African Journal of Applied Research
Vol. 11, No. 1 (2025), pp.786-813
http://www.ajaronline.com
https://doi.org/10.26437/ajar.v11i1.
Received: July 23, 2024
Peer reviewed: September 7, 2024
Revised: November 10, 2024
Published: January 2025

CYBERSECURITY AND BUSINESS SURVIVAL IN NIGERIA: BUILDING CUSTOMER'S TRUST

Onatuyeh, E. A.[1], Oghorodi, D.[2], Okpako, E. A.[3], Ojei, E.[4], Osakwe, G.[5], Chinedu, N. B.[6], Okoh, S. K.[7], Odu, V. C.[8], Chinedu, P. U.[9] and Nwankwo, W.[10]

[1]*Department of Accounting, Delta State University of Science and Technology, Ozoro, Nigeria.*
[2]*Department of Computer Science, Delta State University of Science and Technology, Ozoro, Nigeria.*
[3]*Department of Cyber Security, University of Delta, Agbor, Nigeria.*
[4]*Department of Software Engineering, Delta State University of Science and Technology, Ozoro, Nigeria.*
[5&10]*Department of Cyber Security, Delta State University of Science and Technology, Ozoro, Nigeria.*
[6]*Department of Industrial Chemistry, Delta State University of Science and Technology, Ozoro, Nigeria.*
[7]*Delta State University of Science and Technology, Ozoro, Nigeria.*
[8]*West African Examinations Council, Lagos, Nigeria.*
[9]*Department of Information Technology, Delta State University of Science and Technology, Ozoro, Nigeria.*
[1]*edwin.onatuyeh@yahoo.com*

ABSTRACT

Purpose: This paper investigates the role of cybersecurity in ensuring business survival and fostering customer trust in Nigeria.

Design/Methodology/Approach: A qualitative documentary review approach was employed, analysing legislations, policies, standards, and regulations related to cybersecurity from 2000 to 2024, especially those instruments that impact business survival in Nigeria and beyond. The study utilised thematic and comparative analysis to extract insights and identify gaps in the existing frameworks.

Findings: The research reveals that while existing legal instruments on cybersecurity provide a foundational framework for protecting businesses, legislative, enforcement, compliance, and awareness gaps persist across the socioeconomic sphere, hence the continued losses from cyber threats and attacks. Businesses with robust cybersecurity practices were reported to enjoy higher customer trust and operational sustainability levels. However, weak compliance and inadequate awareness hinder the full potential of these measures.

Research Limitation: The study is limited to a thematic review of existing documents, which may not fully capture real-time business practices and challenges.

Practical Implication: Strengthened cybersecurity measures promote trust in digital transactions, reduce the risk of cybercrime, and ensure the continuity of businesses, contributing to economic stability and improved consumer confidence in Nigeria's digital economy.

Social Implication: The findings provide actionable recommendations for policymakers to enhance the effectiveness of cybersecurity legislation and for business leaders to adopt best practices in securing their operations and building trust.

Originality/Value: It contributes to existing knowledge by linking robust cybersecurity practices with enhanced customer trust and operational sustainability.

Keywords: *Business survival. customer trust. cybersecurity. data protection. Nigeria*

INTRODUCTION

Trust is a fundamental currency in digital transformation, as transparency directly impacts business credibility (Venkatraman, 2024). A company can lose 30% of its value if trust is compromised, while a 10% increase in trust correlates with 0.8% more economic growth (Venkatraman, 2024). Businesses operate in a volatile, uncertain, complex, and ambiguous (VUCA) environment, making risk management, cybersecurity, and customer trust crucial for sustainability (von Spreti et al., 2021). The rapid adoption of digital payment systems highlights Nigeria's digital economy, where 64.7% of consumers use mobile wallets, and 80% of banks plan to shift to cloud-based platforms (ACI Worldwide & GlobalData, 2024).

The Rising Threat of Cybercrime in Nigeria

Cybercrime threatens Nigeria's economic and business landscape. Cybercrime costs are projected to exceed $12 trillion globally by 2025 (Akintaro, 2024), and Nigeria ranks 5th in global cybercrime behind Russia (Bruce et al., 2024). 1 in 4 Nigerian consumers (25.2%) were victims of fraud in 2021, with 27% falling prey to confidence scams, and 14.3% experiencing card fraud (Adaramola, 2023). Nigeria, South Africa, Egypt, and Kenya lose $2.4 billion annually to cybercrime (Tredger, 2023). Critical sectors such as finance, telecommunications, energy, and government services are highly targeted (World Economic Forum, 2023).

The widespread reliance on digital platforms increases exposure to data breaches, ransomware, phishing, and identity theft (Acheme et al., 2023; Chinedu et al., 2021). Nigeria loses over $500 million annually to cybercrimes (NCC, 2023). The 2022 cyberattack on a foremost Nigerian financial institution eroded public trust, making consumers more cautious about online financial data sharing. Despite the Nigeria Data Protection Act (NDPA) of 2023, enforcement remains weak, with organisations struggling due to resource constraints and a lack of cybersecurity expertise.

Low cybersecurity awareness among businesses and customers makes them vulnerable to social engineering attacks (World Economic Forum, 2023). Beyond financial losses, cyber incidents cause reputational damage, reducing consumer confidence and business competitiveness.

The Need for a Holistic Cybersecurity and Trust-Building Approach

Existing research focuses on technical cybersecurity solutions, such as firewalls and encryption (Nwankwo et al., 2023; Nwankwo, 2020), but psychological and relational factors of trust remain underexplored. This study aims to develop hybrid strategies for Nigerian businesses to strengthen customer trust amid growing cybersecurity threats, address Nigeria-specific cybersecurity challenges, such as infrastructural deficits, socio-economic barriers, and cultural perceptions of privacy, and propose an interdisciplinary cybersecurity model integrating law, technology, psychology, and business practices.

THEORIES AND DEVELOPMENTS UNDERPINNING THE STUDY

The relationship between cybersecurity and business survival, particularly in the Nigerian context, has gained attention in recent years due to the increasing reliance on digital systems. Several theoretical frameworks can be applied to understand the intricate dynamics of cybersecurity and its role in fostering customer trust, which is vital for business continuity and growth.

Trust Theory

Trust is foundational to any business relationship, particularly in an increasingly digitalised environment where cyber threats are pervasive. According to Mayer et al. (1995), trust is the willingness of a party to be vulnerable to the actions of another based-on expectations of positive outcomes. In the context of cybersecurity, businesses must earn and maintain customer trust by demonstrating effective data protection, secure transactions, and transparency. The trust theory is especially relevant in Nigeria, where cybersecurity concerns are heightened due to growing cybercrime and online fraud incidents. Trust is thus crucial in mitigating customers' security concerns and fostering long-term relationships (Mayer et al., 1995).

Technology Acceptance Model (TAM)

The TAM(Davis,1989) posits that perceived ease of use and perceived usefulness are key factors that influence users' acceptance of new technologies. In cybersecurity, businesses need to ensure that customers perceive the technological solutions they offer as applicable and easy to engage with. When customers trust that a business has strong cybersecurity measures in place, they are more likely to adopt and use its online services. This model has been used to explain user behaviour in various technology and cybersecurity applications, providing insights into how Nigerian businesses can implement secure digital platforms that customers are willing to trust (Davis, 1989).

Social Exchange Theory (SET)

The SET focuses on the reciprocal nature of interactions within relationships, emphasising the role of trust and perceived benefits in determining the quality and longevity of these relationships

Received: July 23, 2024
Peer reviewed: September 7, 2024
Revised: November 10, 2024
Published: January 2025

(Blau, 1964). In the context of cybersecurity, businesses that provide secure environments are seen as offering more value to their customers, thereby fostering trust and loyalty. For Nigerian businesses, SET suggests that when companies invest in cybersecurity, they protect their assets and enhance their reputation, thereby benefiting from a loyal customer base that trusts them with sensitive information (Blau, 1964).

Risk Management Theory

Risk management theory underpins businesses' strategic approach to mitigate potential losses from cyber threats. According to Knight (1921), businesses face inherent risks that must be evaluated and mitigated. In Nigeria, where cyber threats are escalating, businesses need to employ robust risk management strategies to safeguard customer data. Thus, cybersecurity measures are critical to reducing the risk of data breaches and associated reputational damage. By effectively managing these risks, businesses can ensure their survival and build customer trust through their demonstrated commitment to security (Knight, 1921).

