

COMPLIANCE AS A CATALYST: PROPOSING THE REGULATORY-DRIVEN CYBERSECURITY ALIGNMENT (RDCA) THEORY FOR INSTITUTIONAL CYBERSECURITY GROWTH IN EMERGING ECONOMIES

Asere Gbenga Femi^{1*}, Adenomom Monday Osagie¹, Mangbon Innocent Label²
¹Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria
²Department of General Studies, Federal School of Statistics, Manchok, Nigeria

Corresponding Author: aseregbenga@gmail.com

Received 02 December 2025 Received in revised form 08 December 2025 Accepted 10 December 2025
 Received 13 December 2025

ABSTRACT

In many emerging economies, regulatory compliance is often perceived as a bureaucratic necessity. This paper challenges that notion by proposing the Regulatory-Driven Cybersecurity Alignment (RDCA) Theory, which posits that compliance can be a powerful catalyst for institutional cybersecurity growth. Focusing on Nigeria’s data privacy landscape especially the Nigeria Data Protection Regulation (NDPR) the RDCA Theory illustrates how regulatory obligations serve as a trigger for cybersecurity capacity building, particularly when organizations align legal mandates with strategic IT operations. Grounded in Institutional Theory and Protection Motivation Theory, the model captures the dynamic interplay between external regulatory pressure and internal organizational response. Empirical insights from Nigerian sectors such as banking, healthcare, and education reveal that when compliance is framed as a strategic priority, it leads to stronger investment in cybersecurity infrastructure, training, and governance. However, disparities in compliance among SMEs versus large corporations highlight the need for scalable, inclusive approaches. The study concludes that in under-resourced environments, Regulation-Driven Alignment can provide a pathway to resilient cybersecurity if adequately supported by policy and leadership.

Keywords: Regulatory Compliance, Cybersecurity Maturity, Data Privacy Regulation, Institutional Alignment, Emerging Economies

1. INTRODUCTION

In today’s increasingly digital and data-driven world, cybersecurity has emerged as a fundamental pillar of organizational resilience, particularly in emerging economies. These nations face rising cyber threats due to rapid technological adoption, low awareness levels, and limited resources to secure digital infrastructures [1]. Despite these challenges, regulatory frameworks have begun to play a transformative role in encouraging organizations to prioritize cybersecurity practices. Data privacy regulations, such as the Nigeria Data Protection Regulation (NDPR), are designed to enforce protective standards for personal information. However, beyond their legal function, these regulations are beginning to serve as catalysts for broader cybersecurity transformations within institutions. Regulatory compliance, traditionally viewed as a procedural obligation, is now being reinterpreted as a strategic driver of cybersecurity alignment. This shift is particularly relevant in contexts where organizations lack mature risk management systems. While existing theories such as Regulatory Compliance Theory emphasize the role of laws in ensuring organizational conformity [2], they often fail to explain the

transformation process through which compliance efforts lead to long-term improvements in cybersecurity maturity. Likewise, traditional Risk Management Frameworks (e.g., NIST, ISO 27001) are designed for contexts with well-developed governance and technical capabilities features often absent in many organizations across Africa, Asia, and Latin America [3].

This paper introduces the Regulatory-Driven Cybersecurity Alignment (RDCA) Theory as a novel framework that bridges the gap between regulatory compliance and cybersecurity development. Drawing from Institutional Theory [4], the RDCA Theory posits that external pressures such as data privacy regulations drive internal organizational change, leading to improved cybersecurity practices. It integrates concepts from the Technology-Organization-Environment (TOE) framework [5] and Protection Motivation Theory [6], offering a multidimensional explanation of how regulation motivates not only legal adherence but also technological investment, policy reform, and employee training. The RDCA Theory is particularly applicable to emerging economies, where formal institutional structures coexist with informal practices, resource constraints, and uneven enforcement.

