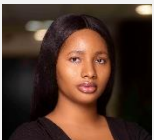


Key contacts



Cyriacus C Orlu
Partner,
Dispute Resolution
cyriacus.orlu@templars-law.com



Pamela Ojiego
Associate,
Finance
pamela.ojiego@templars-law.com

TEMPLARS ThoughtLab

Managing Cyber Disputes in Nigeria's Digital Economy

Introduction

As the transition towards a fully digital economy continues to gain traction globally and within the Nigerian commercial space, the resolution of cyber-related disputes has become one of the most pressing issues for businesses operating in the Nigerian market¹. Cases of cyberattacks, ransomware, unsolicited data intrusion, amongst other cybersecurity breaches have become a regular menace affecting businesses in today's cyberspace². As Nigeria embraces digitization at swift pace, businesses are now dealing with loads of sensitive personal data as well as online transactions which of course, make them prime victims of cybercrime activities³ or cybersecurity breaches. While response capabilities to cyber incidents are important, there are also legal questions emanating from the incidents that businesses may have to contend with, particularly relating to how disputes around such events can be resolved. It is against the foregoing that this article sets out to discuss how Nigerian businesses can approach cyber-related disputes through the various dispute resolution mechanisms: mediation, arbitration, or litigation. The article will conclude by providing practical strategies for Nigerian businesses to manage cybersecurity disputes.




¹ Samson Akintaro, 'Shortage of Cybersecurity Skills Threatens Nigeria's Digital Economy—Adewale Obadare' (*Nairametrics* 18 November 2024) <<https://nairametrics.com/2024/11/18/shortage-of-cybersecurity-skills-threatens-nigerias-digital-economy-adewale-obadare/>> accessed 20 November 2024.

² Wasyihun Sema Admass, Yirga Yayeh Munaye and Abebe Abeshu Diro, 'Cyber Security: State of the Art, Challenges and Future Directions' (2024) *Cyber Security and Applications* volume 2, 100031 <[Cyber security: State of the art, challenges and future directions - ScienceDirect](#)> accessed 06 April 2025

³ Nwachukwu Ugbomah, Nduka Omede and Obi Ugochukwu, 'Cybercrime: Predictive Impact on E-Commerce in Nigeria' (2022) 1 | *Scholarly Journal of Social Sciences Research* 2955.

The Growing Threat of Cybersecurity Incidents for Nigerian Businesses

Many businesses in Nigeria have increasingly come to embrace digital technologies with the primary aim of increasing their operational effectiveness and interactions with customers⁴. However, while this holds great benefits for profitability and efficiency, it also leaves these businesses vulnerable to cyberattacks. According to a 2023 National Information Technology Development Agency (NITDA) report, cybercrime negatively affects the Nigerian economy, leading to the loss of billions of naira every year. Based on the NITDA report, during the year under review, Nigeria, South Africa, Egypt and Kenya accounted for 60% of the \$4 billion annual cost of cybercrime in Africa⁵. These include data breaches, ransomware, and system intrusion, each with possible impacts of operational disruption, financial loss, reputational damage, and potential litigation. Lawsuits and increased regulatory scrutiny almost invariably follow, especially if consumer data has been compromised or service delivery has been disrupted. According to the International Institute for Conflict Prevention and Resolution, over ninety-five percent of all business information is in digital format, and that paradigm presents a host of potential dispute issues⁶. Hence, the discourse on the various approaches to resolving such cyber-related disputes becomes inevitable.

Resolution Type	Key Attributes	Best Used When	Legal Backing
 Mediation	Confidential, non-confrontational, fast	Parties want privacy and cooperation	AMA 2023, Lagos Multi-Door Courthouse
 Arbitration	Confidential, expert-driven, enforceable	Technical or cross-border cyber issues	AMA 2023, LCIA (UK), AAA (US)
 Litigation	Public, binding, regulated	High-stakes, criminal, public policy issues	Cybercrimes Act 2015, Data Protection Act 2023

Mediation: A Flexible, Client-Centric Approach

Mediation enjoys a burgeoning reputation as an effective and go-to means for the resolution of cybersecurity disputes as it helps organizations resolve their disputes away from the eyes of the public in a non-confrontational way, as opposed to the traditional route of litigation⁷. This is quite useful in cases where one of the parties is exposed to reputational damage or highly technical disagreement in which both parties want to minimize exposure.