Diffusion of Innovations Theory

Everett Rogers' Diffusion of Innovations Theory (1962) explores how new technologies spread within a society. This theory is crucial in understanding how businesses adopt cybersecurity innovations, such as encryption or multi-factor authentication, to enhance customer trust. In Nigeria, where digital transformation is rapidly advancing, businesses must communicate the benefits of their cybersecurity measures to customers in a way that encourages adoption. Companies can build consumer confidence and foster loyalty by effectively diffusing cybersecurity innovations, ensuring continued success in a competitive market.

The Global Digital Landscape

The evolution of computing began in the 1960s, with ARPANET (1969) laying the foundation for the modern internet and the first email transmission (1971). The 1980s saw the rise of personal computing, marked by the launch of the IBM PC (1980) and the development of the Domain Name System (DNS) (1983), simplifying internet navigation. The concept of e-commerce emerged in 1984, and in 1989, Tim Berners-Lee invented the World Wide Web, revolutionising internet accessibility.

The 1990s witnessed mass internet adoption with the dot-com boom, driven by innovations such as the first website (1991) and the launch of Netscape Navigator (1994). The rise of Google (1998) and the launch of Alibaba and Amazon (1999) reshaped digital commerce. However, the dot-com bubble burst in 2000, causing major market disruptions. In 2004, Facebook introduced a new era of social media, followed by the iPhone (2007), which revolutionised mobile computing. The emergence of Bitcoin and blockchain (2008) and the launch of Uber (2009) further transformed digital finance and transportation.

The 2010s saw rapid digital transformation fueled by mobile apps, big data, and the gig economy. The launch of Instagram (2010) emphasised visual content in social media. The rise of Lyft and Airbnb (2011) drove the sharing economy, while cybersecurity concerns led to Nigeria's Cybercrime Act (2015). That same year, the United Nations declared internet access a fundamental human right. In 2018, the European Union enacted the General Data Protection Regulation (GDPR), marking a turning point in data privacy laws, which Nigeria reinforced in 2019 with the Nigeria Data Protection Regulations.

The 2020s have been defined by accelerated digital transformation driven by the COVID-19 pandemic, which increased remote work, e-commerce, and digital payments. The rise of NFTs (2021) introduced digital ownership, while AI, machine learning, and IoT (2022) continued automation across industries. E-commerce growth (2023) underscored the shift toward online business platforms, and Nigeria's Data Protection Act (2023) replaced the 2019 regulations, strengthening data security and privacy (Krysovatyy et al., 2024; Irughe et al., 2022; Daniel et al., 2021; Momoh et al., 2021). This ongoing digital evolution highlights the need for adaptive policies and cybersecurity measures to address emerging privacy, security, and ethical governance challenges in an increasingly digital world.

Elements of Digital Business

Digital business encompasses various components that work together to create an integrated, efficient, and innovative online ecosystem. These elements include Digital services, the Internet of Things (IoT), Artificial Intelligence (AI), and Digital marketing.

Digital Services

Digital services are online platforms and applications that facilitate various business and personal activities. These services enable individuals and organisations to engage in digital transactions, access resources, and perform essential functions more efficiently than traditional methods. Examples include e-commerce platforms that allow the buying and selling of goods and services online, e-healthcare systems that offer telemedicine and remote consultations, e-education platforms that provide online learning and virtual classrooms, and many others. These digital services streamline processes, enhance accessibility, and increase the reach of businesses, contributing to economic growth and societal well-being (Nwankwo et al., 2023).

Internet of Things

IoT is a network of interconnected physical devices communicating and sharing data over the internet. IoT enables the automation of tasks and processes by allowing devices to interact autonomously and transmit real-time information. This includes applications such as smart homes, where devices like thermostats, security cameras, and appliances can be controlled remotely, and industrial IoT systems that monitor and optimise manufacturing processes. By providing seamless data exchange between devices, IoT facilitates more efficient operations, improves decision-making, and enhances user experiences (Nwankwo et al., 2022a; Nwankwo et al., 2021; Nwankwo et al., 2019).

Artificial Intelligence (AI) and Machine Learning (ML)

AI refers to the development of systems that can perform tasks typically requiring human intelligence, such as problem-solving, decision-making, and language understanding. ML, a subset of AI, uses algorithms and data to enable systems to learn from experience, adapt to new information, and improve performance over time without explicit programming. These technologies have revolutionised numerous industries by automating tasks, enhancing efficiency, and providing personalized experiences. For instance, AI-driven recommendation engines power personalised shopping experiences on e-commerce platforms, while ML algorithms are used to optimise supply chains, predict consumer behaviour, and enhance customer service (Ukhurebor et al., 2021).

Digital Marketing

Digital marketing refers to the use of online platforms and tools to promote products, services, and brands to a global audience. It leverages a range of strategies, such as search engine optimisation (SEO), content marketing, social media marketing, email marketing, and online advertising, to engage potential customers, increase visibility, and drive sales. Through digital marketing, businesses can target specific demographics, track customer interactions, and adapt campaigns in real-time for maximum impact. This approach allows businesses to reach a larger, more diverse audience, with the ability to analyze and optimize the effectiveness of marketing efforts, making it a key component of modern business strategies. When integrated into a cohesive digital business strategy, these four elements create a dynamic, responsive, and scalable business model that can adapt to the market's evolving needs, drive innovation, and offer enhanced services to customers.

Digital Landscape across Africa

Africa has made significant strides in digital transformation over the past decade, with various countries developing policies, adopting innovative technologies, and addressing challenges unique to the continent. Many African countries are experiencing increased internet penetration and smartphone adoption. Mobile money and FinTech solutions are gaining popularity, enabling greater financial inclusion and access to banking services. Startups and tech hubs are on the rise in various African cities, fostering innovation and entrepreneurship. Governments also support the tech sector by implementing policies encouraging investment and digital infrastructure development. The leading digital economies in Africa are: Nigeria, with a large population and growing internet penetration; South Africa, with a well-established infrastructure and tech-savvy population; Kenya and Tanzania, known for their innovative solutions; and Egypt, a large population and emerging digital economy.

Received: July 23, 2024
Peer reviewed: September 7, 2024
Revised: November 10, 2024
Published: January 2025

Egypt: Digital Leadership in North Africa

Egypt's digital transformation is driven by its Vision 2030, which focuses on creating a knowledge-based economy (Egypt Vision 2030, n.d.). The government has prioritized ICT infrastructure development, e-government services, and digital inclusion initiatives. For instance, Egypt's ICT sector recorded a 16% growth during the 2020/2021 fiscal year, making it the fastest-growing economic sector (Amr Talaat, 2021). In terms of legislation, Egypt enacted the Personal Data Protection Law (Law No. 151 of 2020) to regulate data handling and attract data-driven investments (Talaat, 2021). Despite these advancements, challenges persist, including digital literacy gaps and the need for advanced cybersecurity measures (Mahmoud, 2022).

South Africa: A Regional Powerhouse

South Africa's National Development Plan 2030 integrates ICT as a central pillar for economic growth (South Africa National Planning Commission, 2012). Projects like South Africa Connect aim to achieve universal broadband coverage (AU, 2020). The country also introduced the Protection of Personal Information Act (POPIA), which aligns with global data protection standards (POPIA, 2013). The ICT sector contributes about 3% to South Africa's GDP, with robust fintech and e-commerce growth (World Bank, 2023). However, South Africa faces challenges like digital inequality and skills shortages, which hinder equitable digital access (Nkuna, 2022).

Nigeria: The Giant of Africa

Nigeria's National Digital Economy Policy and Strategy (2020–2030) aims to diversify the economy through technology, with initiatives like the Digital Nigeria Program promoting digital literacy and access (Federal Ministry of Communications, 2020). The ICT sector contributed 15% to GDP in 2021, fueled by fintech and e-commerce innovations (Financial Times, 2023). Nigeria leads Africa in real-time digital payments, processing 3.7 billion transactions in 2021 and ranking 6th globally, with projections exceeding 8.9 billion transactions by 2027 (ACI Worldwide & GlobalData, 2024). Digital businesses have significantly boosted employment, creating 2.2 million jobs in Nigeria (2020–2022) due to low entry barriers, remote work, and the gig economy (Nigerian Tribune, 2023).

