International Journal of Business & Law Research 14(2):439-453, April-June, 2026

© SEAHI PUBLICATIONS, 2026 www.seahipublications.org **ISSN: 2360-8986**

DOI:10.5281/zenodo.21998823

The Legal Implications Of Ransomware Attacks On Public And Private Institutions In Nigeria

Kelvin Bribena PhD[1]

Faculty of Law,
Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria
kelvinbribena@gmail.com, kbribena@edu.ndu.org

ABSTRACT
Ransomware attacks have become a significant legal and cybersecurity threat to public and private institutions in Nigeria due to increasing dependence on digital infrastructure for governance, banking, healthcare, education, telecommunications and commercial activities. Such attacks commonly involve unauthorised access to computer systems, encryption or exfiltration of data, interruption of institutional operations and demands for payment before access is restored or stolen information is withheld from publication. Accordingly, this article examined the legal implications of ransomware attacks on public and private institutions in Nigeria, with particular reference to the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended in 2024, the Nigeria Data Protection Act 2023, the Constitution of the Federal Republic of Nigeria 1999, the Designation and Protection of Critical National Information Infrastructure Order 2024 and other relevant regulatory instruments. The study adopted a doctrinal legal research methodology, relying principally on primary and secondary sources of law through the use of statutes, judicial decisions, regulations, government cybersecurity policies and other relevant documents to analyse the adequacy of Nigeria's existing legal framework. The article found that although existing legislation criminalises most activities associated with ransomware and imposes important cybersecurity and data-protection obligations on institutions, nevertheless, significant gaps remain in relation to mandatory ransomware reporting, coordinated institutional response, cross-border enforcement and regulation of ransom payments. Therefore, the paper recommended, first, the adoption of a comprehensive national ransomware response framework establishing clear reporting, coordination and incident-management obligations for public and private institutions. Second, it recommended the introduction of specific statutory or regulatory rules governing ransom payments, including mandatory law-enforcement notification, sanctions and terrorism-financing screening, and enhanced approval requirements for payments involving public funds or critical infrastructure.

Keywords: Ransomware; Cybercrime; Cybersecurity; Data Protection; Critical Infrastructure; Institutional Liability.

1. INTRODUCTION

Information and communication technologies have become essential to contemporary governance and commercial activity. Government ministries maintain electronic records; universities operate digital registration and learning systems; hospitals increasingly rely on electronic medical information; banks provide almost continuous electronic services; telecommunications companies maintain national communications infrastructure; and private businesses routinely store commercial information in interconnected computer systems and cloud environments. This transformation has created substantial

[1]**Kelvin Bribena**, LLB, BL, LLM, M.Sc, M.Ed, LLD, ACIArb, FNIMN, Head of Department, Jurisprudence and International Law, Faculty of Law, Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria

economic and administrative benefits. It has, however, also created vulnerabilities capable of being exploited by organised cybercriminals.

Ransomware represents one of the most serious manifestations of this vulnerability. In its traditional form, ransomware is malicious software that encrypts files or otherwise prevents legitimate users from accessing a computer system until a ransom is paid. Modern ransomware operations have become considerably more sophisticated. Attackers may first infiltrate a network, acquire administrator privileges, disable security systems, extract confidential data and then encrypt operational systems. The attackers subsequently demand payment, frequently in cryptocurrency, and threaten either permanent loss of access or publication of stolen information. This practice is commonly described as "double extortion". Some criminal groups go further by contacting customers, employees or business partners whose information has been stolen, thereby creating additional pressure on the affected institution.[2]

The effects of such an attack are not confined to the compromised computers. Where ransomware affects a hospital, the availability of medical records and diagnostic systems may be interrupted. Where a bank is attacked, electronic payments, customer accounts and transaction infrastructure may be endangered. An attack against a university may compromise student records, research information and admission systems. Government institutions may lose access to administrative records or information necessary for public services. Consequently, ransomware should no longer be regarded merely as an information-technology problem. It is simultaneously a criminal-law, privacy, regulatory, contractual, corporate-governance and national-security concern. Research on ransomware has similarly demonstrated that its consequences include operational, financial and social harms extending well beyond the amount demanded by attackers.[3]

The Nigerian threat environment makes this inquiry particularly important. On 8 July 2024, the Nigeria Computer Emergency Response Team (ngCERT) warned that it had detected increased ransomware activity by the Phobos ransomware group against critical cloud-service providers within Nigerian cyberspace. The advisory identified organisations serving government agencies, financial institutions, telecommunications companies, educational institutions, healthcare providers and non-governmental organisations as among those potentially exposed.[4] In September 2024, ngCERT issued another high-risk advisory concerning ransomware groups exploiting vulnerabilities in backup infrastructure and warned that successful exploitation could result in system takeover, data exfiltration and ransomware deployment.[5] These official warnings demonstrate that ransomware is not a hypothetical concern for Nigeria.

Nigeria possesses a comparatively broad legislative framework addressing cybercrime. The principal legislation is the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, substantially affected by the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024.[6] The Nigeria Data Protection Act 2023 creates an additional compliance framework where an attack compromises personal data.[7] The Constitution protects privacy, while the 2024 Designation and Protection of Critical National Information Infrastructure Order extends special attention to strategically important information systems. Sector-specific regulators, particularly the Central Bank of Nigeria, also impose cybersecurity requirements on regulated organisations.

Nevertheless, ransomware exposes a distinctive difficulty. Nigerian legislation does not require a provision expressly labelled "ransomware offence" before ransomware conduct becomes punishable.

---

[2] Chiamaka Ohakwe, 'The Rise of Ransomware Attacks in Nigeria' (18 January 2025) SSRN <https://doi.org/10.2139/ssrn.5277510> **accessed 8 August 2026**.

[3] Nandita Pattnaik and others, 'It's More Than Just Money: The Real-World Harms from Ransomware Attacks' (2023), examining operational, social and human harms generated by ransomware incidents <http://doi.org/10.48550/arXiv2307.2855> accessed 12 August 2026

[4] ngCERT, 'Escalation of Ransomware Attack in Nigeria' (n 1).