⁴ Franklin Nakpodia and others, 'Digital Technologies, Social Entrepreneurship and Resilience during Crisis in Developing Countries: Evidence from Nigeria' (2023) 30 International Journal of Entrepreneurial Behaviour & Research.

⁵ Zakariyya Adaramola, 'How Cyber-Attacks Exposed Nigeria's IT Security Vulnerability in 2023 - Daily Trust' (<https://dailytrust.com/28-December-2023/<https://dailytrust.com/how-cyber-attacks-exposed-nigerias-it-security-vulnerability-in-2023/>> accessed 22 November 2024)

⁶ Kenneth N Rashbaun, 'Mediation of Cyber Disputes: ADR Moves into the Digital Age' <CyberArticle.pdf> accessed 22 November 2024.

⁷ Kenneth Rashbaum, 'Mediation of Cyber Disputes: ADR Moves into the Digital Age as Originally Appeared in Law360' (2017) <CyberArticle.pdf> accessed 22 November 2024.

In Nigeria, the Arbitration and Mediation Act 2023 (the AMA) is the principal National legislation regulating the practice of mediation in the country. In terms of the mediation architecture, the Lagos Court of Arbitration and Multi-Door Courthouses across various States of the federation where the facility exists, offer their platforms to conduct mediation with instituted frameworks that have provisions for alternative dispute resolution⁸. For instance, the Lagos Multi-Door Courthouse has embedded mediation within the mainstream process of dispute resolution, offering mediation as early before court litigation. Mediation is particularly effective for resolving cybersecurity disputes, as it allows the parties to collaboratively determine appropriate compensation or corrective measures⁹. This is especially useful where the wrongdoer (such as a service provider) acknowledges responsibility for a breach, or where both parties seek a mutually agreeable resolution without the complexities of a trial.

Internationally, mediation has also proven to be effective in cyber disputes. In the United Kingdom, the Centre for Effective Dispute Resolution (CEDR) has drafted rules that cater for cyber-related dispute mediation¹⁰, and in the United States, the American Arbitration Association (AAA) offers ADR services that help in unknotting complex cybersecurity claims¹¹.

For Nigerian businesses, adopting mediation for the resolution of cybersecurity disputes can offer flexibility and confidentiality, effectively addressing the sensitivities surrounding data breaches.

Arbitration: A Structured Yet Confidential Resolution Process

While arbitration is more formal than mediation, it retains one great advantage: confidentiality¹². In cybersecurity disputes, arbitration ensures that parties benefit from the technical knowledge of the arbitrators, especially in cases where resolution is faster than adjudication in court¹³. Most cyber disputes, especially cross-border data breaches or ransomware, involve technology that requires technical knowledge that is not easily available from regular courts.

In Nigeria, the AMA is also the principal National legislation regulating arbitration proceedings in the country. Section 1 of the Act allows Nigerian companies to insert arbitration clauses in agreements, including those entered with IT companies, cybersecurity firms, and other service providers. As an example, when a Nigerian company contracts with a European cybersecurity company to install systems for securing data, it may include an arbitration clause to resolve dispute(s) that may arise from the contract through arbitration.

Comparing what obtains in Nigeria with the UK and the US, both jurisdictions are increasingly incorporating arbitration clauses for resolving cybersecurity issues. In the UK, the London Court of International Arbitration (LCIA) has offered mechanisms which address complicated and cross-

⁸ Olusola Joshua Olujobi and others, 'Commercial Dispute Resolution: Has Arbitration Transformed Nigeria's Legal Landscape?' (2018) IX Journal of Advanced Research in Law and Economics (JARLE) 204 <<https://www.cceol.com/search/article-detail?id=695051>> accessed 22 November 2024.

⁹ These cyber security disputes do not include cybercrimes in Nigeria, as mediation cannot be employed as a means of resolving crimes, cybercrimes inclusive.