Regulatory frameworks like the Nigeria Data Protection Regulation (NDPR) and the Cybercrimes Act support cybersecurity and data privacy (NDPR, 2019). The National Digital Economy Policy and Strategy (NDEPS) launched in 2019, aims to lift 100 million Nigerians out of poverty in 10 years. Despite these advancements, challenges such as inadequate infrastructure, regulatory gaps, and cybersecurity risks remain barriers to sustained digital growth (Olowokure, 2022). Addressing these issues is crucial for realizing Nigeria's digital economy potential.

Received: July 23, 2024
Peer reviewed: September 7, 2024
Revised: November 10, 2024
Published: January 2025

Ghana: A Rising Star in West Africa

Ghana's Digital Ghana Agenda focuses on enhancing ICT infrastructure and services. Programmes like the National Identification System and Mobile Money Interoperability have boosted financial inclusion (Bawumia, 2022). The country also enacted the Data Protection Act (2012) to safeguard personal information (Data Protection Act, 2012). Ghana's ICT sector has seen growth, with tech startups thriving in fintech and e-commerce. However, challenges such as limited digital literacy and infrastructure deficits in rural areas remain barriers to progress (Owusu-Ansah, 2023; Sackey et al., 2023).

Kenya: The Silicon Savannah

Kenya is a digital innovation hub, with its Digital Economy Blueprint serving as a roadmap for transformation (AU, 2020). The success of mobile money platforms like M-Pesa underscores Kenya's leadership in digital financial services. The ICT sector grew by 10.3% in 2020, contributing significantly to GDP (World Bank, 2023). Legislation like the Data Protection Act (2019) aligns with global standards, ensuring data privacy and security (Data Protection Act, 2019). However, challenges include digital inequality and cybersecurity risks, especially in rural areas (Mwangi, 2022).

Tanzania: Emerging Digital Economy

Tanzania's digital transformation is guided by the National ICT Policy (2016), focusing on infrastructure expansion and e-government services (AU, 2020). Mobile money platforms like Tigo Pesa and M-Pesa have boosted financial inclusion. The Electronic and Postal Communications Act provides a framework for e-commerce and cybersecurity. While the ICT sector is growing, challenges such as low digital literacy and inadequate rural infrastructure persist (Lusekelo, 2022; Kingu & Gomera, 2022).

Cyber Security and Business Survival

The role of cybersecurity in ensuring business continuity is well-documented. Von Solms and Van Niekerk (2013) highlight that effective cybersecurity strategies are essential for protecting organisational assets and maintaining operational integrity. However, many businesses in Nigeria lack the technical infrastructure and expertise to implement these strategies effectively (Adeleke et al., 2021). The economic cost of cyberattacks in Nigeria is significant, with the Nigerian Communications Commission (2023) reporting annual losses exceeding $500 million. Despite these losses, cybersecurity investment remains low among Nigerian businesses, particularly SMEs, which often view cybersecurity as unnecessary (Agboola & Olayemi, 2022).

Customer trust is critical to business sustainability, especially in the digital economy. Studies by Gefen et al. (2003) and Jarvenpaa et al. (2000) emphasise the importance of trust in fostering long-

Received: July 23, 2024
Peer reviewed: September 7, 2024
Revised: November 10, 2024
Published: January 2025

term customer relationships. Cybersecurity breaches erode this trust, as customers perceive vulnerabilities in the organisation's ability to protect their data (Ponemon Institute, 2022). In Nigeria, the trust deficit is exacerbated by frequent data breaches and inadequate response mechanisms (Odunlade & Bamidele, 2021). Mishra et al. (2017) propose that trust can be rebuilt through transparent communication, robust security measures, and compensatory services after incidents, but these strategies are rarely implemented in Nigeria.

Nigeria has made strides in establishing cybersecurity legislation, such as the Cybercrimes Act 2015 and the recent Nigeria Data Protection Act 2023. These laws provide a foundational framework for protecting businesses and customer data. However, weak enforcement remains a significant challenge, as Ekong and Ekong (2020) noted. Regulatory bodies like the Nigeria Data Protection Bureau (NDPB) and the Nigerian Communications Commission (NCC) face resource constraints and jurisdictional overlaps, limiting their effectiveness (World Economic Forum, 2023). Adebayo and Salau (2022) argue that the legislation does not adequately address emerging threats, such as ransomware and social engineering, which require more proactive and adaptive legal frameworks.

Awareness and compliance are critical for effective cybersecurity implementation. Ashford (2017) notes that low awareness among employees and customers creates vulnerabilities that cybercriminals exploit. This gap is particularly pronounced in Nigeria, with many businesses failing to conduct regular cybersecurity training for their staff (Adeleke et al., 2021). Furthermore, Odunlade and Bamidele (2021) found that customers are often unaware of their rights under the law or best practices for protecting their data, leaving them vulnerable to fraud and identity theft. This lack of awareness undermines the effectiveness of existing cybersecurity measures and exacerbates the trust deficit.

Recent studies highlight the need for interdisciplinary approaches integrating technology, psychology, and business practices to address cybersecurity challenges. Von Solms and Van Niekerk (2013) propose that businesses must move beyond technical solutions to adopt holistic frameworks that include trust-building mechanisms. Similarly, several authorities have advocated the role of public-private partnerships in strengthening cybersecurity resilience, particularly in developing economies (World Economic Forum,2023; Nwankwo & Kiffordu,2019; Nwankwo & Ukurebor,2019). However, Agboola and Olayemi (2022) note that Nigerian businesses lag in adopting these trends, primarily due to resource constraints and a lack of strategic planning.

Cyber Security Best Practices and Trust

Effective cybersecurity begins with risk assessments to identify and mitigate vulnerabilities. The NIST Cybersecurity Framework (2023) and ISO/IEC 27001 emphasise proactive risk

Received: July 23, 2024
Peer reviewed: September 7, 2024
Revised: November 10, 2024
Published: January 2025

management, yet many Nigerian businesses adopt reactive approaches, weakening their defence against cyber threats (Humphreys, 2016; Agboola & Olayemi, 2022).

Incident response plans (IRPs) help mitigate cyber breaches, but many Nigerian businesses lack structured IRPs, leading to delayed recovery and loss of customer trust (SANS Institute, 2020; Adeleke et al., 2021). Encryption and access controls, such as end-to-end encryption (E2EE) and multi-factor authentication (MFA), are critical for data security, but resource constraints hinder widespread adoption among SMEs (Center for Internet Security, 2022; Odunlade & Bamidele, 2021).

Transparency in data handling fosters trust, and public disclosure of security policies and breach responses reassure customers (Mishra et al., 2017). Regulatory compliance with NDPA and GDPR promotes accountability, enhancing customer confidence in data protection efforts (Adebayo & Salau, 2022). Cybersecurity education campaigns, including phishing simulations and awareness training, empower customers against social engineering threats, yet Nigerian businesses rarely implement such initiatives (Ashford, 2017).

A proactive, transparent, and customer-engaged cybersecurity approach is essential for building resilience and sustaining trust in Nigeria's digital economy.

METHODOLOGY

This qualitative exploratory study focuses on understanding and interpreting the existing legislative and policy landscape to provide actionable recommendations for improving cybersecurity and customer trust in Nigeria. The approach used is qualitative content analysis. This methodology systematically reviews and interprets existing documents to extract relevant insights and address the research objectives. Below is an outline of the methodology:

Research Strategy

The study adopts a qualitative documentary review approach, analysing secondary sources such as legislation, policies, regulations, standards, and scholarly publications related to cybersecurity and business survival in Nigeria.

Data Collection

The sources of data are:

a) Specific international legislations in the United States, India, China, the European Union, the United Kingdom, and Nigeria related to cyber security and business survival.
b) National cybersecurity strategies, business regulations, and data protection policies in Nigeria.
c) Thirty impactful published papers relevant to the convergence of cybersecurity legislation, policies, and business survival.

The inclusion criteria are documents published within the last 10–15 years for contemporary relevance, materials focused on Nigeria or comparative studies involving similar socio-economic contexts, and papers addressing the relationship between cybersecurity, business continuity, and customer trust.
On the other hand, irrelevant publications that were not focused on cybersecurity and business survival and outdated policies or legislations that were no longer in force in Nigeria were excluded.

