-all approach that fails to account for the materially different risk profiles of a fintech processing millions of daily transactions, a logistics company managing supply chain data, and a small legal firm storing client files in the cloud. Sector-specific risks demand sector-specific solutions, and those solutions are more likely to emerge from sophisticated commercial negotiation within each industry than from a centralised regulatory mandate.

The more appropriate role for Nigerian regulators in this space may therefore be not to prescribe contractual content but to provide clear, non-binding guidance that businesses may draw upon as a reference point in their negotiations, while empowering the NDPC and sector-specific regulators to enforce the obligations that already exist under the NDPA and the Cybercrimes Act with greater consistency and transparency. The critical gap in Nigeria's current framework is not the absence of regulatory prescription. It is the absence of enforcement clarity and judicial precedent that tells businesses what adequate contractual cyber risk allocation actually looks like in practice.



MY PERSPECTIVE



Too many businesses in Nigeria still treat cybersecurity as someone else's problem; the IT department, the tech vendor, or some external party to handle, a mindset both dangerous and increasingly expensive.

Every day, commercial agreements are signed in Nigeria without a single clause addressing what happens when a cyberattack disrupts performance, with no force majeure provision covering ransomware, no indemnity that survives a data breach, and no notification obligation that protects either party. When something goes wrong, everyone looks for someone else to blame in a contract that was never built to answer that question.

The law in Nigeria is catching up, and the Cybercrimes Amendment Act 2024, the NDPA 2023, and the GAID 2025 are meaningful steps forward, but legislation sets the floor and not the ceiling. It is lawyers, compliance officers, and business leaders who must do the harder work of translating those statutes into contracts that actually protect their clients and organisations.

Cyber risk is not coming. It is already here, and the only question worth asking now is whether your contracts are ready for it.

RECOMMENDATIONS

Addressing cyber liability in Nigeria requires coordinated action across the legal, regulatory, and commercial landscape. No actor can close the gap alone, and the recommendations below reflect that shared responsibility.

For Businesses and Legal Practitioners: The contract remains the most immediate and accessible tool for managing cyber risk, and businesses may wish to begin by auditing their existing commercial agreements for cybersecurity gaps. Force majeure provisions, security warranties, indemnity clauses, liability caps, and breach notification obligations are all areas where targeted improvements can significantly reduce exposure. Vendors and data processors may also be subjected to cybersecurity due diligence as part of standard onboarding processes, and cyber insurance may be procured and aligned with the organisation's contractual indemnity framework to eliminate coverage gaps. Where required under the NDPA 2023 and the GAID 2025, businesses may consider appointing Data Protection Officers and documenting breach response plans that are tested and kept up to date.

For Policymakers and Regulators: The NDPC and the CBN may consider issuing supplementary guidance on the minimum contractual provisions appropriate for technology service agreements involving personal data or critical financial infrastructure. Such guidance need not be prescriptive but may serve as a practical reference point for businesses seeking to align their commercial arrangements with regulatory expectations. Investment in judicial capacity through the National Judicial Institute may also prove invaluable as the volume of cyber-related commercial disputes continues to grow. Nigeria would also benefit from accelerating its engagement with the Budapest Convention on Cybercrime, formally known as the Council of Europe Convention on Cybercrime, which entered into force on July 1, 2004. It is the first and most comprehensive international treaty specifically addressing cybercrime, with 81 states having ratified it as of August 2025.[44] Its

objectives are threefold: harmonising national laws related to cybercrime, supporting the investigation of cyber offences, and increasing international cooperation in the fight against cybercrime. Practically, accession to the Convention grants Nigeria access to a 24 hour, seven day a week network of contact points for rapid cross border assistance in cybercrime investigations, expedited mechanisms for the preservation and disclosure of electronic evidence across borders, and a framework for mutual legal assistance that does not require dual criminality in all cases.[45] Given that cross-border attacks account for a significant proportion of cyber incidents affecting Nigerian businesses and institutions, accession to the Budapest Convention would materially strengthen Nigeria's capacity to trace perpetrators, recover assets, and enforce judgments across jurisdictions in a manner that bilateral arrangements alone cannot replicate.