¹⁰ CEDR, 'Centre for Effective Dispute Resolution Mediator Guide to Online Mediation Guide to Online Mediation' (2020) <<https://www.cedr.com/wp-content/uploads/2020/03/Mediator-Guide-to-Online-Mediation-1.pdf>> accessed 22 November 2024.

¹¹ American Arbitration Association, 'AAA Cybersecurity & Data Privacy | ADR.org' (Adr.org2024) <<http://www.adr.org/TechnologyServices>> accessed 22 November 2024.

¹² Vancouver International Arbitration Centre, 'Difference between Arbitration and Mediation – VanIAC' (vaniac.org2024) <<https://vaniac.org/mediation/what-is-mediation-arbitration/difference-between-arbitration-and-mediation/>> accessed 22 November 2024.

¹³ Magdalena Lagiewska, 'New Technologies in International Arbitration: A Game-Changer in Dispute Resolution?' (2023) 37 International Journal for the Semiotics of Law – Revue internationale de Semiotique juridique 851-864. <<https://www.tandfonline.com/doi/pdf/10.1080/17445019.2024.2311111>> accessed 25 March 2025

border cyber-related disputes¹⁴. In the US, the Federal Arbitration Act encourages arbitration for issues involving technology and cybersecurity, thus helping organizations resolve various issues without having to go through burdensome court procedures¹⁵. In South Africa¹⁶ and Ghana¹⁷, arbitration along with the court system is preferred for the resolution of commercial disputes, even though the regions are yet to put in place normative frameworks that specifically deal with cyberspace related issues. Nigerian businesses may find it useful to implement and take advantage of arbitration regimes that are swift, specialized, and enforceable across borders.

Litigation: An Option for High-Stakes or Public Accountability

Notwithstanding the advantages presented by ADR mechanisms, there are cybersecurity disputes that necessitate the use of litigation. The resort to litigation is often inevitable in certain instances, notably: for cyber offences or cybercrimes, or disputes arising from public policy issues or where there has been no resolution reached with mediation thus, the parties seek a resolution that is irrevocably binding.

In Nigeria, the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 (the Cybercrime Act) provides a legal framework for prosecuting cyber-related offenses. Section 24 of the Cybercrime Act for instance, makes it an offence to gain access and alter data without permission, which may lead to disputes. The Nigerian Data Protection Act, 2023 also protects the right of data subjects to their data, such that data controllers will require the consent of the data subject before processing the data¹⁸. Caselaw jurisprudence as mirrored by decisions such as *Ezugwu Emmanuel Anene v. Airtel Nigeria Ltd*¹⁹ and *FRN vs Wilfred Fajemisin*²⁰ all reflect the willingness of Nigerian courts to deal with infractions of the Cybercrime Act, indicating the subsisting relevance of litigation in the resolution of cybersecurity disputes and infractions in Nigeria.

However, the Nigerian judiciary still grapples with some litigation challenges such as lack of adequate capacity development amongst judges and protracted delays in the determination of court cases²¹ and these shortcomings in our opinion, could equally plague and make the litigation of cyber related issues unattractive. On the other hand, the courts in the UK have greatly improved in dealing with challenges associated with cybersecurity litigation. The implications of the case of *Lloyd v Google LLC*²² for data protection litigation were significant, as it offered grounds for new action and pioneered mechanisms for group claims for infringement of privacy. Similarly, the US has

¹⁴ Jacomijn van Haersolte-van Hof and Romilly Holland, <Chapter 3 What makes for Effective Arbitration? A Case Study of the London Court of International Arbitration Rules in: International Organizations and the Promotion of Effective Dispute Resolution> accessed 20 March 2025.

¹⁵ Paul J. Morrow, 'Cybersecurity and Artificial Intelligence Dispute Resolution: From Contention to Synergy' <[65839357b20ba.pdf](#)> accessed 20 March 2025

¹⁶ 'Dispute resolution practices progressing across the continent' <[Dispute resolution practices progressing across the continent](#)> accessed on 20 March 2025

¹⁷ Gwendy Miranda Bannerman, Nana Ama Botchway, Achia Akobour Debrah 'Arbitration in Ghana' <[Ndowuona - Arbitration in Ghana](#)> accessed on 20 March 2025

¹⁸ Section 26 of the NDPA 2023

¹⁹ FCT/HC/CV/545/2015 (Unreported). Where the court considered the provisions of section 26 of the NDPA 2023 and awarded 5 million naira against Airtel for disturbing Mr Anene's telephone line with unsolicited messages.