Data Analysis

The Content Analysis Framework (CAF) employed in this study entails the following:

a. Thematic analysis: Recurring themes were identified, such as "impact of cybersecurity on trust," "legislative frameworks for cybersecurity," and "business resilience strategies." Further, we categorise insights into themes aligning with the study’s objectives.
b. Comparative analysis: Here, we compare different policies and legislations to assess their effectiveness in promoting business survival and building customer trust. We also contrast Nigerian cybersecurity frameworks with those of other nations to identify gaps or best practices.
c. Framework for analysis. We employed Braun & Clarke's (2006) thematic analysis framework, which entails familiarising the data and generating initial codes, searching for themes, reviewing themes, refining and naming themes and reporting, respectively.

Validity and Reliability

To ensure valid results, we employed two strategies: triangulation, which validates findings by cross-referencing insights from multiple sources, such as aligning legislative analysis with findings from published research papers, and Expert Validation, which uses feedback from legal and cybersecurity experts to ensure accurate interpretation of legislative documents.

FINDINGS AND DISCUSSION

Cyber Insecurity and its Impact on Business

The Information and Communications Technology (ICT) sector has significantly contributed to Nigeria’s GDP, with growth driven by the telecommunications sub-sector. In Q2 2022, ICT contributed 18.44% to Nigeria’s real GDP, rising to 19.78% in 2024, with telecommunications accounting for 16.36% (Michael, 2023; Akintaro, 2024b; NBS, 2024).

Despite this progress, cybercrime poses a major threat to Nigeria’s digital economy. In 2024, the Economic and Financial Crimes Commission (EFCC) reported over $500 million in losses from phishing, identity theft, and online fraud (Odeniyi, 2024). Cybercrime costs are projected to exceed $10.5 trillion by 2025 (Mgboji, 2024). The financial impact extends beyond direct losses, affecting business profitability, customer trust, and operational stability. SMEs, which dominate Nigeria's economy, remain highly vulnerable due to limited cybersecurity resources (Deloitte, 2024).

The EFCC, established in 2004, has intensified cybercrime enforcement, securing over 2,800 convictions in 2022 and launching a Cybercrime Rapid Response Service (Sibe & Kaunert, 2024; EFCC, 2024). However, limited funding, technology constraints, and low cybersecurity awareness hinder effective cybercrime prevention. Addressing these gaps through education, policy reforms, and enhanced cybersecurity infrastructure is essential for sustaining Nigeria's digital economic growth.

National and International Cybercrime Legislation

With the rapid increase in cybercrime and its impact on businesses, nations globally have recognised the need for robust cybercrime legislation. Cybercrime laws aim to protect individuals, businesses, and governments by addressing the specific challenges posed by the digital landscape. However, cybercrime legislation's scope, content, and effectiveness vary widely across different jurisdictions (Goodman & Brenner, 2019). Thus, we explore the nature and scope of national cybercrime laws, discussing key legislation from various countries, their strengths and weaknesses, and their role in influencing business growth and trust in Nigeria.

Emergence of Cybercrime Laws

Cybercrime laws have evolved to address new and emerging cyber threats. The earliest laws were predominantly adaptations of traditional criminal laws, but as cybercrime grew more complex, dedicated cybercrime legislation became necessary (Brenner, 2019). Over time, laws have expanded to cover a range of activities, including unauthorised access, hacking, identity theft, child exploitation, and data breaches (Clough, 2015). Additionally, many countries have integrated cybersecurity requirements, making it mandatory for organisations to implement specific security standards to prevent data breaches.

Influential National Cybercrime Laws and Frameworks

Nigeria is a trade partner of major economies such as the United States, the United Kingdom, China, Europe, and India. The implication is that the cyber security posture of such economies influences Nigeria in several ways.

The United States

The United States has a robust cybercrime legal framework, with key laws addressing various cybersecurity aspects. The Computer Fraud and Abuse Act (CFAA) (1986) criminalises unauthorised system access, data theft, and cyber espionage (Brenner, 2019). The Electronic Communications Privacy Act (ECPA) (1986) regulates electronic communication privacy but is often criticised as outdated (Goodman & Brenner, 2019). The Cybersecurity Information Sharing

Act (CISA) (2015) promotes public-private collaboration by facilitating cyber threat information exchange (Clough, 2015).

The NIST Cybersecurity Framework (CSF), developed by the National Institute of Standards and Technology, provides a structured approach to cybersecurity risk management with five core functions: Identify, Protect, Detect, Respond, and Recover. Organisations widely use it to enhance cyber resilience, with the most recent version being NIST CSF 2.0 (NIST, 2023). The ISO/IEC 27001 standard, maintained by ISO and IEC, sets international guidelines for establishing and maintaining Information Security Management Systems (ISMS). Unlike the freely available NIST CSF, ISO/IEC 27001 requires certification through independent audits, strengthening organisations' security credibility (Humphreys, 2016). The CIS Controls (Version 8), developed by the Center for Internet Security (CIS), provide 18 prioritised security actions tailored to different organisational needs. These cost-effective controls help businesses, especially SMEs, mitigate cyber threats efficiently (Center for Internet Security, 2022). Together, these frameworks and regulations enhance cybersecurity resilience in the U.S. and influence global cybersecurity practices.

European Union

The European Union (EU) has implemented several policies and directives to establish a unified approach to cybercrime and cybersecurity. EU’s General Data Protection Regulation (GDPR) is the EU’s primary data protection law. GDPR indirectly addresses cybercrime by imposing strict requirements on data protection and breach notification (Goddard, 2017). GDPR requires organisations to implement robust cybersecurity measures and mandates fines for non-compliance, thus promoting accountability in data handling. The EU’s Directive on Attacks Against Information Systems was enacted to harmonize cybercrime laws across its member states. It criminalises unauthorised access, system interference, and data interference, setting a standard across EU countries (Gercke, 2018). The Network and Information Security (NIS) Directive was implemented in 2016. The NIS Directive sets minimum cybersecurity requirements for operators of essential services (e.g., energy, banking, transport) and digital service providers. The directive aims to protect critical infrastructure from cyber threats by establishing national frameworks for incident response and reporting (Gercke, 2018).

The United Kingdom

The United Kingdom has implemented several cybercrime laws to address various cyber threats. The Computer Misuse Act (CMA) was enacted in 1990. The CMA criminalises unauthorised access to computer systems, denial-of-service attacks, and unauthorised modifications. The CMA has been amended multiple times to keep up with evolving cyber threats (Wall, 2017). The UK’s Data Protection Act (DPA) is the UK’s implementation of the GDPR. It requires organisations to protect personal data and provides individuals with rights regarding their personal information (Clough, 2015).

The Investigatory Powers Act, known as the "Snooper's Charter," gives the UK law enforcement and intelligence agencies broad surveillance powers, including access to online communications. While it aims to enhance national security, it has been controversial due to privacy concerns (Goddard, 2017). Other notable instruments are: Data Protection Act (DPA), Network and Information Systems Regulations (NIS Regulations), Telecommunications (Security) Act, Product Security and Telecommunications Infrastructure (PSTI) Act, Cyber Security and Resilience Bill, Cyber Essentials Scheme, Investigatory Powers Act.

India

India has developed several laws and frameworks to combat cybercrime. We will present some of these laws. India foremost Information Technology Act (ITA) came into force in 2000. This act is India's primary legislation on cybercrime and e-commerce. It addresses issues like hacking, identity theft, and financial fraud, and provides a legal framework for digital signatures and electronic contracts (Basu, 2019).

Indian Penal Code (IPC) includes sections that address cybercrimes related to fraud, impersonation, and threats. The IPC has been amended to incorporate cybercrime-related provisions (Basu, 2019). India's Data Protection Bill although not yet fully implemented, is expected to set comprehensive data protection and privacy standards, similar to the GDPR (Basu, 2019). Similar legislations include the National Cyber Security Policy 2013, the Personal Data Protection Bill proposed in 2019, the CERT-In Guidelines 2013, and the ISO/IEC 27001 adopted in India in 2013.

China

China has a strict and expansive approach to cybercrime and cybersecurity regulation. China's Cybersecurity Law was enacted in 2017. This law requires organisations to implement cybersecurity measures, mandates data localisation, and grants authorities access to data for national security purposes. It also applies to foreign companies operating in China, making compliance essential for global businesses (Clough, 2015).

China's Data Security Law was implemented in 2021. This law focuses on protecting national data and requires organisations to assess the security risks of their data handling practices. It is part of China's broader efforts to control and protect data within its jurisdiction (Goodman & Brenner, 2019). Table 5 presents the primary regulatory instruments to cyber security in China. Other Chinese cybersecurity regulatory instruments are Cybersecurity Law, Data Security Law, Personal Information Protection Law (PIPL), Multi-Level Protection Scheme (MLPS) 2.0, Cryptography Law, and the ISO/IEC 27001 standard.