[5] Nigeria Computer Emergency Response Team, 'Ransomware Groups Targeting Critical Systems in Nigeria', Advisory No ngCERT-2024-0033, 13 September 2024.

[6] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended by the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024.

[7] Nigeria Data Protection Act 2023

The legal characterisation depends instead upon the acts performed during the attack: unauthorised access, interference with computer systems, unlawful interception, theft of credentials, extortionate communications, fraud, destruction or alteration of data, conspiracy and money laundering. This functional approach has advantages because it accommodates changing technologies. At the same time, the absence of a comprehensive ransomware-specific regulatory framework leaves uncertainty concerning such matters as ransom payments, compulsory ransomware reporting, the role of boards and accounting officers, cyber-insurance arrangements and coordination among regulatory agencies.

The problem is even more complicated from the perspective of an institution that becomes a victim. The fact that an organisation has been attacked does not automatically mean that it has violated the law. Cybersecurity regulation does not ordinarily impose strict liability merely because an attacker succeeded. Nevertheless, where personal information is compromised, the Nigeria Data Protection Act requires consideration of whether the institution adopted appropriate technical and organisational safeguards.[8] The organisation may additionally have notification obligations and could become liable where its own inadequate practices materially contributed to foreseeable loss. The legal implications of ransomware must therefore be studied from both directions. The first concerns the criminal responsibility of the perpetrators and persons facilitating the attack. The second concerns the responsibilities of the institution whose systems have been compromised. This article adopts that dual approach.

2. Understanding Ransomware and its Institutional Consequences

Ransomware is best understood as a method of digitally enforced coercion. Although the malicious program used to encrypt information is central to many attacks, contemporary ransomware campaigns involve a sequence of activities. Initial access may be obtained through phishing, compromised passwords, exposed remote-access services, software vulnerabilities or malicious insiders. Once access has been achieved, attackers may move through the network, escalate privileges, identify valuable information and disable backup or recovery infrastructure. Encryption may occur only after substantial confidential information has been copied.

Consequently, the legal wrong does not begin when a ransom note appears. An attacker who covertly enters an institutional network has already potentially committed an offence relating to unauthorised access. Copying confidential information can create additional offences and civil consequences. Interfering with or encrypting files may constitute system interference. Threatening to publish data unless payment is made introduces extortion. Receiving and laundering cryptocurrency obtained from victims introduces financial-crime dimensions.

This sequence is particularly important when Nigerian statutes are applied to ransomware because the Cybercrimes Act regulates conduct rather than merely particular malware names. Section 6 criminalises specified forms of unlawful access to computers and computer networks.[9] Section 8 directly addresses system interference by prohibiting intentional or fraudulent conduct that seriously hinders a computer system through activities including transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.[10] Encryption deliberately designed to prevent an organisation from accessing its own systems falls naturally within the concept of serious interference.

Ransomware has also evolved from simple encryption into an organised criminal economy. Ransomware-as-a-Service arrangements allow malware developers to provide technical platforms to affiliates who identify and attack victims in return for a share of ransom payments. Research examining ransomware payment ecosystems demonstrates the economic sophistication of these networks and the importance of cryptocurrency in enabling cross-border criminal transactions.[11] This creates difficulties for traditional law enforcement because the developer, affiliate, negotiator, infrastructure provider and person laundering proceeds may be located in several jurisdictions.

[8] Nigeria Data Protection Act 2023, s 39

[9] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended), s 6.

[10] Ibid, s 8.

[11] Kris Oosthoek, Jack Cable and Georgios Smaragdakis, 'A Tale of Two Markets: Investigating the Ransomware Payments Economy' (2022), analysing ransomware-payment activity and Ransomware-as-a-Service structures <https://doi.org/10.48550/arXiv.2205.05028> accessed 12 August 2026

Institutional harm also varies according to the victim. A private retail company may principally suffer loss of revenue and customer confidence. A government institution may be unable to perform statutory duties. A financial institution may experience systemic consequences if payment infrastructure becomes unavailable. A healthcare institution may confront risks to life where clinicians cannot access patient information. Recent empirical research examining hospital ransomware incidents outside Nigeria found substantial reductions in hospital activity during attacks and measurable adverse consequences for patients.[12] Although those findings arise from another jurisdiction, they demonstrate why cybersecurity obligations in sectors such as healthcare cannot be reduced merely to protecting information confidentiality.

Three information-security principles-confidentiality, integrity and availability-are consequently important to the legal analysis. Ransomware may compromise all three. Data exfiltration compromises confidentiality; unauthorised alteration compromises integrity; and encryption or system shutdown compromises availability. Nigerian data-protection legislation expressly recognises these dimensions.

3. The Nigerian Legal Framework Governing Ransomware

3.1 The Constitution and the Right to Privacy

Section 37 of the Constitution of the Federal Republic of Nigeria 1999 guarantees and protects the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications.[13] Although the provision was drafted before contemporary ransomware became a significant threat, Nigerian jurisprudence increasingly recognises data privacy as falling within the constitutional protection of privacy.

The Court of Appeal's decision in *Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v National Identity Management Commission* is particularly significant.[14] The Court recognised the relationship between personal-data protection and the constitutionally protected right to privacy. This constitutional foundation means that a ransomware incident involving unauthorised acquisition or disclosure of personal information may implicate more than statutory data-protection standards. Depending on the circumstances, it may engage a fundamental right.

For public institutions, this is especially important. Government agencies hold extensive information concerning citizens, including identification records, financial information, employment records, health information and other sensitive materials. The state's obligation to respect privacy cannot logically be confined to refraining from intentional intrusion. Modern data governance increasingly requires reasonable safeguards against unauthorised interference by third parties.

That proposition should nevertheless be applied cautiously. The occurrence of a ransomware attack does not automatically establish a constitutional violation by the victim institution. The relevant question would ordinarily include whether the institution's own acts or omissions amounted to an unlawful interference or whether statutory security duties were breached. This is where the Nigeria Data Protection Act becomes particularly important.

3.2 Nigeria Data Protection Act 2023

The Nigeria Data Protection Act 2023 applies broadly to the processing of personal data and covers data controllers and processors operating in Nigeria as well as specified processing involving persons in Nigeria.[15] Public authorities and private entities may therefore fall within its requirements.

Section 39 imposes one of the most significant legal duties for ransomware purposes. Data controllers and processors are required to implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data in their possession or control. The provision

[12] Hannah Neprash, Claire McGlave and Sayeh Nikpay, 'Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients' (2026) 18(1) American Economic Journal: Economic Policy 256 <https://doi.org/10.1257/pol.20240594> accessed 8 August 2026.

[13] Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37.

[14] Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v National Identity Management Commission (2021) LPELR-55623(CA). See also Felix Emmanuel, 'Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v National Identity Management Commission: A Milestone towards a Human Right-Based Approach to Data Protection in Nigeria' (2022) 16(1) Nigerian Juridical Review 306 <https://doi.org/10.56284/tnjr.v16i1.24> accessed 8 August 2026.

[15] Nigeria Data Protection Act 2023, ss 1–3

expressly contemplates protection against unlawful destruction, loss, alteration, disclosure and access.[16]

The Act does not impose one universal technological standard. Appropriateness is assessed by reference to matters including the amount and sensitivity of the information, potential harm to data subjects, the scale and duration of processing, and the availability and cost of security technologies. This is a risk-based model. A large bank holding financial information belonging to millions of customers is therefore expected to implement more sophisticated protection than a very small enterprise handling relatively limited personal information.

Section 39 goes further by identifying measures which may include encryption, pseudonymisation, mechanisms for ensuring confidentiality, integrity, availability and resilience, procedures for timely restoration of data following technical incidents, periodic risk assessments, regular testing and continuous updating of security measures.[17] The statutory reference to restoration and resilience has obvious relevance to ransomware. An institution that cannot recover because it maintained no viable backups, did not segregate backup systems from production networks and conducted no recovery testing may have difficulty demonstrating effective compliance.

Nevertheless, regulatory liability should not be confused with strict liability. Sophisticated attackers can compromise well-secured organisations. The appropriate question is whether the organisation took reasonable and proportionate measures having regard to the risks it faced. Security must therefore be assessed prospectively rather than purely with hindsight.

Section 40 creates breach-notification obligations. Where a processor becomes aware of a personal-data breach, it must notify the relevant controller or engaging processor. A data controller must notify the Nigeria Data Protection Commission within 72 hours of becoming aware of a breach likely to result in risk to the rights and freedoms of individuals.[18] Where the breach is likely to create a high risk, communication to affected data subjects may also be required.[19]

This means that once ransomware involves personal information, incident management becomes a legal exercise as well as a technical one. Within the first hours of discovery, the institution must determine whether information has merely been encrypted or has also been accessed or exfiltrated, identify categories of affected records, preserve evidence, assess potential harm and decide whether notification thresholds have been met.

Failure to satisfy the Act can produce significant consequences. The NDPC may issue compliance and enforcement orders, require remediation, order compensation and impose remedial fees. For a data controller or processor of major importance, the maximum statutory remedial fee may be the greater of ₦10 million and two per cent of annual gross revenue for the preceding financial year.[20] For organisations outside that category, the applicable standard maximum is the greater of ₦2 million and two per cent of annual gross revenue.[21]

Consequently, ransomware can create a form of "dual exposure": the institution is a victim of criminal conduct but may nevertheless face regulatory consequences if its own handling of personal information fell below legal standards.

3.3 Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as Amended in 2024

The Cybercrimes Act is the principal Nigerian statute addressing conduct associated with ransomware. Its importance lies in the breadth of its provisions.

First, section 6 criminalises specified unauthorised access to computer systems and networks.[22] Ransomware operators frequently obtain unauthorised entry before installing malicious code or acquiring data. Access conducted for purposes of obtaining confidential information, industrial secrets or classified information attracts significant criminal consequences.

Second, section 8 criminalises system interference. A person who, without lawful authority and intentionally or for fraudulent purposes, seriously hinders the functioning of a computer system

[16] Ibid, s 39(1).
[17] Ibid, s 39(2).
[18] Ibid, s 40(2).
[19] Ibid, s 40(3).
[20] Ibid, s 48; Nigeria Data Protection Commission, guidance on enforcement and remedial fees.
[21] Ibid
[22] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended), s 6.

through damaging, deleting, deteriorating, altering or suppressing computer data or other interference commits an offence.[23] Ransomware encryption is an almost paradigmatic form of system interference because its purpose is to prevent the lawful owner or operator from using information or systems according to their intended function.

Third, section 12 deals with unlawful interception of non-public transmissions and computer data.[24] This can become relevant where attackers monitor internal communications or intercept credentials during network compromise.

Fourth, section 13 criminalises computer-related forgery where a person knowingly accesses a computer or network and inputs, alters, deletes or suppresses data so that unauthentic data will be treated as authentic. Nigerian appellate jurisprudence has considered this provision in *Julius v Federal Republic of Nigeria*.[25] Although ransomware is distinguishable from traditional computer forgery, an attack that alters institutional records for fraudulent purposes could invoke this provision.

Fifth, section 22 deals with identity theft and impersonation, including fraudulent use of passwords or other unique identification features. Stolen credentials are frequently central to ransomware operations.

Sixth, the amended section 24 concerning malicious or threatening communications may also have relevance to ransomware extortion. It criminalises specified threats communicated through computer systems, including threats directed at property or reputation for purposes of obtaining money or another thing of value.[26] A threat to release commercially damaging or confidential material unless a company pays money may therefore engage the extortion-related elements of the provision, depending on the facts.