²⁰ FCT/HC/CV/545/2015 (Unreported). where the accused person was found to have fraudulently impersonated himself online with the intent to defraud unsuspecting foreign nationals under false pretence and was sentenced further to the Cybercrime Act.

²¹ Muiz Adeyemi Banire, 'The Challenges of The Judiciary in Contemporary Nigeria' (2021)

[https://mabandassociates.com/pool/THE%20CHALLENGES%20OF%20THE%20JUDICIARY%20IN%20CONTEMPORAR Y%20NIGERIA.pdf](https://mabandassociates.com/pool/THE%20CHALLENGES%20OF%20THE%20JUDICIARY%20IN%20CONTEMPORAR%20NIGERIA.pdf) accessed 23 November 2024.

²² [2021] UKSC 50. the UK Supreme Court held that representative actions for data breaches under the Data Protection Act 1998 require proof of individual damage, rejecting "loss of control" alone as a basis for compensation. While the claim failed, the case spotlighted the challenges and potential for group claims in UK data protection litigation. † sparked renewed discussions on the need for legislative reform to allow for collective redress mechanisms in data protection breaches, similar to class actions in jurisdictions like the US.

seen major cyber-related court cases, including Equifax Data Breach Litigation²³, which highlights the courts' capacity to impose substantial penalties for cybersecurity failures.

Strategies for Nigerian Businesses to Manage Cybersecurity Disputes

Nigerian business could better manage cybersecurity disputes arising from their business activities by adopting the underlisted measures:

Include ADR Clauses in Cyber-related Contracts: Nigerian businesses must ensure that third-party vendor arrangements and cybersecurity service contracts include ADR clauses such as arbitration and mediation. These types of disputes inform cyber incidents can be effectively managed through well-considered and good written contract provisions. **Adopt Comprehensive Cybersecurity Policies:** The implementation of proactive cybersecurity measures minimizes the chances of conflict occurrence. Conducting frequent security review, training of personnel, and the adherence to the Nigeria Data Protection Act can avert such threats in advance, thus equipping the stakeholders against the impending attack.

Leverage Industry Expertise in Dispute Resolution: Involving skilled professionals in cyber dispute resolution like arbitrators with an IT background or forensic experts, can lead to better results. Organizations that are experiencing cyber-related disputes ought to procure expert legal advice, taking into account the best practices from other jurisdictions such as the UK, US, Ghana, and South Africa.

Stay Updated on Regulatory Developments: It is imperative for Nigerian business people to pay attention to changes in the laws, especially the Cybercrimes Act and the Nigerian Data Protection Act, and any other regulations that apply. Following local and global business norms lowers the chances of legal risks, while also improving the level of defenses that may be needed if a conflict arises.

Utilize Insurance for Cyber Incidents: Cyber liability insurance is becoming a more popular means of dealing with the economic effects of cyber incidents. The culture of insurance can help cover and cushion expenses or costs associated with settling cybersecurity disputes.

Conclusion

The growth of the Nigerian digital economy and the increased involvement of businesses in the space, comes with a corollary risk of cyber-related incidents and disputes. However, with resolution techniques such as mediation, arbitration, and litigation, Nigerian businesses would be in a better place to deal with these issues. Drawing from international practices, these businesses can learn to incorporate ADR clauses, leverage industry expertise, and adhere to regulatory standards, creating a more resilient approach to cyber disputes. Furthermore, employing the appropriate measures, Nigerian businesses can safeguard their interests and lessen the impacts of such challenges during this era of high digital activity.

²³ Federal Trade Commission, 'Equifax Data Breach Settlement' (Federal Trade Commission, February 2024) <<https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement>> accessed 22 November 2024.