Nigeria

Nigeria has witnessed a rise in cybercrime due to increased internet penetration and digital adoption. To combat these threats, the country has implemented cybercrime laws and data protection frameworks to protect individuals, businesses, and national security.

Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015

The Cybercrimes Act of 2015 is Nigeria's primary legislation against cybercrime, criminalising offences such as hacking, cyberstalking, identity theft, and phishing (Okeshola & Adeta, 2013). Key provisions include:

a. Unauthorized Access and Hacking – Criminalizes unauthorised access to computer systems (Cybercrimes Act, 2015, Section 6).
b. Cyberstalking and Cyberbullying – Prohibits online harassment and threats (Adekoya, 2020).
c. Financial Fraud and Identity Theft – Targets phishing and credit card fraud (Cybercrimes Act, 2015, Sections 13–15).
d. Child Exploitation and Pornography – Outlaws child pornography and online exploitation (Odumesi, 2014).
e. Cyberterrorism and National Security – Addresses threats to critical infrastructure (Adekoya, 2020).
f. Data Protection – Mandates financial data security but lacks a comprehensive data protection framework (Cybercrimes Act, 2015, Section 43).
g. Penalties and Sanctions – Includes severe punishments, such as up to five years for cyberstalking (Cybercrimes Act, 2015, Section 24).

While the Act has improved Nigeria's cybercrime response, critics argue that vague definitions and broad law enforcement powers raise privacy concerns (Adekoya, 2020).

Nigeria Data Protection Act (NDPA), 2023

The Nigeria Data Protection Act (NDPA) was enacted in 2023 to strengthen data privacy and align with global standards like the **EU GDPR** (Nigeria Data Protection Act, 2023). Key provisions include:

a. Personal Data Processing – Requires explicit user consent before collecting or processing personal data.
b. Individual Rights – Grants individuals the right to access, rectify, delete, and object to data processing (Nigeria Data Protection Act, 2023).
c. Data Security and Breach Notification – Organizations must report breaches to the Nigeria Data Protection Bureau (NDPB) within 72 hours.
d. Data Protection Officers (DPOs) – Organizations must appoint DPOs to oversee compliance.

e. Cross-Border Data Transfers – Restricts data transfers to countries without adequate data protection laws.
f. Penalties – Non-compliance can result in fines of up to 2% of annual revenue or ₦10 million (Nigeria Data Protection Act, 2023).

The NDPA enhances privacy protection and global compliance, but enforcement challenges and SME compliance remain concerns (Ezejiofor et al., 2020).

Nigeria Data Protection Regulation (NDPR), 2019

Introduced by NITDA, the NDPR set the foundation for Nigeria's data protection laws. It mandates:

a. Data Collection and Consent – Organizations must obtain explicit consent for data collection (Ezejiofor et al., 2020).
b. Data Breach Notification – Requires breach reporting within 72 hours (NDPR, 2019).
c. Data Security Standards – Establishes encryption and access control measures.
d. Penalties for Non-Compliance – Organizations face up to 10 million Naira in fines (NDPR, 2019).

Despite its effectiveness, awareness and enforcement gaps hinder full compliance (Ezejiofor et al., 2020).

Other Cybersecurity Frameworks in Nigeria

a. NITDA Act (2007) establishes cybersecurity guidelines and policies (Odumesi, 2014).
b. The CBN Cybersecurity Framework (2018) requires banks to implement risk assessments, incident response plans, and data protection mechanisms (Ewelukwa, 2017).
c. Nigeria Data Protection Commission (NDPC) – Enforces compliance, imposes penalties, and promotes global data security standards (NDPC, 2023).

Role of National Cybercrime Laws in Combating Cybercrime

National cybercrime laws play a crucial role in addressing cyber threats by providing a legal framework for prosecuting cybercriminals, protecting data, and enforcing cybersecurity standards. While national laws vary, they share common objectives: safeguarding public and private sectors from cyber threats, protecting individuals' personal information, and enabling law enforcement agencies to investigate and prosecute cybercrime effectively (Brenner, 2019). Effective cybercrime legislation also encourages organisations to adopt cybersecurity measures and promotes a culture of accountability and resilience. For instance, GDPR and similar data protection laws in other regions have incentivised companies to prioritise data protection, reducing vulnerabilities and improving overall cybersecurity (Goddard, 2017). National cybercrime laws form the foundation of a country's approach to cybersecurity and cybercrime prevention. While these laws provide critical protections, they must adapt to the rapidly changing cyber threat landscape. As we proceed, it is essential to recognise the strengths and limitations of national laws and explore how international cooperation can complement these frameworks to create a safer, more resilient digital ecosystem.

Challenges in National Cybercrime Legislation

Cybercrime legislation globally confronts a myriad of issues, including jurisdiction, technological advancement, harmonisation, security, and privacy.

Jurisdictional Issues

One of the primary challenges in enforcing cybercrime laws is jurisdiction. Cybercrimes often involve parties from multiple countries, complicating the question of which country's laws apply and how they should be enforced (Holt & Bossler, 2016). For example, coordinating the investigation and prosecution can be challenging if a hacker based in one country targets victims in another. Nigeria is a signatory to international treaties like the African Union Convention on Cyber Security and Personal Data Protection, but more international cooperation is needed to tackle cross-border cybercrime (Ezejiofor et al., 2020).

Rapid Technological Advancement

The rapid evolution of technology often outpaces legislative processes, leaving gaps in cybercrime laws (Wall, 2017). Many cybercrime laws were enacted years ago and have not been updated to reflect new cyber threats, such as ransomware, cryptocurrency fraud, and IoT vulnerabilities. This issue is evident in the United States' ECPA, which has not kept pace with modern communication technologies (Goodman, 2019).

Balancing Security and Privacy

Many cybercrime laws, particularly those granting surveillance powers, raise privacy concerns. Laws like the UK's Investigatory Powers Act and China's Cybersecurity Law provide broad monitoring capabilities, which some critics argue infringe on citizens' rights to privacy (Goddard, 2017). Balancing security needs with privacy rights is an ongoing debate in cybercrime legislation (Nwankwo et al.,2022c; Nwankwo et al.,2022d).

While some regions, such as the European Union, have tried to harmonise cybercrime laws, disparities between national laws remain a significant barrier to effective cross-border cooperation (Gercke, 2018). This lack of harmonisation allows cybercriminals to exploit gaps in different jurisdictions, particularly those with weaker or outdated laws.

Enforcement and Resource Constraints

Due to limited resources and expertise, Nigeria faces significant challenges in enforcing cybercrime laws. Law enforcement agencies often lack the technical skills and tools to investigate and prosecute cybercrime (Adekoya, 2020) effectively.

Public Awareness and Compliance

While frameworks like the NDPR set high standards for data protection, many organisations and individuals lack awareness of these regulations, leading to low compliance rates (Ewelukwa, 2017). Education and awareness programs are essential to improve compliance and foster a culture of cybersecurity.

Building Trust to Aid Business Survival

Trust is an intangible yet vital asset in business, shaping stakeholder relationships and influencing long-term sustainability (Bachmann & Zaheer, 2006). Unlike financial assets, trust lacks standardised valuation but is a strategic resource that fosters a commitment to business success (Barney & Hansen, 1994). However, it is fragile—quickly eroded by data breaches or ethical lapses—and requires proactive risk management for restoration (Mayer et al., 1995).

Risk Management and Compliance for Trust Restoration

Risk management frameworks, such as ISO 31000, emphasise proactive risk identification, mitigation, and monitoring to safeguard stakeholder confidence (ISO, 2018). A comprehensive approach that integrates legal compliance, best practices, and cybersecurity technologies is essential (Lacey, 2010). Adopting ISO 27001 and GDPR compliance demonstrates a commitment to data protection, aligning with global standards (ISO, 2013).

Transparency is crucial in rebuilding trust. Organisations must communicate **honestly** about operations, security incidents, and remediation measures (Palenchar & Heath, 2007). Effective strategies include:

a. Timely breach disclosure to authorities and stakeholders.
b. Regular security updates and visible improvements.
c. Implementing cybersecurity measures like encryption, multi-factor authentication, and third-party audits (Cavusoglu et al., 2004).