For Industry Collaboration: There is an opportunity here that the market has not yet fully seized. Legal, IT, and compliance professional bodies may collaborate to develop model cybersecurity contract clauses tailored to the Nigerian market, giving businesses of all sizes a practical starting point without the burden of commissioning bespoke legal advice. The fintech, banking, and telecommunications industries may also explore structured frameworks for cyber threat intelligence sharing, recognising that in a connected digital economy, one organisation's vulnerability is everyone's risk.

CONCLUSION

The conversation about cybersecurity in Nigeria has been dominated by the technical and the criminal: how to prevent attacks and how to prosecute attackers. What has received far less attention is the question that sits at the heart of every disrupted transaction, every compromised dataset, and every failed digital obligation: who bears the legal consequences when a cyberattack occurs?

This article has largely examined the circumstances in which parties may seek to avoid liability through force majeure, frustration, or contractual limitation. But the harder and more important question is who ultimately bears the loss when those defences are unavailable or fail. The honest answer is that liability will depend on the weight of evidence in each case, including whether the affected party demonstrated negligence in its security practices, complied with its regulatory obligations under the NDPA and the Cybercrimes Act, gave adequate notice following the incident, and if the contractual arrangements between the parties had been structured to allocate the risk in advance. The courts will weigh the totality of the evidence and reach a conclusion specific to the circumstances before it. This is precisely why cyber liability cannot be resolved through a one-size-fits-all approach, and why the work of building robust contractual frameworks, maintaining regulatory compliance, and developing judicial capacity is not optional. It is the only reliable foundation on which liability can be anticipated, managed, and fairly resolved.

Nigeria is operating in a different world now, one where a payment gateway can be disabled before breakfast, where customer data can be exfiltrated without a single physical intrusion, and where the legal consequences of a cyberattack can outlast the attack itself by years. The businesses and practitioners that recognise this shift and respond to it with urgency are not being alarmist. They are being prepared.

The legal framework in Nigeria is moving in the right direction. But laws do not draft contracts, lawyers do. Regulations do not manage risk, businesses do. Statutes do not build resilience, people do. The gap between where Nigeria's cyber liability framework is today and where it needs to be will not be bridged by legislation alone. It will be achieved one well drafted contract at a time, one proactive legal conversation at a time, one board that decides to take cyber risk seriously at a time.

