Knowledge and Compliance of Cyber Regulation among Selected Online Businesses in Akwa Ibom State

Aniebo C. Samson[a], Emmanuel T. Nessi[b]*, Eno-Obong Blaise Akpan[c]
[a]Faculty of Communication and Media Studies, University of Uyo, Uyo, Akwa Ibom State, Nigeria
*Corresponding author: emmypedia@gmail.com

Abstract
The rise of digital technologies has transformed the business landscape, with the Internet becoming a critical platform for e-commerce and digital marketing. Despite regulatory efforts, awareness and compliance with cyber regulations remain limited. This study investigated online business operators' awareness and compliance with cyber regulations, as well as the challenges they encounter. Guided by the Protection Motivation Theory, the study surveyed 384 online business operators within Akwa Ibom's digital space, employing a simple random sampling technique and using a questionnaire as the data collection instrument. Findings reveal that 49.1% of online businesses are aware of cyber regulations but face difficulties in complying due to complex policies, rapid technological changes, and other factors. To address these challenges, the study recommends that policymakers and cybersecurity stakeholders provide regular training and educational programmes for online business owners and employees on cybersecurity regulations and data privacy policies to enhance understanding and improve compliance.

Keywords: Awareness, Knowledge, Compliance, Cyber Regulation, Online Businesses, Nigeria

Introduction

Effective communication is the backbone of modern society, facilitating the exchange of ideas, information, and values. In today's globalised world, the importance of communication cannot be overstated. As a multifaceted concept, communication has been defined and redefined by scholars across various disciplines. Charles (2021) defines communication as the transfer or exchange of messages, emotions, thoughts, and knowledge through symbols. Ochonogor and Ikpegbu (2017) emphasise communication as the process of exchanging information through shared meaning, highlighting the significance of context and interpretation. The advent of new media technologies has revolutionised communication, enabling rapid information dissemination and global connectivity (Castells, as cited in Hartley, 2006). This shift has profound implications for businesses, which now rely heavily on digital communication tools. Ogaraku and Archibong (2017) observe that technology has blended business and human communication, making information exchange a vital component of contemporary business operations.

The internet, social media, and other digital platforms have transformed how businesses operate, interact with customers, and disseminate information within and outside organisational structures. However, this increasing reliance on digital communication also raises concerns about business operators' awareness of cyber regulations and their level of compliance. The complexities of cyberspace make regulating behaviour particularly challenging (McQuail, 2010). As Oni (2020) notes, social media and other digital platforms have introduced new challenges in terms of information dissemination, regulatory enforcement, and compliance.

The potential for unchecked information creation and propagation in the digital sphere has significant implications for businesses, policymakers, and individuals alike.

In Akwa Ibom State, the digitally-driven business environment presents both opportunities and challenges. As businesses become increasingly dependent on digital communication, the need for effective cyber regulation and compliance becomes more critical. This study, therefore, seeks to examine the current state of cyber regulations and provide insights for policymakers, online business operators, and individuals navigating the complexities of digital communication.

Statement of the Problem

The rapid growth of digital technologies in Nigeria has significantly transformed the business landscape, particularly in Akwa Ibom State. The state was recently recognised as the Most Digitally Compliant State in Nigeria by the National Information Technology Development Agency (NITDA), owing to its notable progress in the IT sector (Onuegbu, (2023,). These improvements include enhanced internet connectivity, full automation of civil services, a modern state website for citizen engagement, and the adoption of official government emails. This recognition underscores the growing importance of digital compliance in the region. Nevertheless, the effectiveness of existing cyber regulations in governing online business operations remains uncertain. Although Nigeria has implemented several cyber regulations, such as the Nigeria Data Protection Regulation (NDPR) and the Cybercrime Act, which aim to ensure stability, prevent disorder, and promote the public good in digital spaces, the extent to which these frameworks are known and adhered to by online businesses in Akwa Ibom State is unclear.

Despite the presence of these regulatory instruments, there is limited empirical evidence on the awareness, understanding, and compliance levels among online business operators in the state. To bridge this knowledge gap, this study investigates the influence of cyber regulations on online business operations in Akwa Ibom State. Specifically, it seeks to assess the level of awareness, knowledge, and compliance with cyber regulations among these businesses.