Beyond compliance, businesses must align with stakeholder expectations by fostering a culture of accountability and ethical conduct (Dirks & Ferrin, 2001). Training employees on data protection, ethical behaviour, and security protocols reinforces an organisation's commitment to trust.

Regulatory Obligations under the NDPA and Cybercrimes Act

The Nigeria Data Protection Act (NDPA), 2023 mandates organisations to:

a. Obtain consent before using website cookies and clearly disclose their purpose (NDPA, Section 5(6)).
b. Report data breaches to the Nigeria Data Protection Commission (NDPC) within 72 hours (NDPA, Section 40).
c. Provide affected customers with support services, such as credit monitoring, and offer compensation where necessary.

Additionally, Section 21 of the Cybercrimes Act requires businesses to:

a. Report cybersecurity incidents to the Nigeria Computer Emergency Response Team (ngCERT) immediately to enable intervention.
b. Failure to report within seven days attracts a ₦2 million fine and denial of internet services (Cybercrimes Act, Section 21(3)).
c. Banks and financial institutions must report breaches to the Central Bank of Nigeria (CBN), while telecom firms and ISPs must notify the National Communications Commission (NCC).

Aside from the legislation, every business owner should implement a well-defined incident response and risk management plan (Nwankwo & Olayinka,2019) that allows the business to react swiftly and effectively to breaches, minimizing damage and recovery time (see Figure 1).

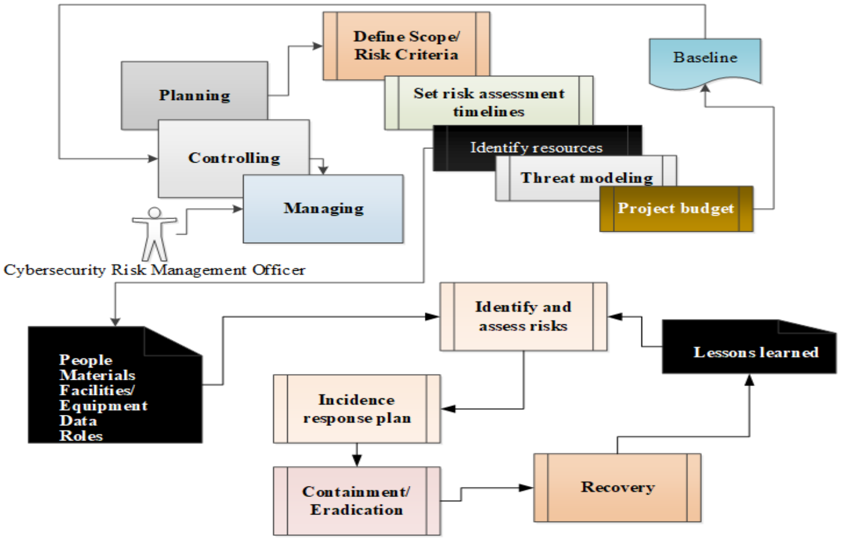

Figure 1: Incidence response-driven risk management cyber security framework for Business owners [Source, Author]

Received: July 23, 2024
Peer reviewed: September 7, 2024
Revised: November 10, 2024
Published: January 2025

Employee training on cyber hygiene reduces the risk of phishing and social engineering attacks. Businesses can differentiate themselves by integrating cybersecurity into their value propositions, fostering customer trust and loyalty, particularly in financial services (Porter & Heppelmann, 2014). Public-private partnerships (PPPs), such as Nigeria's Interpol Cybercrime collaboration, strengthen cyber resilience through coordinated efforts (World Economic Forum, 2023; Nwankwo et al., 2022b).

Key cybersecurity measures for business survival include:

a. Deploying anti-malware software and endpoint protection
b. Outsourcing cybersecurity to specialized firms
c. Establishing online safety guidelines
d. Encrypting stored and transmitted data
e. Implementing multi-factor authentication (MFA) and strong passwords
f. Regular cybersecurity audits and network monitoring
g. Applying timely security patches
h. Adopting a robust risk management strategy

A proactive cybersecurity approach enhances business resilience, trust, and long-term sustainability.

CONCLUSION

This study underscores the pivotal role of cybersecurity in ensuring business survival and fostering customer trust in Nigeria's evolving digital economy. Through a comprehensive review of existing legislations, policies, and scholarly works, it highlights the strengths and limitations of frameworks such as the Nigeria Cybercrimes Act 2015 and the Nigeria Data Protection Act 2023 (NDPA). The findings reveal that while these frameworks provide a foundational structure for combating cyber threats, gaps in enforcement, compliance, and adaptability to emerging threats hinder their effectiveness.

Businesses that proactively adopt robust cybersecurity measures not only safeguard their operations but also enhance customer trust, thereby achieving long-term sustainability. By emphasizing the critical need for legislative enhancements, widespread awareness, and business commitment to cybersecurity, this research offers actionable recommendations for stakeholders.

Policymakers must focus on stricter enforcement mechanisms, regular updates to existing regulations, and fostering collaborations with the private sector. Businesses, on the other hand,

Received: July 23, 2024
Peer reviewed: September 7, 2024
Revised: November 10, 2024
Published: January 2025

must prioritize compliance with cybersecurity frameworks, invest in advanced protective measures, and build customer-centric trust strategies.

Future research should expand on this study by incorporating empirical data through surveys, interviews, and case studies involving key stakeholders such as businesses, policymakers, and consumers. Additionally, longitudinal studies could examine the long-term impacts of cybersecurity breaches and compliance on business sustainability. Exploring the integration of emerging technologies like artificial intelligence, blockchain, and machine learning into Nigeria's cybersecurity framework could provide deeper insights into innovative solutions for enhancing business resilience and trust in the digital age. This future work would bridge the gap between policy and practice, contributing to a more secure and trustworthy digital ecosystem in Nigeria.

REFERENCES

Acheme, S. O., Nwankwo, W., Acheme, D., & Nwankwo, C. P. (2023). A crypto-stego distributed data hiding model for data protection in a single cloud environment. In Z. Hu, Y. Wang, & M. He (Eds.), *Advances in intelligent systems, computer science and digital economics IV. CSDEIS 2022.* Lecture notes on data engineering and communications technologies (Vol. 158). Springer, Cham.

ACI Worldwide & GlobalData(2024). The Global Real-Time Payments Report.

Adaramola,Z.(2023). How Cyber-Attacks Exposed Nigeria's IT Security Vulnerability In 2023. https://dailytrust.com/how-cyber-attacks-exposed-nigerias-it-security-vulnerability-in-2023 /

Adebayo, F., & Salau, A. (2022). Emerging Cybersecurity Threats in Nigeria: A Legal Perspective. *Journal of Law and Technology in Africa*, 7(1), 12-26.

Adekoya, A. A. (2020). Cybercrime legislation in Nigeria: Analysis of the Cybercrimes Act 2015. *Journal of Law and Criminal Justice*, 8(1), 67-85.

Adeleke, A., Agwu, P., & Johnson, T. (2021). Cybersecurity Practices in Nigerian SMEs. *Journal of Cybersecurity Research*, 18(3), 45-58.

Agbeboaye,C.(2024). Investigative Analysis of Cybercrime in Nigeria: Using Theft Triangle. *J. Electrical Systems,* 20(4s0, 1275-1282

Agboola, A., & Olayemi, A. (2022). Cybersecurity Challenges in Nigerian Financial Institutions. *Journal of Digital Security,* 15(4), 45-60.

Akintaro,S.(2024a). Cost of cybercrime to reach over $12 trillion globally by 2025 – Report. https://nairametrics.com/2024/01/25/cost-of-cybercrime-to-reach-over-12-trillion-globally-by-2025-report/

Akintaro,S.(2023). ICT contributed 15.97% to Nigeria's real GDP in Q3 2023. https://nairametrics.com/2023/11/24/ict-contributed-15-97-to-nigerias-real-gdp-in-q3-2023/

ISSN: 2408-7920

Akintaro,S.(2024b). ICT contributed 16.66% to Nigeria's real GDP in Q4 2023. https://nairametrics.com/2024/02/23/ict-contributed-16-66-to-nigerias-real-gdp-in-q4-2023/

Akintaro,S.(2024c). ICT's contribution to Nigeria's real GDP hits 19.78% in Q2 2024 - NBS. https://nairametrics.com/2024/08/26/icts-contribution-to-nigerias-real-gdp-hits-19-78-in-q2-2024-nbs/

Ashford, W. (2017). Employee Awareness in Cybersecurity. *Computer Weekly*, 15(2), 10-12.