1. Cost of a Data Breach Report 2024 IBM Security: https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs accessed on the 13th of February 2026.
2. Statista Market Insights: Expected Cost of Cybercrime Until 2028, :https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/ accessed on the 13th of February 2026.
3. Nigeria Records 119,000 Data Breaches in Q1 2025, Nairametrics (May 10, 2025): https://nairametrics.com/2025/05/10/nigeria-records-119000-data-breaches-in-q1-2025-ranks-34th-globally-report/ accessed on 13th February 2026.
4. Tech Gyant, Nigeria Financial Institutions Lose Trillions to Cyberattacks in 7 Years https://techgyant.com/nigeria-financial-institutions-lose-trillions-to-cyberattacks-in-7-years/ accessed on the 13th of February 2026.
5. CBN Financial Stability Report 2024 / NIBSS Fraud Report 2024 ,Central Bank of Nigeria / NIBSS: https://www.cbn.gov.ng / https://www.nibss-plc.com.ng accessed on the 14th of February 2026.
6. Techpoint Africa, Court Extends Freezing Order on 818 Accounts Linked to N10 Billion Cyberattack on Hope PSBank (October 15, 2024): https://techpoint.africa/news/court-extends-freezing-order-hope-psbank/ accessed on the 15th of February 2026.
7. Infusion Lawyers (August 31, 2024) NDPC's N555.8 Million Fine Against Fidelity Bank: Insights and Lessons,: https://infusionlawyers.com/2024/08/31/ndpcs-555-8-million-fine-against-fidelity-bank-over-alleged-data-privacy-violation-insights-and-lessons/ accessed on the 15th of February 2026.
8. Hope PSB Hit by N6.5 Billion Cyberattack, Begins Recovery , TechCabal (July 25, 2024): https://techcabal.com/2024/07/25/hope-psb-cyberttack-6-5bn/ accessed on the 16th of February 2026
9. State of Ransomware 2024, Sophos: https://www.sophos.com/en-us/whitepaper/state-of-ransomware accessed on the 16th of February 2026.
10. Princeps Credit Systems Ransomware Attack 2025, CYFIRMA: https://www.cyfirma.com/research/cyber-threat-assessment-on-nigeria/ accessed on the 17th of February 2026.
11. Cybersecurity Laws and Regulations Report 2025 Nigeria, ICLG: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/nigeria accessed on the 17th of February 2026.
12. Verizon 2024 Data Breach Investigations Report: https://www.verizon.com/business/resources/reports/dbir/ accessed on the 17th of February 2026.
13. Verizon 2025 Data Breach Investigations Report: https://www.verizon.com/business/resources/reports/dbir/ accessed on 17th of February 2026.
14. Cybercrimes (Prohibition, Prevention, etc.) Act 2015 Nigeria CERT: https://cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf accessed on the 17th of February 2026.
15. Templars Law, Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024 — Analysis (August 2024): https://www.templars-law.com/app/uploads/2024/08/Cybercrimes.pdf accessed on the 17th of February 2026.
16. Mondaq, SPA Ajibade and Co, The National Assembly Amends the Cybercrimes Act (May 2024): https://www.mondaq.com/nigeria/security/1466724/the-national-assembly-amends-the-cybercrimes-prohibition-prevention-etc-act accessed on the 17th of February 2026.
17. Nigeria's Cybercrime Reform, NALTF (August 2025): https://naltf.gov.ng/nigerias-cybercrime-reform/ accessed on the 17th of February 2026.
18. CookieYes, Nigeria Data Protection Act 2023 Overview: https://www.cookieyes.com/blog/nigeria-data-protection-act-ndpa/ accessed on the 17th of February 2026.
19. Nigeria's New Data Protection Act, Explained- Future of Privacy Forum: https://fpf.org/blog/nigerias-new-data-protection-act-explained/ accessed on the 17th of February 2026.
20. NDPC General Application and Implementation Directive (GAID) 2025 -DLA Piper Privacy Matters (June 2025): https://privacymatters.dlapiper.com/2025/06/nigeria-ndpc-issues-gaid-key-compliance-insights/ accessed on the 17th of February 2026.
21. Lawcare Nigeria - Globe Spinning Mills (Nig.) Plc v. Reliance Textile Industries Ltd (2017) LPELR 41433 (CA)
22. Miller Canfield - Preparing for Cyberattacks and Limiting Liability: https://www.millercanfield.com/resources-Preparing-for-Cyberattacks.html accessed on the 17th of February 2026.
23. Mayer Brown 2024 Cyber Litigation Legal Update: https://www.mayerbrown.com/en/insights/publications/2024/10/2024-cyber-litigation-legal-update-what-your-business-needs-to-know accessed on the 18th of February 2026.
24. Nwaolisah v. Nwabufoh (2011) LPELR 2115 (SC)
25. White and Case LLP Cybersecurity Developments and Legal Issues: https://www.whitecase.com/insight-alert/cybersecurity-developments-and-legal-issues accessed on the 20th of February 2026.
26. Force Majeure Unlocked: Your Comprehensive Guide to Contract Clauses Sirion (January 2026): https://www.sirion.ai/library/contract-clauses/force-majeure/ accessed on the 22nd of February 2026.
27. Building Cyber Resilience into Vendor Contracts, LinkedIn / Legal Commentary (April 2023): https://www.linkedin.com/pulse/building-cyber-resilience-vendor-contracts- accessed on the 22nd of February 2026.
28. The Fine Print: Key Contract Clauses Impacting Cyber Liability, NH Business Review (April 2024): https://www.nhbr.com/the-fine-print-key-contract-clauses-impacting-cyber-liability/ accessed on the 25th of February 2026.
29. Bloomberg Law Checklist: How to Manage Privacy and Cybersecurity Law Risks in Vendor Contracts (November 2025): https://pro.bloomberglaw.com/insights/privacy/checklist-managing-privacy-and-cybersecurity-law-risks-in-vendor-contracts/ accessed on the 25th of February 2026.
30. Navigating Cyber Insurance for Vendor Agreements - Amwins: https://www.amwins.com/resources-and-insights/market-insights/article/navigating-cyber-insurance-for-vendor-agreements accessed on the 26th of February 2026.

31. Mondaq, SPA Ajibade and Co, The National Assembly Amends the Cybercrimes Act (May 2024): https://www.mondaq.com/nigeria/security/1466724/the-national-assembly-amends-the-cybercrimes-prohibition-prevention-etc-act accessed on the 17th of February 2026.

32. Nigeria's Cybercrime Reform, NALTF (August 2025): https://naltf.gov.ng/nigerias-cybercrime-reform/ accessed on the 17th of February 2026.

33. CookieYes, Nigeria Data Protection Act 2023 Overview: https://www.cookieyes.com/blog/nigeria-data-protection-act-ndpa/ accessed on the 17th of February 2026.

34. NIBSS Fraud Report 2024 -Nigeria Inter Bank Settlement System: https://www.nibss-plc.com.ng accessed on the 2nd of March 2026

35. Information Commissioner's Office v. Advanced Computer Software Group Ltd and its Group Entities, ICO Monetary Penalty Notice, 27 March 2025, penalty of £3,076,320 imposed under Article 83 of the UK General Data Protection Regulation and Section 155 of the Data Protection Act 2018. https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited/ accessed on the 4th of March 2026.

36. Mayer Brown,2024 Cyber Litigation Legal Update: What Your Business Needs To Know: https://www.mayerbrown.com/en/insights/publications/2024/10/2024-cyber-litigation-legal-update-what-your-business-needs-to-know accessed on the 5th of March 2026.

37. Supra

38. Singapore's Revamped Cybersecurity Law: Key Amendments- Lexology / Baker McKenzie (November 2025): https://www.lexology.com/library/detail.aspx?g=1bce5f1c-df5f-4db9-a330-a53fb4f04383 accessed on the 6th of March 2026.

39. Clifford Chance -Cybersecurity Update: Singapore's Cybersecurity Act Extends its Reach: https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2024/05/cybersecurity-update-singapore-cybersecurity-act-extends-its-reach.html accessed on the 7th of March 2026.

40. Hogan Lovells -Provisions in Singapore's Cybersecurity Amendment Act: https://www.hoganlovells.com/en/publications/provisions-in-singapores-cybersecurity-amendment-act-came-into-force-on-31-october-2025 accessed on the 7th of March 2026.

41. Provisions in Singapore's Cybersecurity (Amendment) Act Came Into Force on 31 October 2025- Hogan Lovells: https://www.hoganlovells.com/en/publications/provisions-in-singapores-cybersecurity-amendment-act-came-into-force-on-31-october-2025 accessed on the 7th of March 2026.

42. Cybersecurity Laws and Regulations Report 2025 Nigeria ICLG (November 6, 2024): https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/nigeria accessed on 10th of March 2026.

43. More Than Malware: Unmasking the Hidden Risk of Cybersecurity Regulations- International Cybersecurity Law Review, Springer Nature: https://link.springer.com/article/10.1365/s43439-024-00111-7 accessed on the 13th of March 2026.

44. Budapest Convention on Cybercrime-Council of Europe: https://www.coe.int/en/web/cybercrime/the-budapest-convention accessed on the 14th of March 2026.

45. Comparative Analysis: The Budapest Convention vs the UN Convention Against Cybercrime — Digital Watch Observatory: https://dig.watch/updates/comparative-analysis-the-budapest-convention-vs-the-un-convention-against-cybercrime accessed on the 15th of March 2026.

Temitope Omojugba

Associate

temitope@acandelp.com