Objectives of the Study

The objectives of this study are to:

1. Ascertain the level of knowledge and compliance of online businesses with cyber regulations in Akwa Ibom State.
2. Investigate the extent to which compliance with cyber regulations influences online business operations in Akwa Ibom State.
3. Identify the challenges faced by online businesses in complying with cyber regulations in Akwa Ibom State.

Research Questions

The following research questions guide the study:

1. What is the level of knowledge of, and compliance with, cyber regulations among online businesses in Akwa Ibom State?
2. How does compliance with cyber regulations influence online business operations in Akwa Ibom State?
3. What challenges do online businesses face in complying with cyber regulations in Akwa Ibom State?

Literature Review

Review of Concepts

Online Business

Online business, also referred to as e-business or digital business, involves the use of the internet and digital technologies to facilitate business transactions, deliver services, and sell products (Kumar, 2018). This model has transformed traditional business operations by

enabling entrepreneurs to access a global market with relatively low startup costs (Turban et al., 2018). A major advantage of online business, as noted by Chaffey, Hemphill, and Edmundson-Bird (2019), is its ability to transcend geographical limitations, allowing businesses to operate around the clock and serve customers worldwide. Online business models come in various forms (Ithinklogistics, 2019, cited in Mputle, 2020), including Business-to-Business (B2B), Business-to-Consumer (B2C), Consumer-to-Business (C2B), Consumer-to-Consumer (C2C), Business-to-Government (B2G), Government-to-Consumer (G2C), Government-to-Government (G2G), Business-to-Employee (B2E), and Business-to-Business-to-Customer (B2B2C). Each model reflects different types of interactions between individuals, businesses, and government bodies in the digital space.

To thrive in the online business environment, entrepreneurs must build a strong foundation in digital marketing strategies such as search engine optimization (SEO), social media marketing, and content marketing (Chaffey et al., 2019). Additionally, investing in reliable e-commerce platforms, secure payment systems, and efficient logistics infrastructure is critical to delivering seamless customer experiences (Laudon & Traver, 2019). The rise of the digital economy has significantly reshaped business landscapes, introducing new forms of communication, data-driven growth, service-oriented products, automation through artificial intelligence (AI), and innovative models like platform-based businesses (OECD, 2019). As such, online business is not only a modern business trend but also a vital component of the global economy, offering entrepreneurs such as those in Akwa Ibom State expanded opportunities for growth and competitiveness in both local and international markets.

Cyber Regulations

Cybersecurity regulations are laws and legal standards that govern how organisations protect their digital assets, data, and networks from cyber threats and data breaches. These regulations stipulate the types of controls organisations must implement, how customer data must be protected, who is accountable and responsible for ensuring security, and how organisations should manage risk within third-party vendor networks. They often vary by industry, region, and the sensitivity of the data involved. For organisations, complying with cybersecurity regulations is crucial not only for safeguarding sensitive information but also for avoiding penalties, legal consequences, and reputational damage (Bitsit, 2023; CSA, 2020). Given the importance of regulation in society, the OECD (2019) notes that governments and regulators play a major role in promoting digital innovation and incentivising the development of new technologies for the benefit of the public. By establishing general rules that reflect societal values and preferences, regulators can foster broad consumer interests and limit potential unintended negative consequences of technological advancement. However, regulatory frameworks often lack the agility required to keep pace with rapid technological development. Moreover, digital technologies challenge traditional regulatory approaches by blurring market definitions, complicating enforcement mechanisms, and transcending domestic and international administrative boundaries.

Altamuro (2022), cited in Folorunso et al. (2024), asserts that organisations must now operate in an increasingly regulated environment where compliance with cybersecurity regulations and standards is essential. Failure to comply can adversely affect a company's brand, financial standing, legal position, and operational integrity. One of the most immediate and tangible consequences of non-compliance is the imposition of legal and financial penalties. Regulatory bodies impose fines and sanctions on organisations that fail to adhere to cybersecurity laws and standards (Morrow & Fitzpatrick, 2020). These penalties can vary considerably depending on the nature of the violation and the specific regulatory framework involved (Folorunso et al., 2024).