AU. (2020). Digital Transformation Strategy for Africa 2020–2030. African Union.

Bachmann, R., & Zaheer, A. (2006). *Handbook of Trust Research.* Edward Elgar Publishing.

Barney, J. B., & Hansen, M. H. (1994). "Trustworthiness as a source of competitive advantage." *Strategic Management Journal*, 15(S1), 175-190.

Basu, S. (2019). Cyber Law in India. New Delhi: LexisNexis.

Bawumia, M. (2022). Mobile Money Interoperability in Ghana. *Nigerian Tribune*.

Blau, P. M. (1964). Exchange and Power in Social Life. Wiley.

Brenner, S. W. (2019). Cybercrime: Criminal threats from cyberspace. Routledge.

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N. & Varese, F. (2024) Mapping the global geography of cybercrime with the World Cybercrime Index. PLoS ONE 19(4): e0297312. https://doi.org/10.1371/journal.pone.0297312

CBN(2018). Guidelines on Cybersecurity for Banks and Other Financial Institutions in Nigeria. Central Bank of Nigeria.

Center for Internet Security (2022). CIS Controls Version 8. https://www.cisecurity.org/controls

Chinedu, P.U., Nwankwo, W., Aliu,D., Shaba,S.M., Momoh,M.O. (2020). Cloud Security Concerns: Assessing the Fears of Service Adoption. *Archive of Science and Technology*, 1(2), 164-174

Chinedu, P. U., Nwankwo,W., Olanrewaju,B. S.,& Olayinka T. C.(2018). Cloud-Based Virtual Organization Framework for Optimizing Corporate Value Chain. *International Journal of Discrete Mathematics*, 3(1), 11-20

Chinedu, P. U., Nwankwo, W., & Eze, U. F. (2013). Enterprise Cloud Adoption: Leveraging on the Business and Security Benefits*, West African Journal of Industrial and Academic Research*, 7(1).

Chinedu, P. U., Nwankwo, W., Masajuwa, F. U. & Imoisi, S. (2021). Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models. *Review of International Geographical Education (RIGEO)*, 11(7), 956-974. Doi: 10.48047/rigeo.11.07.92

Clough, J. (2015). Principles of Cybercrime. Cambridge University Press.

Cybercrimes (Prohibition, Prevention, Etc.) Act. (2015). Federal Government of Nigeria.

Cybercrime Magazine (2024). Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024. https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

Daniel,A., Shaba, S.M., Momoh, M.O., Chinedu, P. U., & Nwankwo, W.(2021). A Computer Security System for Cloud Computing Based on Encryption Technique. *Computer Engineering and Applications*, 10(1),41-53.

Data Protection Act (2012). Republic of Ghana.

Data Protection Act (2019). Republic of Kenya.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340.

Deloitte. (2024). *Nigeria Cybersecurity Outlook 2024*. https://www.deloitte.com/content/dam/assetszone1/ng/en/docs/services/riskadvisory/2023/Nigeria%20Cybersecurity%20Outlook%202024.pdf

Drapkin, A. (2023). Data Breaches That Have Happened in 2022 and 2023 So Far. https://tech.co/news/data-breaches-updated-list

EFCC. (2024). *EFCC Unveils Cybercrime Rapid Response Service*. https://www.efcc.gov.ng/efcc/news-and-information/news-release/10471-efcc-unveils cybercrime-rapid-response-service

Egypt Vision 2030. (2020). Egyptian Government. https://mped.gov.eg/Files/Egypt_Vision_2030_EnglishDigitalUse.pdf

Ekong, U., & Ekong, E. (2020). Evaluating the Effectiveness of Cybersecurity Policies in Nigeria. *African Security Review*, 29(1), 34-49.

Ewelukwa, C. O. (2017). Cybersecurity and the Nigerian financial sector: Challenges and regulatory perspectives. International Journal of Banking and Finance, 10(2), 89-105.

Ezejiofor, R. A., Enebeli, O. F., & Nwokoye, E. O. (2020). Nigeria Data Protection Regulation: Implications and challenges. *International Journal of Data Protection and Cybersecurity*, 6(1), 45-56.

Federal Ministry of Communications. (2020). National Digital Economy Policy and Strategy. Government of Nigeria.

Financial Times (2023). Digital Economy in Africa: A Focus on Nigeria. *Financial Times*.

Fox, J. (2023). Top Cybersecurity Statistics for 2024. Cobalt. https://www.cobalt.io/blog/cybersecurity-statistics-2024

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51-90.

Gercke, M. (2018). Understanding cybercrime: Phenomena, challenges, and legal response. Council of Europe.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703-705.

Goodman, M., & Brenner, S. W. (2019). Cybercrime and cyberterrorism: A study of legal policies and judicial decisions. Criminal Law Bulletin.

Holt, T. J., & Bossler, A. M. (2016). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.

Humphreys, E. (2016). Information Security Management Standards: Compliance, Governance, and Risk Management. *Computers & Security*, 56, 55-67.

Idris,A(2023). Data: Digital payment is having its best year in Nigeria. https://techcabal.com/2023/08/04/data-digital-payment-is-having-its-best-year-in-nigeria/

Iroanusi, Q.(2022). *Over 2,800 persons convicted of cybercrime in 2022 – EFCC*. https://www.premiumtimesng.com/news/top-news/562065-over-2800-persons-convicted-of-cybercrime-in-2022-efcc.html?tztc=1

Irughe, D. U., Nwankwo, W., Nwankwo, C. P., & Uwadia, F. (2022). Resilience and security on enterprise networks: A multi-sector study. *2022 5th Information Technology for Education and Development (ITED*), 1–7. https://doi.org/10.1109/ITED56637.2022.10051458.

ISO. (2013). *ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements.* International Organization for Standardization.

ISO. (2018). *ISO 31000: Risk management – Principles and guidelines.* International Organization for Standardization.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (2000). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication*, 5(2). https://doi.org/10.1111/j.1083-6101.2000.tb00337.x

Kifordu, A., Nwankwo,W., & Ukpere, W.(2019). The Role of Public Private Partnership on the Implementation of National Cybersecurity Policies: A Case of Nigeria. *Journal of Advanced Research in Dynamical and Control Systems,* 11(8), 1386-1392. Special issue.

Kingu, A., & Gomera, W. C. (2022). An Assessment of The Impact of Digitalization of Microcredit Services on Micro and Small Enterprises. African Journal of Applied Research, 8(1), 121-137.

Knight, F. H. (1921). *Risk, Uncertainty, and Profit*. Houghton Mifflin.

Krysovatyy, A., Desyatnyuk, O., & Ptashchenko, O. (2024). Digital innovations and their ramifications for financial and state security. African Journal of Applied Research, 10(1), 431-441.

Lacey, D. (2010). Managing the human factor in information security: How to win over staff and influence business managers. Wiley.

Lusekelo, A. (2022). Digital Growth in Tanzania: Opportunities and Challenges. *Tanzanian Economic Review*.

Mahmoud, A. (2022). Egypt's ICT Sector: Growth and Challenges. *Middle East Journal of Economics*.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709-734.

Mgboji,K. (2024). *Cost Of Cybercrime Projected To Exceed $10.5trn In 2024*. Retrieved from https://newtelegraphng.com/cost-of-cybercrime-projected-to-exceed-10-5trn-in-2024/

Michael,C.(2023). Nigeria's ICT sector grows by 8.6%, highest in 3 years.

https://businessday.ng/technology/article/nigerias-ict-sector-grows-by-8-6-highest-in-3yrs/

Mishra, A., Dash, S. B., & Cyr, D. (2017). Customer compensation and trust recovery effectiveness post-data breach. *Journal of Business Research*, 86, 219-232.

Momoh, M. O., Chinedu, P., Nwankwo, W., Aliu, D., & Shaba, M. (2021). Blockchain Adoption: Applications and Challenges. International *Journal of Software Engineering and Computer Systems*, 7(2), 19–25. https://doi.org/10.15282/ijsecs.7.2.2021.3.0086

NBS(2024). Nigeria's GDP by sector: First Quarter Report 2024, National Bureau of Statistics. https://nigerianstat.gov.ng/elibrary/read/1241506

NDPR. (2019). Nigeria Data Protection Regulation. National Information Technology Development Agency.

Nigerian Communications Commission (2023). *Annual Report on Cybersecurity Threats in Nigeria*. Abuja, Nigeria.