Section 27 additionally extends criminal liability to attempts, conspiracy, aiding and abetting.[27] This is particularly significant for Ransomware-as-a-Service, where multiple persons may perform separate roles in developing malware, acquiring access credentials, negotiating with victims and laundering proceeds.

The Act therefore possesses sufficient breadth to prosecute much of the conduct constituting ransomware without the legislature having created a single offence labelled "ransomware". The challenge lies less in the absence of criminalisation than in attribution, investigation, evidence preservation, international cooperation and prosecution.

3.4 Critical National Information Infrastructure

Ransomware becomes especially serious where it affects systems essential to national security, economic stability, healthcare or public administration.

The Designation and Protection of Critical National Information Infrastructure Order 2024 was made pursuant to the Cybercrimes Act.[28] The Order designates computer systems, networks and communications infrastructure across strategic sectors as Critical National Information Infrastructure. The listed sectors include power and energy, water, information and communications technology, banking, finance and insurance, health, public administration, education, and defence and security.[29]

This represents an important development. An attack on a university network, hospital information system or financial infrastructure may no longer be understood merely as an attack against an individual organisation; depending on the system involved, it may threaten infrastructure legally recognised as nationally critical.

The Order also reflects a shift from reactive criminal prosecution towards preventive cybersecurity governance. Institutions operating designated infrastructure should therefore understand cybersecurity resilience as part of institutional and national-security responsibilities.

[23] Ibid s 8.
[24] Ibid s 12.
[25] Julius v Federal Republic of Nigeria (2021) LPELR/LCN-15094(CA); Cybercrimes Act, s 13.
[26] Ibid s 24 as amended by s 5 of the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024.
[27] Ibid s 27
[28] Designation and Protection of Critical National Information Infrastructure Order 2024, SI No 21 of 2024.
[29] Ibid, para 2 and Schedule.

3.5 National Cybersecurity Policy and Strategy

Nigeria's National Cybersecurity Policy and Strategy 2021 recognises that national dependence on digital infrastructure creates risks to the economy, government and security.[30] It emphasises public-private cooperation, multi-stakeholder engagement, critical-infrastructure protection, capacity building and incident-response mechanisms. Although policy instruments do not necessarily create the same directly enforceable obligations as legislation, they influence the expected standard of institutional governance. They also demonstrate that cybersecurity is no longer viewed by government solely as a specialist technological matter.

This has consequences for institutional leadership. A board of directors, permanent secretary, chief executive, vice-chancellor, hospital administrator or other senior decision-maker cannot reasonably treat severe cyber risks as matters exclusively delegated to junior information-technology personnel. Cybersecurity increasingly concerns enterprise risk, statutory compliance and continuity of essential services.

3.6 Sector-Specific Regulation

Certain private institutions face additional sectoral obligations. Financial institutions provide a useful example. The Central Bank of Nigeria's 2024 Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks sets minimum cybersecurity controls relating to governance, risk management, resilience, monitoring, regulatory compliance and enforcement.[31]

Accordingly, a ransomware attack on a bank may activate several overlapping legal regimes: the Cybercrimes Act concerning the offender, the Nigeria Data Protection Act concerning personal-data security, CBN cybersecurity requirements, contractual obligations to customers and potentially wider financial-sector regulatory duties. The same general principle applies in telecommunications and other regulated industries. Ransomware risk is therefore not governed by a single statute but by a layered framework.

4. Criminal Liability of Ransomware Attackers

The primary criminal responsibility clearly lies with the persons who unlawfully deploy ransomware. Depending upon the attack, multiple offences may arise from one criminal campaign. Unauthorised penetration of a network can create liability under section 6 of the Cybercrimes Act. Encryption and disabling of operational systems can constitute system interference under section 8. Theft of credentials may engage identity-related offences. Interception or copying of communications can create additional liability. Manipulation of records may constitute computer-related forgery. Threats demanding payment may engage the amended provisions dealing with extortionate communications. Persons who assist, conspire or provide operational support may be liable under section 27.

The facts may also support ordinary criminal offences outside the Cybercrimes Act. A ransomware campaign is fundamentally designed to compel a victim to transfer property or money through threats. Depending upon the circumstances and applicable criminal legislation, offences relating to fraud, extortion or obtaining property may therefore arise alongside cybercrime charges.

Furthermore, criminal proceeds do not lose their unlawful character merely because they are received through cryptocurrency. Section 18 of the Money Laundering (Prevention and Prohibition) Act 2022 prohibits, among other things, the conversion, transfer, acquisition, use, retention or control of funds or property where the person knows or reasonably ought to know that they constitute proceeds of unlawful activity.[32] Cryptocurrency received through ransomware can therefore create money-laundering liability when subsequently transferred, converted or concealed.

Ransomware organisations frequently operate through layered payment arrangements intended to obscure the destination of criminal proceeds. Cryptocurrency mixing, intermediary wallets and foreign exchanges may complicate investigations but do not change the underlying legal character of the proceeds.

The Cybercrimes Act also contains important provisions on jurisdiction. Under section 50, the Federal High Court can exercise jurisdiction in circumstances including offences committed within Nigeria

[30] Federal Republic of Nigeria, National Cybersecurity Policy and Strategy 2021.

[31] Central Bank of Nigeria, Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks 2024, replacing the earlier 2018 framework.

[32] Money Laundering (Prevention and Prohibition) Act 2022, s 18

and certain offences committed outside Nigeria where the victim is a Nigerian citizen or resident or where the alleged offender is present in Nigeria and is not extradited.[33] Section 51 makes offences under the Act extraditable, while section 52 authorises mechanisms for international investigative and prosecutorial cooperation.[34]

These provisions are especially important because ransomware is inherently transnational. A Nigerian institution may be attacked by persons operating servers in several countries, demanding payment to a wallet maintained through another jurisdiction and laundering the proceeds elsewhere. Nevertheless, statutory jurisdiction does not eliminate practical enforcement difficulties. Identifying the person behind an IP address, online alias or cryptocurrency wallet may require cooperation from foreign service providers, exchanges and law-enforcement agencies. Even after identification, extradition may depend upon treaty arrangements, domestic laws of the requested state, dual criminality and diplomatic cooperation. The distance between legal jurisdiction and practical custody therefore remains considerable.

5. Legal Implications for Public Institutions

Public institutions occupy a distinctive position because a ransomware incident may interrupt the exercise of statutory functions and compromise large quantities of information entrusted to government.

5.1 Data-Protection Responsibility

Government ministries, departments, agencies, public universities and public healthcare institutions frequently process personal data. The Nigeria Data Protection Act (NDPA) is therefore highly relevant to them. A public institution cannot avoid data-protection obligations simply because it exercises governmental functions. Where ransomware compromises citizen records, the institution must assess its statutory security controls, whether personal data was exposed and whether notification to the NDPC and affected individuals is required.

Sensitive information deserves particular attention. Healthcare data, biometric information and other sensitive categories may expose affected individuals to substantial harm. Public institutions maintaining such data should therefore adopt security controls proportionate to the sensitivity and scale of processing.

The consequences of inadequate protection are not merely administrative. The recognition of data protection within constitutional privacy jurisprudence means that serious mishandling of citizen information may potentially produce fundamental-rights litigation alongside statutory remedies.[35]

5.2 Continuity of Public Services

A ransomware attack may also interfere with the legal duty of a public body to deliver services. Consider a hospital that cannot retrieve patient records, a public university unable to access examination results or a ministry unable to process licences and benefits. The legal concern is no longer confined to the confidentiality of information. The availability of systems becomes central to lawful and effective administration. This reinforces the significance of section 39 of the NDPA, which expressly recognises availability and resilience and contemplates procedures for timely restoration following technical incidents.

The 2024 Critical National Information Infrastructure Order strengthens this obligation conceptually by designating sectors including public administration, education and health. Institutions operating critical infrastructure should therefore maintain tested incident-response plans, segregated backups, alternative communication systems and arrangements for continuing essential operations during a digital outage.

5.3 Accountability for Cybersecurity Governance

A ransomware attack often reveals institutional weaknesses that existed long before the attack: unsupported software, uncontrolled administrator privileges, unpatched vulnerabilities, inadequate network segmentation, absence of multifactor authentication or backups that were never tested. Where such weaknesses result from systemic neglect, questions of administrative accountability arise. Senior

[33] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended), s 50.
[34] Ibid ss 51–52.
[35] Constitution of the Federal Republic of Nigeria 1999, s 37; Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v National Identity Management Commission (n 14).

officers may not personally configure firewalls, but institutional leadership controls budgets, procurement, policy, staffing and risk priorities. Cybersecurity governance should therefore be allocated at management level and incorporated into internal audit and risk-management arrangements.

This should not lead to scapegoating officials whenever sophisticated cybercriminals succeed. Rather, accountability should distinguish between a genuinely unavoidable compromise and a foreseeable risk that remained untreated despite warnings, audits or repeated vulnerabilities.

5.4 Public Disclosure and Transparency

Public institutions may face tension between transparency and operational security after an attack. Premature disclosure of technical details may assist attackers or compromise an investigation. Excessive secrecy, however, can expose citizens to additional harm where stolen data is likely to be exploited. The data-breach notification rules provide one statutory mechanism for balancing these interests. Where thresholds are satisfied, notification cannot simply be avoided to protect institutional reputation. An effective public-sector ransomware policy should therefore identify who is authorised to communicate with the public, the regulator and affected individuals. Concealment should never substitute for incident response.

6. Legal Implications for Private Institutions

Private organisations confront many of the same data-protection obligations but also face contractual, corporate and commercial consequences.

6.1 Regulatory Liability

A private organisation that processes personal information must comply with the NDPA. Following an attack, regulators may examine whether the institution had reasonable access controls, vulnerability-management procedures, security monitoring, staff training, backup arrangements and incident-response processes.

Ransomware is therefore capable of converting cybersecurity deficiencies into measurable regulatory exposure. For organisations designated as controllers or processors of major importance, potentially significant remedial fees may apply.

It is important, however, that regulatory assessment remains proportionate. Security regulation should encourage reasonable prevention without creating the false assumption that every successful attack proves negligence. A competent assessment must consider the sophistication of the attacker, the controls in place, the organisation's response and whether recognised vulnerabilities had been ignored.

6.2 Contractual Liability

A private institution may owe contractual obligations to customers, suppliers or business partners concerning confidentiality, data protection, service availability and cybersecurity.

Cloud-service agreements, outsourcing arrangements and technology contracts often allocate responsibilities for security incidents. A ransomware attack may therefore trigger disputes concerning which party was responsible for patching software, maintaining backups, monitoring systems or notifying affected customers.

The increase in outsourced technology creates particular legal complexity. An organisation may store information with a third-party processor but remain the data controller. Section 29 of the NDPA requires appropriate arrangements between controllers and processors and obliges organisations engaging processors to ensure relevant data-protection requirements are satisfied.[36]

Consequently, outsourcing infrastructure does not amount to outsourcing legal responsibility. Organisations should ensure that technology contracts contain meaningful cybersecurity clauses, incident-notification timelines, cooperation requirements, audit rights, recovery obligations and clear allocation of liability.

6.3 Negligence and Duty of Care

A ransomware victim may also face civil claims where third parties suffer foreseeable loss because reasonable security precautions were not adopted. Nigerian tort law generally requires proof of a duty of care, breach, causation and damage.

The difficult question is determining the content of reasonable care in a cybersecurity environment. Reasonableness cannot mean perfect security. Rather, factors may include the sensitivity of the

[36] Nigeria Data Protection Act 2023, s 29.

information, known threats, applicable regulatory standards, previous incidents, industry practices, cost and feasibility of protective measures.

The NDPA's risk-based security provisions may influence this assessment. Failure to comply with a statutory security obligation can provide powerful evidence concerning the expected standard, although statutory breach and tortious negligence remain analytically distinct.

Causation may be contested. A defendant organisation may argue that the deliberate criminal act of an independent attacker caused the claimant's loss. The claimant may respond that the criminal intervention was precisely the foreseeable risk against which reasonable cybersecurity precautions were required. Courts will therefore need to examine the factual relationship between the organisation's deficiencies and the attacker's success.

6.4 Corporate Governance

Cybersecurity has increasingly become a corporate-governance issue. Boards and senior executives are responsible for identifying material risks to the organisation. Where an enterprise depends heavily upon computer systems, ransomware can produce prolonged business interruption, regulatory sanctions, litigation and reputational damage.

A board that receives repeated warnings about critical vulnerabilities but refuses reasonable remediation without proper risk assessment may create governance concerns. Directors are not expected to possess specialist cybersecurity expertise, but they should obtain competent advice and ensure that appropriate structures exist.

Relevant questions include whether the organisation maintains an incident-response plan, conducts regular security testing, identifies critical assets, uses multifactor authentication, maintains tested offline or segregated backups and periodically assesses third-party risks. The legal significance is that cyber resilience can no longer reasonably be treated solely as a discretionary technical expenditure.

6.5 Cyber Insurance

Cyber insurance may transfer part of the financial consequences of ransomware, including business interruption, forensic investigation, legal expenses and, depending on policy terms and law, extortion-related costs. Research nevertheless shows that ransomware has considerably affected the cyber-insurance market and led insurers to demand stronger security controls from policyholders.[37]

An institution must carefully review policy conditions. Material misrepresentation concerning security practices, failure to comply with specified controls, late notification or exclusions relating to sanctions, war or unapproved ransom payments may affect coverage. Insurance should therefore complement rather than replace cybersecurity. Where recovery depends exclusively upon insurance and ransom payment, the institution remains operationally vulnerable.

7. The Legal Challenge of Ransom Payments

One of the most difficult issues arising after a ransomware attack is whether the victim should pay. From an operational perspective, an institution may believe payment offers the fastest means of restoring essential systems or preventing disclosure of sensitive information. Yet payment creates major legal, ethical and policy risks.

First, there is no guarantee that criminals will provide a functioning decryption tool or delete stolen information. The institution may pay and remain unable to recover. Second, payment finances the ransomware economy and demonstrates that attacks can be profitable. This may encourage future attacks. Third, payment may create serious anti-money-laundering or counter-terrorism concerns depending upon the identity of the recipient. The Terrorism (Prevention and Prohibition) Act 2022 prohibits the provision of funds where a person has the requisite knowledge or reasonable grounds to believe that funds will be used to finance terrorism or a terrorist organisation.[38] Where a ransomware group or recipient is associated with a proscribed or sanctioned entity, payment can therefore create significant legal exposure.

---

[37] Gareth Mott and others, 'Between a Rock and a Hard(ening) Place: Cyber Insurance in the Ransomware Era' (2023) 128 Computers & Security <https://doi.org/10.1016/j.cose.2023.103162> accessed 8 August 2026; Tom Baker and Anja Shortland, 'Insurance and Enterprise: Cyber Insurance for Ransomware' (2023) 48 Geneva Papers on Risk and Insurance-Issues and Practice 275 <https://doi.org/10.1057/s41288-022-00281-7> accessed 8 August 2026.

[38] Terrorism (Prevention and Prohibition) Act 2022, particularly ss 2 and 21–23.

A ransom should consequently never be treated as an ordinary commercial invoice. Institutions considering payment should undertake legal and sanctions due diligence, involve competent law-enforcement and cybersecurity authorities and preserve an auditable record of decision-making.

The absence of a comprehensive Nigerian ransomware-payment statute creates uncertainty. Nigerian law does not presently establish a general rule that every ransomware payment by every victim is automatically lawful or automatically prohibited. Its legality will depend on surrounding facts and applicable criminal, terrorism-financing, sanctions, financial and regulatory law.

Comparative developments demonstrate increasing international debate over whether governments should prohibit or restrict ransom payments, particularly by public bodies and critical infrastructure. Recent scholarship has analysed the advantages and difficulties associated with payment bans, including the danger that an absolute prohibition could create severe consequences where essential services cannot otherwise be restored.[39]

Nigeria would benefit from express national guidance specifying the circumstances in which payment is prohibited, the approvals or reporting obligations applicable to contemplated payments and the treatment of insurers, negotiators and virtual-asset intermediaries.

For public institutions, the argument for stricter rules is particularly strong because payment involves public resources and may directly finance criminal enterprises. A public body should not possess unrestricted discretion to transfer public funds to anonymous cybercriminals.

8. Electronic Evidence, Investigation and Attribution

Successful ransomware prosecution depends upon evidence. Relevant evidence may include system logs, emails, malware files, ransom notes, cryptocurrency wallet addresses, server records, authentication logs, forensic images and communications between attackers and victims.

Electronic evidence in Nigerian proceedings must satisfy applicable evidentiary rules, including the Evidence Act's requirements governing computer-generated evidence.[41] Incident response should therefore preserve forensic integrity from the outset.

An institution that immediately wipes compromised systems without first preserving relevant evidence may unintentionally hinder investigation. Conversely, leaving infected systems connected merely to preserve evidence may increase operational damage. Incident-response planning should reconcile both concerns through forensic imaging and professional evidence handling.

Chain of custody is particularly important. Investigators should document who collected evidence, how it was acquired, when it was transferred and whether the data remained unchanged.

Attribution remains one of the greatest challenges. Ransomware groups deliberately conceal identity through anonymisation networks, compromised infrastructure, false identities, cryptocurrency and servers distributed across several countries.

The Cybercrimes Act's extraterritorial jurisdiction and mutual-assistance provisions are valuable in this regard, but their effectiveness depends upon cooperation. International partnerships between Nigerian authorities, foreign law-enforcement agencies, cybersecurity companies, telecommunications providers and cryptocurrency platforms are therefore essential.

Nigeria's participation in multinational cybercrime enforcement initiatives demonstrates the growing importance of such cooperation. Nevertheless, institutional capacity remains critical. Cyber investigators, prosecutors and judges require specialised technical competence to interpret digital evidence without sacrificing procedural fairness.

9. Challenges in Nigeria's Existing Legal Framework

Although Nigeria possesses substantial cybercrime legislation, several challenges limit its effectiveness against ransomware.

9.1 Absence of a Ransomware-Specific Statutory Framework

[39] Fabian Teichmann, 'International Legal Responses to Ransomware: Toward a Ban on Payments?' (2026) 7 International Cybersecurity Law Review 41 <https://doi.org/10.1365/s43439-025-00167-z> accessed 8 August 2026; Melanie K Worsley, Joseph Kendall-Morwick and Kate A Houston, 'Change Waits for No One: An Examination of the Legal Response to Ransomware Attacks' (2025) Criminal Justice Policy Review <https://doi.org/10.1177/08874034251363431> accessed 8 August 2026.

Existing offences can criminalise ransomware conduct, but the legal regime remains fragmented. No integrated statutory scheme currently addresses ransomware reporting, ransom-payment decisions, negotiation intermediaries, insurer obligations, victim cooperation and cryptocurrency tracing as a unified subject.

A technology-neutral criminal law is desirable because ransomware techniques evolve rapidly. Nevertheless, technology neutrality does not prevent the creation of procedural and regulatory rules specifically addressing ransomware incidents.

9.2 Fragmented Institutional Responsibilities

A significant attack may involve ngCERT, the Office of the National Security Adviser, law-enforcement agencies, the NDPC, sector regulators and possibly the Nigerian Financial Intelligence Unit. Multiple institutions can strengthen oversight, but poorly coordinated jurisdiction can create duplication or delay. Victim organisations should not be left uncertain about whom they must notify during an emergency. Nigeria therefore needs an integrated ransomware incident-reporting protocol specifying lead agencies, notification thresholds, information-sharing arrangements and confidentiality protections.

9.3 Underreporting

Organisations frequently fear reputational damage following cyber incidents. This creates an incentive to conceal attacks, particularly where services are quickly restored. Underreporting undermines national cybersecurity because government cannot accurately assess threat patterns. It also prevents other organisations from learning about attack methods.

The NDPA's 72-hour rule addresses qualifying personal-data breaches but does not necessarily create a universal ransomware-reporting obligation for every institutional ransomware incident. A ransomware attack that substantially disrupts critical services yet demonstrably involves no personal-data compromise illustrates the gap. A dedicated reporting requirement for significant ransomware incidents affecting critical infrastructure would therefore be appropriate.

9.4 Cross-Border Enforcement

Jurisdiction on paper does not automatically result in arrests. Some ransomware groups operate from jurisdictions where law enforcement cooperation is limited. Digital infrastructure can be moved rapidly and cryptocurrency proceeds transferred across borders. Nigeria must therefore strengthen mutual legal assistance, rapid evidence-preservation mechanisms and relationships with foreign cybercrime units.

9.5 Cybersecurity Capacity

Legal rules are ineffective where institutions lack the technical expertise required to comply. Public bodies may face outdated systems, inadequate budgets, procurement delays and shortages of specialised personnel. Recent scholarship examining Nigeria's cybersecurity framework has similarly identified implementation, coordination and capacity challenges notwithstanding the existence of significant legislation and policy.[40] A sustainable legal framework must therefore address capacity, not merely punishment.

9.6 Uncertainty Concerning Ransom Payments

Perhaps the greatest policy gap concerns payment. Organisations need clear guidance regarding when payment is prohibited, when law-enforcement consultation is mandatory, how sanctions screening should occur and whether public institutions may ever pay. Without guidance, decisions may be made under intense operational pressure and without adequate legal scrutiny.

9.7 Third-Party and Supply-Chain Risks

Modern organisations depend on cloud providers, software vendors and managed-service providers. The ngCERT warning of July 2024 concerning attacks against critical cloud-service providers illustrates the potential systemic consequences of compromising one technology provider whose clients span several critical sectors. Cybersecurity law must therefore focus not only upon individual organisations but also upon supply-chain concentration and service-provider obligations.

[40] Polra Victor Falade and Oluwafemi Osho, 'Nigeria's Digital Sovereignty: Analysis of Cybersecurity Legislation, Policies, and Strategies' (2025/2026), discussing implementation, coordination, capacity and legislative challenges in Nigeria's cybersecurity environment <https://doi.org/10.48550/arXiv.2601.06050> accessed 12 August 2026

10. RECOMMENDATIONS

10.1 Adopt a National Ransomware Response Framework

Nigeria should develop a dedicated national ransomware response framework. This need not replace the Cybercrimes Act. Rather, it should coordinate existing laws and provide clear procedures for public and private institutions. The framework should define reportable ransomware incidents, identify responsible authorities, establish escalation procedures and clarify cooperation among ngCERT, law-enforcement agencies, NDPC and sector regulators.

10.2 Mandatory Reporting for Significant Ransomware Incidents

Significant ransomware attacks affecting Critical National Information Infrastructure should be subject to mandatory reporting even where personal data has not been compromised. The purpose should not simply be punitive. Reporting enables threat intelligence, coordinated response and national situational awareness. Reports should be protected appropriately to encourage candid cooperation, while deliberate concealment of a material attack against critical infrastructure should attract regulatory consequences.

10.3 Clarify the Law on Ransom Payments

Nigeria should issue statutory or authoritative regulatory guidance on ransomware payments.

At minimum, the framework should require:

- sanctions and terrorism-financing screening;
- law-enforcement notification before specified payments;
- documented approval by appropriate institutional leadership;
- enhanced rules governing expenditure of public funds;
- reporting of cryptocurrency wallet information; and
- disclosure of payments by insurers or professional negotiators where legally permitted.

An outright prohibition on every payment may be inappropriate without careful study because exceptional cases could involve risks to life or essential services. However, unrestricted payment discretion is equally undesirable.

10.4 Strengthen Cybersecurity Governance

Public and private institutions should formally integrate cybersecurity into enterprise risk management.

Boards and accounting officers should receive regular cybersecurity reports. Institutions should document risk assessments, remediation decisions and residual risk.

At a technical level, reasonable baseline controls should include multifactor authentication, least-privilege access, prompt patch management, endpoint monitoring, network segmentation, secure configuration and tested backup systems.

A particularly important ransomware defence is maintaining backups that attackers cannot easily delete or encrypt. Merely stating that backups exist is insufficient; restoration procedures should be periodically tested.

10.5 Strengthen Data-Protection Compliance

Institutions should treat the NDPA's security provisions as continuing obligations rather than paperwork completed once a year. Data inventories should identify what personal information exists, where it is stored, who can access it and how long it is retained. Information that is no longer required should be securely deleted because unnecessary data retention increases the consequences of ransomware exfiltration.

Institutions processing high-risk information should conduct appropriate data-protection impact and security risk assessments. Incident-response plans should incorporate the 72-hour NDPC notification requirement so that technical teams immediately involve legal and privacy personnel when a compromise is discovered.

10.6 Improve Public-Sector Resilience

Public institutions should receive minimum cybersecurity standards based on the sensitivity and criticality of services they provide. Legacy systems present a particular problem. Government cybersecurity budgets should therefore prioritise essential systems according to risk rather than attempt to replace every system simultaneously.

Critical institutions should maintain offline operational procedures for limited continuation of essential functions during network outages. Hospitals, for example, require arrangements for urgent patient care when electronic systems are unavailable.

10.7 Improve Third-Party Risk Management

Contracts with cloud providers, software suppliers and managed-service companies should contain enforceable cybersecurity provisions. Institutions should require appropriate security standards, timely incident notification, cooperation with forensic investigations, backup arrangements, data-return procedures and appropriate allocation of liability. A supplier's cybersecurity weaknesses can become the customer's legal problem where the customer's data or services are affected.

10.8 Develop Specialist Cybercrime Capacity

Nigeria should continue investing in specialist digital forensic investigators and prosecutors. Judicial training is equally important because ransomware cases may involve complex technical evidence, cryptocurrency tracing and requests for international cooperation. Dedicated or specially trained cybercrime prosecution teams could improve consistency in charging decisions and ensure that appropriate provisions of the Cybercrimes Act are used.

10.9 Strengthen International Cooperation

Sections 50–52 of the Cybercrimes Act provide a useful legal foundation for extraterritorial enforcement and cooperation. These provisions should be complemented by operational relationships allowing rapid preservation of foreign-hosted evidence.

Nigeria should expand participation in international cybercrime operations and establish direct points of contact with major digital-service and virtual-asset providers where permitted by law.

The speed of cooperation is critical because electronic evidence can disappear rapidly.

10.10 Encourage Responsible Cyber Insurance

Cyber insurance should be encouraged as part of comprehensive risk management rather than treated as a substitute for security. Regulators may consider guidance encouraging insurers to verify minimum security standards and to share anonymised threat information.

Policies covering extortion payments should expressly require compliance with Nigerian criminal, terrorism-financing and sanctions law. Insurers should not create incentives for automatic ransom payment where restoration from clean backups would be safer and more sustainable.

10.11 Establish Institutional Incident-Response Teams

Every significant public and private institution should maintain an incident-response structure involving information technology, cybersecurity, legal, communications, management and data-protection personnel.

The first hours following detection are decisive. An institution should already know who has authority to isolate systems, contact law enforcement, engage forensic experts, communicate with regulators, notify insurers and authorise public statements.

Testing the plan through simulation exercises is essential. A ransomware response plan that has never been tested may fail precisely when it is needed.

11. CONCLUSION

Ransomware is no longer simply malicious software that locks computer files. It has developed into a sophisticated form of organised digital extortion capable of disrupting government administration, healthcare, banking, telecommunications, education and ordinary commercial activity. Nigeria's increasing dependence upon digital infrastructure means that the legal significance of such attacks will continue to grow.

Nigeria already possesses important legal tools. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended in 2024, criminalises many of the acts through which ransomware campaigns are carried out, including unauthorised access, system interference, unlawful interception, identity-related offences, threatening communications, conspiracy and aiding or abetting. Its jurisdictional and international-cooperation provisions are particularly important for cross-border attacks.

The Nigeria Data Protection Act 2023 creates another dimension of responsibility. Public or private institutions affected by ransomware are not automatically liable simply because an attacker penetrated their systems. They may, however, face regulatory consequences where they failed to implement appropriate technical and organisational measures or neglected applicable breach-notification requirements. The constitutional recognition of privacy and the Court of Appeal's recognition of data-protection interests further strengthen the legal significance of protecting personal information.

The 2024 Critical National Information Infrastructure Order is also a major development because it expressly recognises the strategic importance of systems supporting sectors including banking, health,

education and public administration. Ransomware targeting such infrastructure is therefore capable of affecting not merely an individual victim but national economic and social stability.

Nevertheless, Nigeria lacks an integrated ransomware-specific framework for institutional reporting, ransom payments and coordinated incident response. Cross-border attribution and enforcement remain difficult, public institutions frequently face cybersecurity capacity constraints and dependence on third-party technology introduces systemic risks.

The appropriate response is therefore not simply to enact harsher criminal penalties. Nigeria requires a coordinated model combining effective criminal enforcement, data-protection compliance, critical-infrastructure resilience, institutional accountability, technical capacity, international cooperation and clearer rules concerning ransom payments.

Ultimately, the most important legal lesson arising from ransomware is that cybersecurity is no longer optional institutional good practice. For organisations responsible for public services, customer information, financial assets or critical infrastructure, cyber resilience has become part of legal compliance, responsible governance and the protection of fundamental rights.