Cyber Regulations in Nigeria

Regulation plays a critical role in guiding the development of online businesses in Nigeria, especially with the growing adoption of digital platforms across the country. For example, in Akwa Ibom State, the increasing number of digital entrepreneurs has underscored the need for effective regulatory oversight. Hartley (2006) defines regulation as the set of rules, boundaries, and codes that govern conduct and communication. In the realm of online business, regulation is essential to maintain market order, protect consumer rights, and foster investor confidence. Several government policies have been implemented to regulate this space, including the National Information Technology Development Agency (NITDA) Act**,** which mandates the registration and licensing of online businesses, and the Nigeria Communication Act (NCA)**,** which governs communication services. Other relevant frameworks include the National Policy on Telecommunications (NPT) and the National Cybercrime Act**,** which addresses various forms of cybercrime.

In recent years, the Nigerian government has made efforts to strengthen its digital regulatory landscape. A significant development is the proposed NITDA Bill 2021**,** which seeks to broaden NITDA's regulatory authority and formalise licensing structures within the technology sector. This bill proposes new licensing categories, including Product License, Service Provider License, and Platform Provider License, and introduces a levy system to support the National Information Technology Development Fund (NITDF). According to Koleolu and Anoh (2021), this bill has the potential to fairly and uniformly regulate Nigeria's technology and startup ecosystem. However, they caution that effective implementation will require collaboration between NITDA and other relevant agencies to harmonise levies, streamline licensing, and avoid regulatory overlap. Compliance with these policies is crucial, as it boosts customer trust, mitigates risks such as cybercrime and data breaches, and enhances the competitiveness of Nigerian online businesses.

The National Cybercrime Act of 2015 is one of the most significant legal frameworks addressing cybersecurity in Nigeria. As internet usage expands, cybercrime has become more sophisticated, with threats such as hacking, phishing, malware, cyberstalking, identity theft, and cyber defamation increasingly affecting individuals and businesses (Hasan, 2013; Vitus, 2023). Enacted on May 15, 2015, the Act provides a comprehensive institutional, legal, and regulatory framework for detecting, preventing, and prosecuting cybercrime in Nigeria (Uba, 2021; Imue, 2021, cited in Okocha and Echoi, 2022). It aims to enhance cybersecurity, protect electronic data and communications, and safeguard intellectual property and individual privacy rights. The Federal Ministry of Justice and the Economic and Financial Crimes Commission (EFCC) serve as the principal enforcement bodies, while other key players include private organisations, government agencies, and the National Security Adviser**,** who oversees national cybersecurity efforts. Additionally, the Cybercrime Advisory Council (CAC)**,** established in 2016, coordinates the implementation of the Act and advises on cybercrime prevention policy. Complementary legislation, such as the Data Protection Bill 2020**,** has also been proposed to provide a robust legal framework for personal data protection and uphold citizens' constitutional rights (Okocha and Echoi, 2022).

Cyber Regulation and Online Business

The rapid advancement of digital media technology has significantly reshaped online business operations globally. As Alegu and Maku (2023) explain, digital technologies have permeated nearly every aspect of human interaction, transforming how businesses engage with customers and market their offerings. By 2010, as much as 75% of business transactions in developed countries were conducted online, with projections indicating a global shift in that direction (Ogedengbe & Adesemoye, 2010, cited in Ramson & Akanmu, 2023). In Nigeria, this trend is evident in how digital platforms allow consumers to browse, purchase, and receive goods and services from the convenience of their homes (Ogaraku & Archibong, 2017). The

growing reliance on digital infrastructure has not only enhanced business efficiency but has also increased the demand for a secure and regulated cyber environment.

Social media, in particular, has emerged as a vital tool for online marketing and customer engagement. Siricharoen (2012, cited in Alegu & Maku, 2023) underscores its flexibility and effectiveness in promoting goods and services regardless of time or location. However, this digital integration also raises significant ethical and regulatory concerns. According to Day (2006), digital technology may become a powerful yet dangerous tool in the hands of unethical users. Adesemoye, Idowu, and Ramson (2023) add that the accessibility and manipulability of digital information expose businesses to the risks of misinformation, loss of control over content, and reputational damage. These challenges underline the need for stronger governance over digital content and operations.

Despite the increasing digitalisation of business, Nigeria's regulatory response has lagged behind the pace of technological innovation. As noted by Adesemoye, Idowu, and Ramson (2023), Nigeria currently lacks sufficient legal safeguards to address the risks and infringements that commonly occur in digital environments. While some countries have established robust privacy and cyber laws, the Nigerian framework still exhibits critical gaps, leaving both businesses and consumers vulnerable. The situation calls for the development of effective cyber regulations that not only secure online transactions but also promote trust and accountability in the digital economy. As technology continues to evolve, aligning Nigeria's legal and regulatory systems with global standards is essential to ensure the safe and sustainable growth of online business.

Empirical Review

Recent empirical studies have increasingly illuminated the multifaceted dynamics and persistent challenges associated with cybersecurity regulation and compliance among online businesses and small and medium-sized enterprises (SMEs) in Nigeria. This body of literature underscores the pivotal role of policymakers, regulatory institutions, and cybersecurity stakeholders in establishing and enforcing robust regulatory frameworks, driving awareness initiatives, and fostering the adoption of best practices to enhance the resilience and integrity of Nigeria's growing e-commerce sector. In particular, scholars have drawn attention to the intersection of cybersecurity awareness, regulatory gaps, and the operational vulnerabilities of SMEs navigating the digital economy.

Oladele and Olumide (2020), in their study on cybersecurity awareness, observed a significant deficit in the understanding and knowledge of cybersecurity regulations among Nigerian online business owners. Their findings suggest that the absence of targeted training programmes and awareness campaigns poses a critical barrier to regulatory compliance. Similarly, Ogunleye and Afolabi (2020) contended that in addition to lacking regulatory awareness, many SME operators in Nigeria are constrained by limited financial resources and inadequate technical expertise, further exacerbating non-compliance. These findings align with Ogene's (2024) continental survey, which revealed that approximately 90% of African businesses, including those in Nigeria, lack fundamental cybersecurity awareness, rendering them highly susceptible to data breaches and financial losses. Comparable trends were reported by Rawindaran, Jayal, and Prakash (2022), who found that only 30% of SMEs in Wales demonstrated familiarity with basic cybersecurity terminology, highlighting a global disparity in cybersecurity literacy.

Moreover, Folorunso et al. (2024) explored the critical linkage between cybersecurity compliance and organisational preparedness, asserting that the implementation of structured compliance frameworks significantly enhances a business's capacity to detect, respond to, and recover from cyber threats. Ogene (2024) further posited that Nigeria's cybersecurity landscape suffers from the absence of comprehensive, adaptive regulatory policies, limited public-sector engagement, and a lack of national infrastructure to support proactive cybersecurity initiatives.

The literature consistently identifies systemic obstacles to compliance, such as weak IT governance, inadequate enforcement mechanisms, underinvestment in capacity development, and a shortage of skilled cybersecurity professionals. These deficiencies leave many sectors particularly those outside the financial industry exposed to phishing attacks, ransomware, data theft, and network intrusions. Consequently, recent research advocates for a national cybersecurity fund, enhanced inter-agency collaboration, and investment in technology-driven security solutions to address the regulatory and operational vulnerabilities of online enterprises.

Taken together, these insights form a compelling basis for examining the specific case of online businesses in Akwa Ibom State. By situating local enterprises within the broader discourse on cybersecurity compliance and awareness, researchers can evaluate how the presence or absence of regulatory knowledge, infrastructure, and enforcement influences business performance in Nigeria's digital economy. Understanding these dynamics will be vital in designing tailored policy interventions and educational strategies aimed at strengthening cybersecurity resilience at the subnational level.

Theoretical Framework

This study is grounded in the Protection Motivation Theory (PMT), propounded by Rogers in 1975 (Ekwenchi & Shadrach, 2023c). The theory was further refine by Maddux, J. E. and Rogers, R. W. in 1983. Basically the theory explains how individuals respond to threats and make decisions to protect themselves (Maddux & Rogers, 1983). According to Shillair (2020), the theory proposes that an individual's motivation to protect themselves depends on two factors: (i) threat appraisal (e.g., the severity and likelihood of the threat) and (ii) coping appraisal (e.g., efficacy of the response and perceived ability to enact the response). The PMT provides a useful framework for understanding the factors influencing online businesses' compliance with cyber regulations. The theory highlights the importance of threat appraisal and coping appraisal in shaping online businesses' motivation to comply with regulatory policies. Specifically, online businesses' perception of the severity and likelihood of cyber threats, as well as their confidence in coping with these threats, play a crucial role in determining their compliance behaviour.

For instance, online businesses perceiving cyber threats as severe and likely are more likely to be motivated to comply with regulations. Conversely, online businesses confident in their ability to cope with cyber threats may be more motivated to comply. The PMT also emphasizes that online businesses' motivation to comply with cyber regulations is influenced by their evaluation of compliance costs and benefits. Online businesses perceiving benefits (e.g., improved security and reputation) as outweighing costs (e.g., financial investment and time) are more likely to comply.

Hence, the study will be of valuable insights into enhancing compliance rates among online businesses in the state.

Methodology

This study employed a survey research design, targeting online businesses in Akwa Ibom State's digital space. The population consisted of 500 online businesses, from which a sample size of 384 was determined using Krejcie & Morgan's formula to ensure a 95% confidence level and 5% margin of error as captured below:

$n = (Z2 * p * q)/E2$

Where:

n represents the required sample size

Z is the Z-score based on the desired confidence level (e.g., 1.96 for a 95% confidence level)

p is the estimated proportion of the target population with a particular characteristic or attribute

q is 1 - p (the complement of p)

E is the desired margin of error, expressed as a decimal (e.g., 0.05 for a 5% margin of error)

Then, $n = (Z2 * p * q) / E2$

= (1.962 * 0.5 * 0.5)/0.052
≈ 384.

A simple random sampling technique was used to select participants from online groups and social media platforms. The questionnaire was designed and validated as the instrument for data collection, which was tested for reliability using Cronbach's Alpha (α = 0.904), indicating high internal consistency. It was closed-ended in structure with question items in 5 point Likert scale (Strongly Agree (SA) = 5, Agree (A) = 4, Fairly Agree (FA) = 3, Disagree (D) =2, Strongly Disagree (SD) = 1). The data analysis were performed using the Statistical Package for Social Sciences (SPSS) version 25.0, with descriptive statistics and numerical descriptions used to present the findings in tables.

Result

Out of the 384 copies of the questionnaire distributed, 375 were found valid for analysis. The tables were presented below.

Table 1: Level of knowledge and compliance of online businesses

Items	SA	A	N	D	SD	Total
Cyber-security awareness programme is an important part in reducing the risks that could potentially lead to cyber threats.	177 (47.2%)	143 (38.1%)	22 (5.9%)	20 (5.3%)	13 (3.5%)	375 (100%)
When online business owners are familiar with cyber security regulations and understand their roles in keeping their business secure, there is far less likelihood that a cyber-attack will take place.	143 (38.1%)	184 (49.1%)	20 (5.3%)	23 (6.2%)	5 (1.3%)	375 (100%)
Operators are becoming increasingly aware and concerned about cyber security risks.	184 (49.1%)	140 (37.3%)	24 (6.4%)	22 (5.9%)	5 (1.3%)	375 (100%)
If businesses handle personal, sensitive, or classified information, regulatory compliance violations are not an option.	180 (48.0%)	148 (39.5%)	34 (9.1%)	8 (3.1%)	5 (1.3%)	375 (100%)
As online operators become more knowledgeable, businesses need to respond by implementing tools and solutions that improve their cyber resilience to increase customer trust.	148 (39.5%)	180 (48.0%)	5 (1.3%)	34 (9.1%)	8 (3.1%)	375 (100%)

Source: Field survey (2023)

The data in Table 1 above show that 177 (47.2%) of the respondents strongly agreed that Cyber-security awareness program is an important part in reducing the risks that could potentially lead to cyber threat, 143 (38.1%) agreed, 22 (5.9%) were neutral, 20(5.3%) disagreed and 13 (3.5%) also strongly disagreed. Also, 143 (38.1%) of them strongly agreed that when operators are familiar with cyber security regulations and understand their roles in keeping their business secure, there is far or less likelihood that cyber-attack will take place, 184 (49.1%) agreed, 20 (5.3%) were neutral, 23 (6.2%) disagreed while 5 (1.3%) strongly disagreed.