Nigeria Data Protection Bureau (2023). *Guidelines for Compliance with the Nigeria Data Protection Act*. Federal Ministry of Communications and Digital Economy.

NIST (2023). NIST Cybersecurity Framework: Version 2.0. U.S. Department of Commerce.

Nkuna, M. (2022). South Africa's Digital Divide: A Persistent Challenge. *South African Journal of ICT*.

Nwankwo, C., Adigwe, W., Nwankwo, W., Kizito, A. E., Konyeha, S., & Uwadia, F. (2022c). An improved password-authentication model for access control in connected systems. *2022 5th Information Technology for Education and Development (ITED)*, 1–8. https://doi.org/10.1109/ITED56637.2022.10051179

Nwankwo, C., Uwadia, F., Nwankwo, W., Adigwe, W., Chinedu, P., & Ojei, E. (2022d). Privacy and security of content: A study of user-resilience and pre-checks on social media. *2022 5th Information Technology for Education and Development (ITED)*, 1–8. https://doi.org/10.1109/ITED56637.2022.10051589

Nwankwo, W. (2020). A review of critical security challenges in SQL-based and NoSQL systems from 2010 to 2019. *International Journal of Advanced Trends in Computer Science and Engineering, 9*(2), 2029–2035.

Nwankwo, W., & Kifordu, A. (2019). Strengthening private sector participation in public infrastructure projects through concession policies and legislations in Nigeria: A review. *Journal of Advanced Research in Dynamical and Control Systems, 11*(08), 1360–1370.

Nwankwo, W., & Ukhurebor, K. E. (2019). Investigating the performance of point-to-multipoint microwave connectivity across undulating landscapes during rainfall. *Journal of the Nigerian Society of Physical Sciences, 1*(3), 103–115. https://doi.org/10.46481/jnsps.2019.16

Nwankwo, W., Adetunji, C. O., Olayinka, A. S., Ukhurebor, K. E., Ukaoha, K. C., Umezurike, C., Chinedu, P. U., & Benson, B. U. (2021). The adoption of AI and IoT technologies: Socio-psychological implications in the production environment. *The IUP Journal of Knowledge Management, 19*(1), 50–75.

Nwankwo, W., Olayinka, A. S., & Ukhurebor, K. E. (2019). The urban traffic congestion problem in Benin City and the search for an ICT-improved solution. *International Journal of Science and Technology, 8*(12), 65–72.

Nwankwo, W., Adetunji, C. O., & Olayinka, A. S. (2022a). IoT-driven Bayesian learning: A case study of reducing road accidents of commercial vehicles on highways. In S. Pal, D. De, & R. Buyya (Eds.), *Artificial intelligence-based Internet of Things systems.* Internet of Things (Technology, Communications and Computing). Springer, Cham. https://doi.org/10.1007/978-3-030-87059-1_15

Nwankwo, W., & Ukaoha, K. C. (2019). Socio-technical perspectives on cybersecurity: Nigeria's cybercrime legislation in review. *International Journal of Scientific and Technology Research, 8*(9), 47–58.

Nwankwo, W., Chinedu, P. U., Masajuwa, F. U., Njoku, C. C., & Imoisi, S. E. (2023). Adoption of i-voting infrastructure: Addressing network-level cybersecurity breaches. *E-Government: An International Journal, 19*(3), 273–303. https://doi.org/10.1504/EG.2023.130582

Nwankwo, W., & Olayinka, A. S. (2019). Implementing a risk management and X-ray cargo scanning document management prototype. *International Journal of Scientific and Technology Research, 8*(9), 93–105.

Nwankwo, W., & Chinedu, P. U. (2018). Security of cloud virtualized resources on a SaaS encryption solution. *Science Journal of Energy Engineering, 6*(1), 8–17. https://doi.org/10.11648/j.sjee.20180601.12

Nwankwo, W., Chinedu, P. U., Daniel, A., Shaba, S. M., Momoh, O. M., Nwankwo, C. P., Adigwe, W., Oghorodo, D., & Uwadia, F. (2023). Educational FinTech: Promoting stakeholder confidence through automatic incidence resolution. In Z. Hu, Y. Wang, & M. He (Eds.), *Advances in intelligent systems, computer science and digital economics IV. CSDEIS 2022.* Lecture Notes on Data Engineering and Communications Technologies (Vol. 158). Springer, Cham. https://doi.org/10.1007/978-3-031-24475-9_78

Nwankwo, W., Kizito, A. E., Adigwe, W., Nwankwo, C. P., Uwadia, F., & Mande, S. (2022b). A community cloud-based store for forensic operations in cybercrime control. *2022 5th Information Technology for Education and Development (ITED)*, 1–8. https://doi.org/10.1109/ITED56637.2022.10051615

Odeniyi,S.(2022). *Nigeria loses over $500m to cybercrime annually – EFCC chair*. Retrieved from https://punchng.com/nigeria-loses-over-500m-to-cybercrime-annually-efcc-chair/

Odumesi, J. (2014). Combating cybercrime in Nigeria: Challenges and opportunities. African *Journal of Criminology and Justice Studies*, 8(1), 91-110.

Odunlade, B., & Bamidele, T. (2021). Customer Trust and Business Continuity: Insights from Nigerian SMEs. *African Journal of Business Management*, 19(2), 98-115.

Okeshola, F. B., & Adeta, A. Y. (2013). The nature, causes, and consequences of cyber crime in tertiary institutions in Zaria-Kaduna state, Nigeria. *American International Journal of Contemporary Research,* 3(9), 98-114.

Palenchar, M. J., & Heath, R. L. (2007). Strategic risk communication: Adding value to society. *Public Relations Review*, 33(2), 120-129.

Ponemon Institute (2022). *Cost of a Data Breach Report*. IBM Security.

POPIA. (2013). Protection of Personal Information Act. Republic of South Africa.

Porter, M. E., & Heppelmann, J. E. (2014). How Smart, Connected Products Are Transforming Competition. *Harvard Business Review*.

Rogers, E. M. (1962). *Diffusion of Innovations*. Free Press.

Purplesec (2022). Cyber Security Statistics: The Ultimate List of Stats Data, & Trends for 2022. https://purplesec.us/resources/cyber-security-statistics/

SANS Institute (2020). Incident Response: Best Practices for Effective Preparation and Execution.

Sackey, E. A., Yandoh, J. B., & Sangban, K. (2023). Interactive Digital Notice Boards for Universities in Ghana. African Journal of Applied Research, 9(1), 153-173.

Sibe, R.T., Kaunert, C. (2024). Cyber Crime in Nigeria—Reviewing the Problems. In: Cybercrime, Digital Forensic Readiness, and Financial Crime Investigation in Nigeria. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-54089-9_2

South Africa National Planning Commission. (2012). National Development Plan 2030. Government of South Africa.

Talaat, A. (2021). ICT Development in Egypt. *Egyptian Ministry of Communications*.

Tredger,C.(2023). Africa's cyber threats triple the global average – Check Point. https://www.itweb.co.za/article/africas-cyber-threats-triple-the-global-average-check-point/KPNG878Nr6Pq4mwD

Ukhurebor, K. E., Nwankwo, W., Adetunji, C. O., & Makinde, A. S. (2021). Artificial intelligence and Internet of Things in instrumentation and control in waste biodegradation plants: Recent developments. In C. O. Adetunji, D. G. Panpatte, & Y. K. Jhala (Eds.), *Microbial rejuvenation of polluted environment.* Microorganisms for sustainability (Vol. 27). Springer, Singapore. https://doi.org/10.1007/978-981-15-7459-7_12

Venkatraman,N.V.(2024). Trust: Business Currency of the Digital Age. https://www.industries.veeva.com/blog/trust_business_currency

Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security,* 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

von Spreti,M., Biberacher,F. & Heinlein,T.(2021). The trust enabler: Building cyber-security strategies for a trusted, digital future. https://www2.deloitte.com/xe/en/insights/topics/digital-transformation/digital-trust-for-future.html

Wall, D. S. (2017). Cybercrime: The transformation of crime in the information age. Polity Press.

Received: July 23, 2024
Peer reviewed: September 7, 2024
Revised: November 10, 2024
Published: January 2025

World Bank(2023). Digital Transformation in Africa. *World Bank Report*.

World Economic Forum (2023). Global Cybersecurity Outlook 2023. Geneva, Switzerland. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf