



**THIRD-PARTY VENDORS AND
CYBER RISK: CONTRACTUAL
ALLOCATION OF LIABILITY IN
NIGERIAN COMMERCIAL PRACTICE**

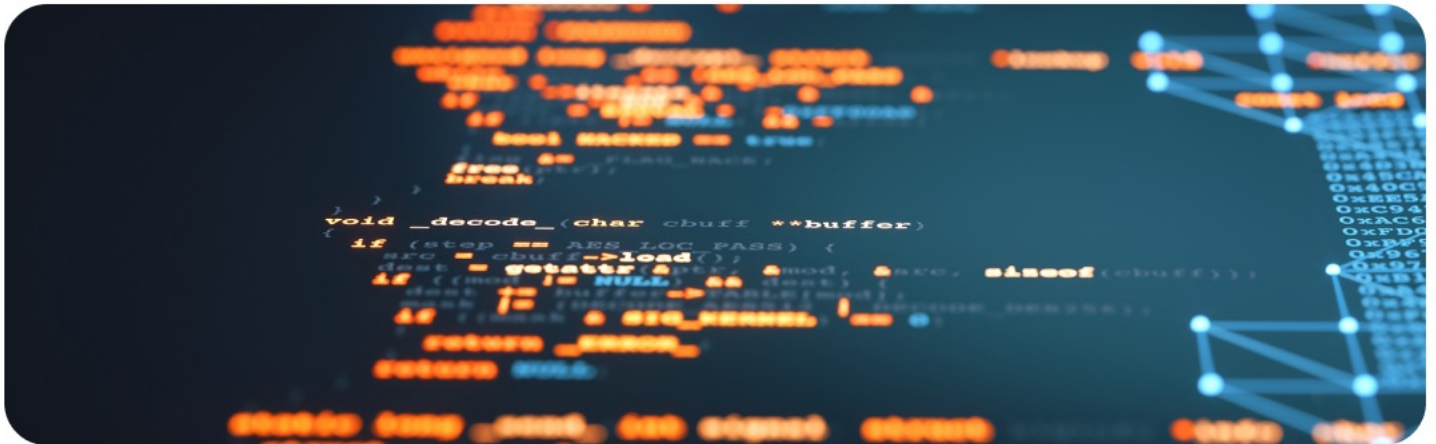
// Temitope Omojugba



**THIRD-PARTY VENDORS AND
CYBER RISK: CONTRACTUAL
ALLOCATION OF LIABILITY IN
NIGERIAN COMMERCIAL PRACTICE**

// Temitope Omojugba

INTRODUCTION



The rapid digitisation of commercial activities has fundamentally transformed the way businesses operate and deliver services. Across various sectors, organisations increasingly rely on third-party vendors such as cloud service providers, payment processors, software developers, data hosting companies, and managed information technology service providers to support critical business functions. While these outsourcing arrangements offer significant advantages in terms of efficiency, scalability, and cost reduction, they also expose businesses to new forms of cyber risk that often lie beyond their direct control.^[1]

In today's interconnected digital ecosystem, a cyber incident affecting a third-party vendor can have far-reaching consequences for the organisations that depend on its services. A security breach at a cloud provider may compromise sensitive customer information; a disruption affecting a payment processor may interrupt commercial transactions; and vulnerabilities within a vendor's systems may provide cybercriminals with access to a company's network infrastructure. Consequently, organisations are increasingly confronted with the reality that their cybersecurity posture is not determined only by their internal controls but also by the security practices of external parties within their supply chain.^[2] The growing prevalence of cyber incidents involving third-party vendors has raised significant legal and commercial questions regarding the allocation of responsibility when such incidents occur. Where a cyberattack, data breach, or service disruption originates from a vendor's systems,

determining liability is often complex. Businesses that incur losses may seek to hold vendors accountable, and vendors frequently rely on contractual limitations, exclusions, and indemnity provisions to restrict their exposure.