In the same vein, 184 (49.1%) strongly agreed that online operators are becoming increasingly aware and concerned about cyber security risks, 140 (37.3%) agreed, 24 (6.4%) were neutral, 22(5.9%) disagreed while 5 (1.3%) strongly disagreed. In addition, 180 (48.0%) of the respondents strongly agreed that If online business operators handle personal, sensitive or classified information, regulatory compliance violations is not an option, 148 (39.5%) agreed, 34 (9.1%) were neutral, 8 (3.1%) disagreed while 5 (01.3%) of them strongly disagreed. In the same vein, 148 (39.5%) of them strongly agreed that as operators become more knowledgeable, they need to respond by implementing tools and solutions that improve their cyber resilience to increase customer, 180(48.0%) agreed, 5 (1.3%) were neutral, 34 (9.1%) disagreed while 8 (3.1%) of them strongly disagreed.

Table 2: Online operators' response on compliance with cyber regulations

Items	SA	A	N	D	SD	Total
Information security and privacy programme plays an essential role in safeguarding an entity's data policy and procedures.	143 (38.1%)	177 (47.2%)	13 (3.5%)	22 (5.9%)	20 (5.3%)	375 (100%)
An effective information security and privacy programme ensures an improved level of data classification.	184 (49.1%)	143 (38.1%)	5 (1.3%)	20 (5.3%)	23 (6.2%)	375 (100%)
I believe that an information security and privacy programme will ensure that third-party vendors who process sensitive data have proper cyber-security measures in place.	140 (37.3%)	184 (49.1%)	5 (1.3%)	24 (6.4%)	22 (5.9%)	375 (100%)

Source: Field Survey (2023)

The data presented in Table 2 above show that 143(38.1%) of the respondents strongly agreed that information security and privacy program plays an essential role in the safeguarding of an entity's data policy and procedures, 177 (47.2%) agreed, 13 (3.5%) were neutral, 22 (5.9%) disagreed while 20 (5.3%) of them strongly disagreed. Also, 184 (49.1%) of them strongly agreed that effective information security and privacy program ensures an improved level of data classification, 143 (38.1%) agreed, 5 (1.3%) were neutral, 20 (5.3%) disagreed while 23 (6.2%) of them strongly disagreed. Also, 140 (37.3%) of the respondents strongly agreed that information security and privacy program will ensure that third-party vendors that process sensitive data have proper cyber-security measures in place, 184 (49.1%) agreed, 5 (1.3%) were neutral, 24 (6.4%) disagreed while 22 (5.9%) of them strongly disagreed.

RQ 3: What are the challenges online businesses are faced with in compliance to cyber regulation in Akwa Ibom State?

Table 3: Responses on the challenges faced by online businesses

Items	SA	A	N	D	SD	Total
Complex regulatory requirements are commonly attributed to cyber-security challenges.	175 (46.7%)	145 (38.9%)	20 (5.3%)	13 (3.5%)	22 (5.9%)	375 (100%)
Rapidly evolving technologies contribute to inefficiencies.	140 (37.3%)	184 (49.1%)	5 (1.3%)	24 (6.4%)	22 (5.9%)	375 (100%)
Resource limitations are often compromised due to the challenges of cyber-security regulations.	143 (38.1%)	177 (47.2%)	22 (5.9%)	5 (1.3%)	24 (6.4%)	375 (100%)

Source: Field Survey (2023)

The computation in Table 3 above reveal that 175 (46.7%) of the respondents strongly agreed that complex regulatory requirements are commonly attributed to cyber-security challenges, 145 (38.9%) agreed, 20 (5.3%) were neutral, 13 (3.5%) disagreed while 22 (5.9%) strongly disagreed. Also, 140 (37.3%) of the respondents strongly agreed that rapidly evolving technologies contributes to inefficiencies, 184 (49.1%) agreed, 5 (1.3%) were neutral, 24 (6.4%) disagreed while 22 (5.9%) strongly disagreed. In addition, 143 (38.1%) of the respondents strongly agreed that resource limitations is often compromised due to the challenges of cybersecurity regulations, 177 (47.2%) agreed, 22 (5.9%) were neutral, 5 (1.3%) disagreed while 24 (6.4%) strongly disagreed.

Discussion

The data analysis reveals a significant increase in awareness among online businesses in the state regarding cybersecurity regulations in Nigeria. Although several studies have reported that most online businesses and their owners lack awareness of cybersecurity regulations and programmes, which hinders their level of compliance (Oladele & Olumide, 2020; Rawindaran et al., 2022; Ogunleye & Afolabi, 2020; Ogene, 2024), online businesses in Akwa Ibom State demonstrate awareness of cyber regulations and data privacy policies.

However, this awareness does not necessarily translate into compliance. The results align with the Protection Motivation Theory (PMT), which posits that an individual's motivation to protect themselves from threats is influenced by their perceived vulnerability, severity, and self-efficacy. In this context, online businesses may not feel vulnerable to cyber threats or may lack the self-efficacy to comply with regulations.

The results further show that respondents believe effective information security and privacy programmes are necessary for data classification and protection and influence compliance. These programmes can help online businesses navigate the complexities of cyber regulations and mitigate the risks associated with non-compliance. This finding is consistent with the study by Folorunso et al. (2024), which observed that compliance is not a one-time effort; it demands regular assessments, updates, and training to ensure that organisations remain aligned with evolving regulatory requirements. Moreover, the results explain that certain challenges hinder online business owners from complying with regulations, such as complex regulatory requirements, limited resources, and rapidly evolving technologies. This underscores the need for adaptive and effective regulatory frameworks, as non-compliance can lead to severe consequences, including legal penalties, financial losses, reputational damage, and operational disruptions (Folorunso et al., 2024). Furthermore, the results highlight the importance of security and privacy protocols in safeguarding daily tasks and ensuring compliance (Ogene, 2024). Although the impact of security compliance extends beyond regulatory adherence, implementing compliance frameworks enhances an organisation's ability to mitigate threats, respond to incidents, and recover from security breaches more effectively (Folorunso et al., 2024).

Conclusion

The study's findings emphasise the importance of cyber regulation in shaping online business operations in Akwa Ibom State. While online businesses in the state are aware of cyber regulations, compliance remains a challenge. A critical factor in addressing this challenge is understanding the psychological factors that influence compliance, particularly the need for individuals to acknowledge their vulnerability to cyber threats, assess the severity of these threats, and develop confidence in their ability to protect themselves within the parameters of a clear, defined compliance framework enforced by regulatory bodies that makes it easier for online business operators to comply with regulations in the state.

Recommendations

Based on the study's findings, the following recommendations are hereby proffered:

1. Policymakers and cybersecurity stakeholders should provide regular training and education programmes for online business owners and employees on cybersecurity regulations and data privacy policies to ensure they understand the importance of compliance.
2. Regulatory bodies should encourage online businesses to implement effective information security programmes that include data classification, access controls, and incident response plans.
3. Regulatory bodies should simplify regulatory requirements and provide clear guidelines and templates for online businesses to follow, making it easier for them to comply with regulations.

References

Acheme, R., & Akanmu, O. (2023). Netvertising. In Esuh, P., Rishante, J. S., & M'Bayo, R. (Eds.), *Marketing, Advertising and Public Relations in the Digital Age* (pp. 74-97). Galda Verlag.

Adesemoye, S. A., Idowu, O., & Ramson, A. (2023). Landmines in digital public relations. In Esuh, P., Rishante, J. S., & M'Bayo, R. (Eds.), *Marketing, Advertising and Public Relations in the Digital Age* (pp. 251-266). Galda Verlag.

Akpan-Obong, P. I. (2009). *Information and communication technology in Nigeria: Prospects and challenges for development*. Peter Lang.

Alegu, J. C., & Maku, B. S. (2023). Perspectives on digital media, propaganda and political public relations. In Esuh, P., Rishante, J. S., & M'Bayo, R. (Eds.), *Marketing, Advertising and Public Relations in the Digital Age* (pp. 222-250). Galda Verlag.

Chaffey, D., Hemphill, T., & Edmundson-Bird, D. (2019). *Digital business and e-commerce management*. Pearson Education.

Charles, U. F. (2021). *Organisational communication audit and management efficiency at Akwa Ibom State University* [Unpublished PhD thesis]. University of Uyo.

Day, L. A. (2006). *Ethics in media communication: Cases and controversies* (5th ed.). Wadsworth Cengage Learning.