This issue has become particularly relevant in Nigeria's evolving digital economy, where businesses increasingly depend on outsourced technology solutions while simultaneously operating within a developing framework of cybersecurity and data protection regulations. The Nigeria Data Protection Act 2023 (NDPA) has reinforced organisational obligations to protect personal data and highlighted the importance of effective vendor oversight. As a result, the question of who bears liability for cyber incidents can no longer be viewed solely through a technical lens; it has become a matter of contractual drafting, regulatory compliance, and corporate risk management.

This article examines the allocation of liability for cyber incidents involving third-party vendors within Nigerian commercial practice. It explores the nature of third-party cyber risk, the contractual mechanisms commonly used to allocate responsibility, the impact of regulatory obligations, and the practical challenges associated with enforcing liability. The article further argues that as businesses become increasingly reliant on external service providers, proactive contractual risk allocation and effective vendor governance must become central components of organisational cybersecurity strategy.

UNDERSTANDING THIRD-PARTY CYBER RISK



Third-party cyber risk refers to the exposure an organisation faces when it relies on external vendors, service providers, or partners that have access to its systems, data, or operational processes. In practical terms, it is the risk that a security weakness, operational failure, or cyber incident affecting a vendor will adversely affect the organisations that depend on that vendor's services.

In modern commercial environments, third-party relationships are no longer peripheral. They are embedded in core business operations. Cloud computing providers host critical infrastructure, payment processors facilitate financial transactions, software vendors manage enterprise systems, and IT service providers maintain security and network operations. This deep integration means that a vulnerability in one vendor can quickly cascade across multiple dependent organisations.

Common examples illustrate the practical reality of this risk. A cloud service provider experiencing a ransomware attack may result in downtime and

potential data exposure for client organisations. A compromised payment processor may disrupt transaction flows and lead to financial loss, customer dissatisfaction, and regulatory scrutiny. Similarly, weak security practices within an IT outsourcing firm may provide attackers with a gateway into multiple clients' systems simultaneously.

These scenarios highlight a fundamental principle of modern cybersecurity: an organisation's security posture is only as strong as the weakest link in its supply chain. Even where a company maintains robust internal controls, its exposure may still be determined by the security standards and operational resilience of its external partners.

This interconnected risk environment has been formally recognised in international cybersecurity governance frameworks. The National Institute of Standards and Technology (NIST) cybersecurity framework identifies supply chain and third-party risk management as a key component of organisational cybersecurity governance. It emphasises the need to identify, assess, and manage risks arising from external dependencies.^[3] Similarly, the International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC 27001) establishes supplier and third-party security management as a core control area within information security management systems.^[4]

In the Nigerian context, this risk is particularly significant due to the rapid adoption of outsourced digital services alongside evolving regulatory oversight. As businesses increasingly depend on external providers for critical digital functions, the consequences of third-party failures extend beyond operational disruption to include legal liability, regulatory exposure, and reputational damage.

Accordingly, understanding third-party cyber risk is essential because it frames the central issue explored in this article: when such risk materialises, how should liability be allocated between the vendor and the organisation that engaged it?

THE CONTRACTUAL FRAMEWORK FOR VENDOR RELATIONSHIPS



The legal basis of vendor relationships in commercial practice is primarily contractual. Organisations engaging third-party vendors, whether cloud service providers, payment processors, software developers, or IT service providers, typically regulate their relationships through contracts and service level agreements (SLAs). These agreements define the scope of services, the obligations of each party, performance expectations, and the remedies available in the event of non-performance or breach.

In cybersecurity-related outsourcing arrangements, contractual obligations operate within the broader framework of the NDPA. Sections 24 and 25 of the NDPA establish the foundational principles governing personal data processing and the lawful bases upon which such processing may be carried out. Section 24 prescribes key data protection principles, including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality. Section 25, on the other hand, sets

out the conditions under which personal data may be lawfully processed, including consent, contractual necessity, legal obligation, and legitimate interests.^[5]

These provisions are further reinforced by Section 29 NDPA^[6] which imposes direct obligations on both data controllers and data processors to ensure that personal data is processed in accordance with the NDPA and that appropriate safeguards are maintained. This statutory allocation of responsibility is particularly significant in vendor relationships, where processing activities are often delegated to third-party service providers.

A critical provision in the context of cyber risk is Section 39(1)NDPA, which requires data controllers and data processors to implement appropriate technical and organisational measures to ensure the security, integrity, and confidentiality of personal data. These measures must protect against accidental or unlawful destruction, loss, misuse, alteration, unauthorised disclosure, or access. This provision forms the statutory foundation for cybersecurity obligations typically reflected in vendor contracts.^[7]

In practice, vendor agreements translate these statutory requirements into enforceable contractual terms. Data protection clauses require compliance with applicable data protection laws and the implementation of adequate security controls. Confidentiality obligations protect sensitive commercial and operational information exchanged during the relationship. Service level agreements establish measurable standards such as uptime commitments, response times, and continuity obligations that are particularly relevant when cyber incidents disrupt service.

Ultimately, the contractual framework serves as the mechanism through which statutory duties under the NDPA are operationalised between parties. Accordingly, liability exposure in vendor relationships is shaped not only by the occurrence of a cyber incident, but by the extent to which the parties properly documented, allocated, and managed their respective obligations within the contractual arrangement.

ALLOCATION OF LIABILITY FOR CYBER INCIDENTS



The occurrence of a cyber incident does not automatically determine who bears responsibility for the resulting loss. In commercial practice, liability is often determined by the contractual framework governing the relationship between the organisation and the third-party vendor. Consequently, where a data breach, ransomware attack, system compromise, or service disruption originates from a vendor's systems, the allocation of liability will largely depend on the contractual provisions agreed by the parties.

One of the most common mechanisms for allocating cyber risk is the limitation of liability clause. These clauses are designed to restrict the amount a party may be required to pay in the event of a breach of contract or other specified failure. Vendors frequently seek to cap their liability at a fixed amount, often calculated by reference to the fees paid under the agreement over a specified period.

Such clauses provide vendors with a degree of financial certainty, but their protection is heavily restricted under Nigerian law in the event of a severe operational failure. Under Nigerian contract jurisprudence, limitation of liability clauses are generally enforceable only where they have been properly incorporated and clearly reflect the parties' mutual intentions. However, in *Niger Insurance Co. Ltd v. Abed Brothers Ltd & Anor* (1976) [8] The Supreme Court established a vital restriction on vendors: a party cannot rely on a limitation or exclusion clause to escape liability for a breach of a fundamental term. The Court emphasised that a contract must be construed as a whole, meaning that if a tech vendor's cybersecurity failure is deemed a total breakdown of their core obligations, the entire liability cap can be invalidated, exposing the vendor to full consequential damages.[9]

Indemnity provisions also play a significant role in allocating cyber-related liability. An indemnity clause typically requires one party to compensate the other for losses arising from specified events or conduct. In the context of cybersecurity, organisations often seek indemnities covering losses resulting from data breaches, unauthorised disclosures of information, regulatory investigations, third-party claims, or vendors' failures to comply with agreed security obligations. The scope of an indemnity provision can therefore determine which party ultimately bears the financial consequences of a cyber incident.

Another important contractual mechanism is the exclusion clause. These provisions seek to exclude liability for certain categories of loss or damage. In technology and outsourcing agreements, vendors commonly exclude liability for consequential, incidental, or indirect losses. Such exclusions can significantly affect the remedies available to an organisation following a cyber incident, particularly where substantial losses extend beyond immediate operational disruption.^[10]

A distinction is therefore commonly drawn between direct and indirect losses. Direct losses are those that flow naturally and immediately from the cyber incident and may include costs associated with system restoration, incident response, forensic investigations, regulatory compliance measures, and financial losses

arising from service downtime. Indirect losses, on the other hand, may include reputational damage, loss of customers, loss of future business opportunities, diminished goodwill, and other consequential commercial losses. While indirect losses may represent the most significant long-term impact of a cyber incident, they are often excluded from recovery under contractual arrangements.^[11]

In practice, vendors frequently seek to minimise their exposure to cyber-related liability through a combination of limitation-of-liability clauses, narrowly drafted indemnities, and broad exclusion provisions. The result is that a substantial portion of the cyber risk may be transferred back to the client, even where the incident originates from the vendor's systems or operations. Consequently, organisations that accept standard vendor terms without careful negotiation may find themselves bearing losses that they assumed would be recoverable.

Ultimately, liability for cyber incidents is rarely determined solely by identifying the source of the breach. Rather, it is often determined by the parties' contractual allocation of risk. For this reason, careful drafting and negotiation of liability provisions remain essential components of effective cyber risk management.

REGULATORY AND COMPLIANCE CONSIDERATIONS



While contractual provisions play a significant role in allocating liability between organisations and third-party vendors, such provisions do not displace regulatory obligations. In the event of a cyber incident involving personal data, organisations must also consider their responsibilities under the NDPA. Consequently, the allocation of contractual liability may not necessarily determine regulatory accountability.

A key consideration under the NDPA is the distinction between a data controller and a data processor. The Act defines a data controller as a person who determines the purposes and means of processing personal data, while a data processor processes personal data on behalf of a data controller.^[12] In many vendor relationships, the engaging organisation acts as the data controller, while the third-party service provider functions as the data processor. This distinction is significant because the Act imposes obligations on both parties regarding the lawful processing and protection of personal data.

As mentioned earlier, data controllers and data processors are required to comply with the data processing principles and accountability obligations prescribed under the NDPA, including technical and organisational measures to guarantee the security of personal data.^[13] These obligations underscore the importance of maintaining effective cybersecurity controls and governance structures throughout the data processing lifecycle.

The distinction between controllers and processors becomes particularly important when assessing liability following a cyber incident. Although a data processor may be directly responsible for an operational failure that results in a data breach, the data controller may nevertheless remain exposed to regulatory scrutiny because it is ultimately responsible for determining the purposes and means of processing personal data. Consequently, the existence of a contractual arrangement transferring certain responsibilities to a

vendor does not necessarily shield an organisation from regulatory consequences. Depending on the circumstances, regulators may examine the conduct of both parties in determining whether adequate safeguards were implemented.^[14]

The outsourcing of services, therefore, does not automatically transfer statutory responsibilities under the NDPA. Organisations cannot avoid regulatory obligations simply by delegating data processing activities to third-party vendors. Where a cyber incident occurs, regulators may assess not only the vendor's action but also whether the organisation exercised reasonable care in selecting, engaging, and supervising that vendor. As a result, contractual provisions allocating liability may coexist with separate regulatory obligations imposed directly by law.^[15]

This position has important implications for vendor risk management. Compliance under the NDPA extends beyond contractual drafting and requires organisations to adopt a proactive approach to vendor oversight. Before engaging a vendor, organisations should conduct appropriate due diligence to assess the vendor's cybersecurity posture, technical competence, data protection practices, and ability to comply with applicable legal and regulatory requirements. This

assessment may include reviewing internal security policies, incident response procedures, prior compliance history, and relevant certifications where available.^[16]

Vendor oversight should also continue throughout the relationship. Organisations should periodically review vendors' compliance with contractual and regulatory obligations, require prompt notification of security incidents, and, where appropriate, reserve contractual rights to conduct audits or obtain independent assurance regarding cybersecurity controls. Such measures not only strengthen cybersecurity resilience but also demonstrate a commitment to regulatory compliance and accountability. The Nigeria Data Protection Commission (NDPC) has further emphasised the importance of accountability and governance structures in ensuring compliance with the NDPA.^[17]

The regulatory framework ultimately reinforces an important principle: organisations may remain accountable for data protection failures even when the immediate cause of the breach lies with a third-party vendor. For this reason, vendor risk management should be viewed not merely as a contractual issue but as a critical aspect of regulatory compliance, corporate governance, and enterprise risk management.^[18]

PRACTICAL GAPS IN NIGERIAN COMMERCIAL PRACTICE



Despite growing awareness of cybersecurity risks and increasing reliance on third-party service providers, significant gaps remain in the way many Nigerian businesses manage vendor-related cyber risks. While contractual safeguards and regulatory obligations provide a framework for addressing such risks, organisations frequently fail to give adequate attention to vendor risk management during the contracting process. Some of the common issues are;

- Over-reliance on standard vendor terms and conditions - Many vendors, particularly large technology providers, cloud service providers, and software vendors, present customers with pre-drafted agreements that are rarely negotiated.^[19] In practice, organisations often accept these terms without conducting a detailed assessment of the liability provisions, cybersecurity obligations, or incident response commitments contained in the agreement. As a result, businesses may unknowingly assume risks that they would otherwise have sought to allocate differently.
- Weak negotiation of liability clauses. As discussed earlier, limitation of liability clauses, indemnity

provisions, and exclusion clauses play a central role in determining who bears the financial consequences of a cyber incident. However, many organisations focus primarily on commercial terms such as pricing, service delivery timelines, and operational requirements, while paying comparatively little attention to risk allocation provisions. This may result in contracts that significantly limit a vendor's liability while leaving the client exposed to substantial financial and regulatory consequences in the event of a cybersecurity failure.

- Inadequate diligence - Limited cybersecurity due diligence before vendor engagement also remains a significant concern. In many cases, organisations assess vendors based on cost, functionality, or market reputation without adequately evaluating the nature of the services being provided. Important considerations such as information security policies, incident response capabilities, compliance history, security certifications, and data protection practices may receive little or no scrutiny prior to engagement.^[20]

These shortcomings are often linked to a broader tendency to underestimate third-party cyber risk at the contracting stage. Many organisations continue to view cybersecurity primarily as a technical or operational issue rather than a legal, regulatory, and commercial risk. This perception can lead to insufficient involvement of legal, compliance, and risk management teams during vendor selection and contract negotiations. In the event of a cyber incident, the organisation may discover that critical issues relating to liability, notification obligations, audit rights, and incident response responsibilities were either inadequately addressed or omitted entirely from the contractual arrangement.

The increasing interconnectedness of digital business operations means organisations are often only as secure as their vendors. Consequently, third-party cyber risk should not be treated as a peripheral concern but as a core component of enterprise risk management. Addressing the practical gaps that currently exist in Nigerian commercial practice will require greater awareness, stronger contractual discipline, and a more proactive approach to vendor due diligence and oversight.^[21]

CHALLENGES IN ENFORCING LIABILITY



Although contractual provisions and regulatory frameworks may provide a basis for allocating responsibility following a cyber incident, enforcing liability in practice is often considerably more complex. Organisations seeking compensation or other remedies may encounter significant legal, evidentiary, and procedural challenges, which we will elaborate on further, particularly where cyber incidents involve sophisticated technological systems, multiple service providers, or cross-border transactions.

1. Evidentiary Challenge - Cyber incidents rarely arise from a single identifiable cause, creating the burden of proving fault or negligence on the part of the vendor. A data breach, ransomware attack, or system compromise may result from a combination of factors, including vulnerabilities within the vendor's systems, inadequate security controls implemented by the client, malicious third-party activity, human error, or unforeseen technical failures. Consequently, establishing that a vendor failed to exercise reasonable care or breached its contractual obligations may require extensive forensic investigations and technical analysis.^[22] The

complexity of modern information systems often makes it difficult to establish a direct causal connection between the vendor's conduct and the loss suffered by the organisation. In addition, interpreting technical evidence often requires the involvement of cybersecurity specialists, digital forensic experts, and other technical professionals capable of explaining complex technological issues to courts or arbitral tribunals.

2. Jurisdictional issues - This particularly occurs where services are provided by foreign technology companies. Many cloud service providers, software vendors, and digital platforms operating in Nigeria are incorporated outside the country and frequently include foreign governing law, jurisdiction, or arbitration clauses in their agreements. As a result, Nigerian organisations seeking to enforce contractual rights may be required to institute proceedings in foreign jurisdictions or participate in international arbitration.^[23] Such processes may involve unfamiliar legal systems, increased legal costs, procedural complexities, and practical difficulties associated with enforcing foreign judgments or arbitral awards.^[24]

3. Technical challenges - Establishing liability frequently requires the production of electronic records, system logs, network activity reports, forensic investigation reports, and other forms of digital evidence. Under Section 84 of the Evidence Act 2011, computer-generated evidence is admissible in legal proceedings subject to compliance with the statutory requirements relating to authenticity and reliability.^[25] Accordingly, organisations seeking to rely on electronic evidence must ensure that such evidence is properly collected, preserved, and documented from the earliest stages of incident response.

4. Statutory requirements - Nigerian courts have repeatedly emphasised the importance of complying with the requirements of Section 84 when tendering electronic evidence. In *Kubor v. Dickson*, the Supreme Court held that parties relying on computer-generated evidence must satisfy the statutory conditions prescribed under the Evidence Act before such evidence can be admitted.^[26] Similarly, in *Dickson v. Sylva*, the Supreme Court clarified that compliance with Section 84 may be established through oral testimony or a certificate of compliance, while distinguishing between the admissibility of electronic evidence and the weight to be attached to it.^[27] These decisions highlight the critical importance of proper evidence preservation and documentation in cyber-related disputes.

5. Delays and costs - This is often associated with dispute resolution in addition to the specialised expertise, which significantly increases the cost and complexity of enforcement proceedings. Cyber incidents often require immediate remedial action to contain the breach, restore operations, and address regulatory concerns, whereas litigation and arbitration proceedings may take months or years to conclude. During this period, organisations may continue to experience financial losses, reputational damage, customer attrition, and regulatory scrutiny. The costs associated with legal representation, forensic investigations, expert witnesses, and dispute resolution proceedings may discourage organisations from pursuing claims, particularly where contractual limitations of liability restrict the amount ultimately recoverable.

These challenges demonstrate that the existence of contractual rights does not necessarily guarantee an effective remedy. A party may possess a strong contractual claim against a vendor and still encounter significant difficulties in proving liability, establishing causation, recovering damages, and enforcing a judgment or arbitral award. Consequently, organisations should consider these enforcement challenges during contract negotiations and adopt proactive measures to prevent cyber incidents rather than relying solely on post-incident remedies.

COMPARATIVE PERSPECTIVE: THE UNITED STATES



The 2024 cyberattack on Change Healthcare, a healthcare technology provider in the United States, illustrates the significant risks associated with third-party service providers. The attack disrupted claims processing and payment systems relied upon by hospitals, pharmacies, insurers, and other healthcare providers across the country, demonstrating how a cyberattack on a single third-party service provider can have widespread operational consequences across an entire sector.^[28]

Following the incident, the United States Department of Health and Human Services (HHS), through the Centers for Medicare & Medicaid Services (CMS), issued guidance granting temporary regulatory flexibilities to state Medicaid agencies. The guidance permitted states to make interim payments to healthcare providers affected by the disruption, enabling them to continue providing essential healthcare services while Change Healthcare restored its systems.^[29] This response demonstrates that managing third-party cyber risk extends beyond establishing legal obligations. It also requires practical regulatory measures to minimise disruption and maintain essential services during a cyber incident.

The legal and regulatory consequences of the Change Healthcare cyberattack remain ongoing, with litigation and regulatory proceedings continuing in the United States. Accordingly, questions relating to the ultimate allocation of liability and recovery of losses have not been finally determined.

The Change Healthcare incident illustrates that regulatory intervention can help preserve the continuity of essential services during a cyber incident, but it does not determine the ultimate allocation of liability. While emergency measures may mitigate immediate operational disruption, questions relating to contractual liability, regulatory responsibility, and financial recovery remain subject to the applicable legal framework and, where necessary, judicial determination. The key lesson is that effective third-party cyber risk management depends not only on regulatory preparedness but also on robust contractual risk allocation and proactive vendor oversight before an incident occurs.

IN SUMMARY



Third-party cyber risk is no longer a peripheral issue in modern business operations. As organisations increasingly rely on external vendors to manage critical systems, process personal data, and provide essential digital services, cyber risks originating from those vendors have become an extension of the organisation's operational and legal risks.

In many Nigerian commercial transactions, vendor relationships are still driven primarily by commercial considerations such as cost, efficiency, and service delivery. Consequently, cybersecurity considerations, including the allocation of responsibilities in the event of a cyber incident, may receive limited attention during contract negotiations. This can create uncertainty where cyber incidents involving third-party service providers result in operational disruption, regulatory exposure, or financial loss.

The increasing dependence on third-party service providers has also blurred the distinction between organisational risk and vendor risk. Although organisations may outsource certain business functions, they often remain accountable for protecting personal data and ensuring the continuity of critical services. This makes third-party cyber risk not only a contractual issue

but also an important aspect of corporate governance, operational resilience, and regulatory compliance.

Accordingly, managing third-party cyber risk requires organisations to consider vendor relationships as part of their broader enterprise risk framework rather than as isolated commercial arrangements.

RECOMMENDATION

The issues examined in this article suggest that organisations should adopt a structured approach to managing third-party cyber risk.

Organisations should conduct appropriate vendor due diligence before engaging third-party service providers, particularly where such vendors process personal data, manage critical systems, or provide essential digital services. Assessing a vendor's cybersecurity practices, compliance history, and incident response capabilities at the pre-contract stage can help identify and mitigate potential risks.

Contracts should clearly allocate cybersecurity responsibilities by incorporating provisions on cybersecurity obligations, incident notification, cooperation during cyber incidents, audit rights, and liability for security failures. These provisions should reflect each party's role and the degree of control exercised over systems, data, and security functions.

Organisations should also ensure that their contractual arrangements align with applicable obligations under the Nigeria Data Protection Act 2023. This will promote compliance and provide greater clarity regarding accountability for the processing and protection of personal data.

In addition, the Nigeria Data Protection Commission may consider issuing further guidance on third-party cyber risk management and vendor governance. Such guidance could assist organisations in implementing consistent contractual standards and strengthening cybersecurity governance across commercial relationships.

CONCLUSION

Third-party vendors have become indispensable to modern business operations, supporting digital transformation, operational efficiency, and technological innovation. However, the increasing reliance on external service providers has also expanded organisations' exposure to cyber risks, with potentially significant operational, financial, regulatory, and reputational consequences.

This article demonstrates that liability arising from third-party cyber incidents is rarely determined solely by the source of the breach. Rather, it is shaped by contractual provisions, applicable regulatory obligations, and the practical realities of enforcement. The effectiveness of

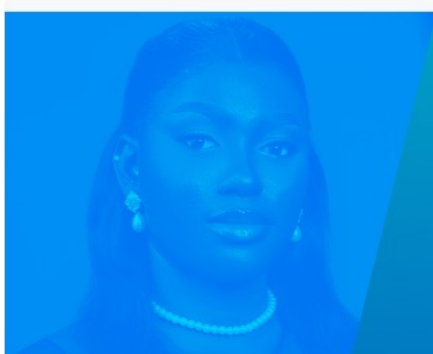
limitation of liability clauses, indemnities, data protection obligations, and vendor oversight mechanisms therefore plays an important role in determining how cyber risks are allocated and managed.

As organisations become increasingly interconnected, managing third-party cyber risk will remain an important aspect of cybersecurity governance and commercial contracting. While the Nigeria Data Protection Act 2023 provides a legal framework for accountability and data protection compliance, its effectiveness will ultimately depend on how those obligations are implemented in practice and adapted to an evolving cyber threat landscape.



REFERENCES

1. Economic Forum, Global Cybersecurity Outlook 2025, Insight Report, January 2025, page 9
2. Jon Boyens et al., Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST Special Publication 800-161 Revision 1 Update 1 (2024), 11, <https://doi.org/10.6028/NIST.SP.800-161r1-upd1> accessed on the 7th of June 2026.
3. National Institute of Standards and Technology, Cybersecurity Framework (CSF) 2.0 (2024), p 20–22 (Govern (GV.SC): Cybersecurity Supply Chain Risk Management) <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> accessed 7 June 2026.
4. International Organization for Standardization (ISO), ISO/IEC 27001:2022 Information Security Management Systems, <https://www.iso.org/standard/27001> accessed on the 7th of June 2026.
5. Sections 24 and 25 Nigeria Data Protection Act 2023.
6. Section 29 Nigeria Data Protection Act 2023.
7. Section 39 Nigeria Data Protection Act 2023.
8. Niger Insurance Company Ltd v. Abed Brothers Ltd & Anor (1976) LPELR-1995 (SC)
9. Franklin Okeke, "Exclusion Clauses: When He Who Pays the Piper Does Not Dictate the Tune!!!", Lelaw Barristers and Solicitors Mondaq (17 June 2020), discussing the operation of exclusion and limitation clauses under Nigerian contract law and the principle that parties are generally free to limit contractual liability. <https://www.mondaq.com/nigeria/contracts-and-commercial-law/954956/exclusion-clauses-when-he-who-pays-the-piper-does-not-dictate-the-tune> accessed on the 9th of June 2026.
10. .F.U. Nwankwo, "Terms and Conditions Apply: The World of Exclusion Clauses in Contracts", Chukwuemeka Odumegwu Ojukwu University Law Journal, discussing the nature and operation of exclusion clauses and judicial approaches to their interpretation <https://www.nigerianjournalonline.com/index.php/COOULJ/article/view/2416> accessed on the 9th of June 2026.
11. Ismail Adua Mustapha & Abdulganiyu Bello, "Doctrine of Exclusion and Limitation Clauses in an Agreement Contract: Approach from the of Carriage by Air", UNIZIK Law Journal Vol. 17 No. 1 (2021), examining the validity and enforceability of exclusion and limitation clauses under Nigerian law.
12. Section 65 (Interpretation), definitions of "Data Controller" and "Data Processor, Nigerian Data Protection Act 2023.
13. Section 39
14. Nigeria Data Protection Commission, Frequently Asked Questions on the Nigeria Data Protection Act 2023, explaining the roles and obligations of data controllers and data processors <https://ndpc.gov.ng/faqs/> accessed on the 8th of June 2026.
15. Ismail Adua Mustapha & Abdulganiyu Bello Supra note 13
16. Nigeria Data Protection Commission, Guidance Notice on Registration of Data Controllers and Data Processors of Major Importance, issued pursuant to Sections 5(d), 44 and 65 of the Nigeria Data Protection Act 2023
17. [6] Nigeria Data Protection Commission, General Application and Implementation Directive (GAID) 2025, provisions relating to accountability, governance, and compliance obligations of data controllers and processors
18. [7] Nigeria Data Protection Commission, Frequently Asked Questions on the Nigeria Data Protection Act 2023, discussing accountability, regulatory oversight, and compliance expectations under the Act, <https://ndpc.gov.ng/faqs/> accessed on the 8th of June 2026.
19. National Institute of Standards and Technology (NIST), Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM) (2024), emphasizing the need for organizations to establish supplier risk management processes and define security requirements for third-party vendors. <https://www.nist.gov/publications/nist-cybersecurity-framework-20-quick-start-guide-cybersecurity-supply-chain-risk> accessed on the 8th of June 2026.
20. NIST Supra note 22
21. ISO/IEC 27001:2022, Annex A 5.19 – Information Security in Supplier Relationships, emphasizing supplier due diligence, contractual security requirements, and ongoing oversight of third-party relationships. <https://www.isms.online/iso-27001/annex-a-2022/5-19-information-security-supplier-relationships-2022/> accessed on the 9th of June 2026.
22. National Institute of Standards and Technology (NIST), Cybersecurity Framework (CSF) 2.0 (2024), Supply Chain Risk Management (C-SCRM) Function, emphasizing identification, assessment, and management of third-party cybersecurity risks.
23. United Nations Commission on International Trade Law (UNCITRAL), Model Law on International Commercial Arbitration 1985, with amendments as adopted in 2006 https://uncitral.un.org/en/texts/arbitration/modellaw/commercial_arbitration accessed on the 9th of June 2026.
24. Convention on the Recognition and Enforcement of Foreign Arbitral Awards 1958 (New York Convention) https://uncitral.un.org/en/texts/arbitration/modellaw/commercial_arbitration accessed on the 9th of June 2026.
25. Section 84, Evidence Act 2011
26. Kubor v. Dickson (2013) 4 NWLR (Pt. 1345) 534
27. Dickson v. Sylva (2016) 8 NWLR (Pt. 1515) 484 SC
28. United States Department of Health and Human Services, Change Healthcare Cybersecurity Incident – CMS Response and State Flexibilities <https://www.hhs.gov/guidance/document/change-healthcare-cybersecurity-incident-cms-response-and-state-flexibilities> accessed on the 23rd of July 2026.
29. Ibid



**Temitope
Omojugba**

Associate

temitope@candelp.com