Ekwenchi, O. C., & Shadrach, I. (2023c). Qualitative analysis of awareness, knowledge, and attitude to online data privacy risks and protection strategies among millennials in selected federal universities in North-East Nigeria. *Nasarawa Journal of Communication and Media Studies, 7*(1).

Folorunso, A., Wada, I., Samuel, B., & Mohammed, V. (2024). Security compliance and its implication for cybersecurity. *World Journal of Advanced Research & Reviews, 24*(1), 2105-2121.

Hartley, J. (2006). *Communication, cultural and media studies: The key concepts* (3rd ed.). Routledge-Taylor & Francis Group.

Hasan, S. (2013). *Mass communication: Principles and concepts*. CBS Publishers and Distributors.

Hirst, M. (2019). *Navigating social journalism*. Routledge.

Koleolu, S. T., & Anoh, E. (2021). The regulation of technology companies in Nigeria: The proposed NITDA Act 2021. https://www.pavestoneslegal.com

Kumar, N. (2018). *E-business: A managerial perspective*. Cengage Learning.

Laudon, K. C., & Traver, C. G. (2019). *E-commerce: Business, technology, society*. Pearson Education.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469–479.

McQuail, D. (2010). *McQuail's mass communication theory* (6th ed.). Sage Publications.

Morrow, P. J., & Fitzpatrick, T. M. (2020). US and international legal perspectives affecting cybersecurity corporate governance. *International Relations, 8*(6), 231-239.

Mputie, I. K. (2020). *Analysing the impacts of e-commerce in South African retail sector: The case of Johannesburg small-medium enterprises* [Unpublished master's dissertation]. University of Johannesburg.

Ochonogor, C. I., & Ikpegbu, E. O. U. (2017). Redirecting Nigerian youths to agriculture through communication for national development. *The Nigerian Journal of Communication, 14*(1), 163–169.

OECD. (2019). *Regulatory effectiveness in the era of digitalisation*. https://www.oecd.org/gov/regulatory-policy/Regulatory-effectiveness-in-the-era-of digitalisation.pdf

Ogaraku, H., & Archibong, B. (2017). Web 2.0, connectedness and conversation in users into commodities and digital audience labour. *The Nigerian Journal of Communication, 1*(14), 37–77.

Ogene, F. (2024). Cybersecurity and IT governance challenges in Nigeria: Strategic investment needs and the path forward for a resilient digital economy. *International Journal of Computer Applications, 186*(55), 41–46.

Ogunleye, O. S., & Afolabi, A. O. (2020). Cybersecurity compliance among online businesses in Nigeria: An exploratory study. *International Journal of E-Business Research, 16*(2), 1–20.

Okocha, D. O., & Echoi, M. P. (2022). Netizens detection and mitigation of crimes in the digital environment in Nigeria: A qualitative analysis. *Lead City Journal of the Social Sciences (LCJSS), 7*, 22–40.

Oladele, A. O., & Olumide, O. O. (2020). Assessing cybersecurity awareness among online business owners in Nigeria. *Journal of Information Security and Cybercrimes Research, 2*(1), 1–15.

Oni, B. O. (2020). Media literacy: Navigating the perilous labyrinth of a media saturated society. In Oloyede, I. B., & Oni, B. O. (Eds.), *Essential Readings in Communication and Media Studies* (pp. 47–59). Stirling-Horden Publishers Ltd.

Onuegbu, C. (2023, October). NITDA honours A-Ibom, Oyo as most digital compliant states in Nigeria: NITDA opens entries for 2021 Innovation Challenge. *Vanguard*. https://www.vanguardngr.com/2023/10/nitda-honours-a-ibom-oyo-as-most-digital compliant-states-in-nigeria/

Rawindaran, N., Jayal, A., & Prakash, E. (2022). Exploration of the impact of cybersecurity awareness on small and medium enterprises (SMEs) in Wales. *Computers, 11*(12), 174.

Shillair, R. (2020). Protection motivation theory. https://researchgate.net/DOI:10.1002/978111901107.iemp0188

Turban, E., McLean, E., & Wetherbe, J. (2018). *Information technology for management: Transforming organizations in the digital economy*. Wiley.

Vitus, E. N. (2023). Cybercrime and online safety: Addressing the challenges and solutions related to cybercrime, online fraud, ensuring a safe digital environment for all users –A case of African states. https://www.researchgate.net/publication/373994007