Empirical evidence from countries like Nigeria supports the conceptual relevance of RDCA. Since the implementation of the NDPR in 2019, there has been a marked increase in cybersecurity investments and awareness, especially among large organizations [7]. However, compliance remains low among small and medium-sized enterprises (SMEs), indicating that regulatory frameworks alone are insufficient without supportive mechanisms such as training, funding, and enforcement. This underscores the need for a theory like RDCA, which not only explains how regulatory pressure affects cybersecurity but also accounts for contextual factors such as organizational size, sectoral maturity, and institutional support systems.

By proposing the RDCA Theory, this paper seeks to expand scholarly understanding of the complex interplay between compliance and cybersecurity. It challenges the binary view of regulation as either effective or ineffective by exploring the processes through which compliance can be a catalyst for institutional cybersecurity growth. In doing so, it provides a more nuanced, adaptable, and scalable framework for policymakers, cybersecurity professionals, and researchers working to enhance digital resilience in emerging economies.

2. SUMMARY OF REVIEWED LITERATURE

The discourse on cybersecurity compliance has evolved from a focus on legal enforcement to a strategic perspective on how compliance shapes organizational behavior and digital resilience. In emerging economies, where digital infrastructure is still developing, and regulatory compliance plays an increasingly important role in guiding institutions toward adopting cybersecurity best practices. Scholars such as [8] argue that compliance initiatives serve as external stimuli, compelling organizations to institute internal controls that reduce cybersecurity risks. Similarly, [9] highlight that regulations like data protection laws can foster institutional awareness and structure in organizations that may otherwise overlook cybersecurity. In Nigeria, the introduction of the Nigeria Data Protection Regulation (NDPR) has been a key policy tool to stimulate such change [7]. Existing theoretical frameworks, however, often fall short in explaining how compliance transitions into long-term cybersecurity maturity, particularly in resource-constrained settings. The Regulatory Compliance Theory, for instance, tends to emphasize the binary outcome of whether or not an organization conforms to rules [2]. While this perspective is valuable in assessing surface-level adherence, it lacks depth in explaining how such

adherence contributes to strategic transformation or capability building. Similarly, the Risk Management Framework (e.g., NIST RMF) assumes the presence of a mature IT ecosystem, which is frequently absent in the informal economies and fragile institutions common in many parts of Africa, Asia, and Latin America [3, 10].

Several scholars have attempted to bridge this gap by integrating institutional and organizational perspectives. The Institutional Theory [4] argues that organizations adopt certain behaviors due to normative, coercive, and mimetic pressures, suggesting that compliance may be driven more by the pursuit of legitimacy than genuine commitment. The Technology-Organization-Environment (TOE) framework offers a more structured approach to understanding innovation adoption, where environmental factors like regulations play a crucial role in influencing internal change [5]. However, the TOE framework has not been widely applied in cybersecurity-specific contexts in developing nations, making its practical contribution somewhat limited. Protection Motivation Theory [6] provides another important perspective, focusing on how perceived threats and the efficacy of protective actions influence decision-making. This theory has been increasingly applied to explain cybersecurity behavior at both the individual and organizational level [11]. Nevertheless, it primarily addresses psychological motivation and lacks a systemic approach to understanding how regulations interact with institutional development, especially in sectors with low technical maturity. Studies like those by [12] and [13] emphasize the need for integrative frameworks that combine behavioral, technological, and regulatory factors to enhance cybersecurity effectiveness.

Given these theoretical gaps, there is a clear need for a more context-sensitive framework that explains how regulatory compliance can act as a catalyst for institutional cybersecurity growth. The proposed Regulatory-Driven Cybersecurity Alignment (RDCA) Theory seeks to fulfill this need by linking data privacy compliance efforts with operational changes, sectoral adaptability, and the progressive development of cybersecurity capabilities. It builds on but extends beyond existing frameworks by explicitly addressing the realities of enforcement limitations, informal economies, and sectoral disparities found in emerging markets. This positions RDCA as a more comprehensive and applicable model for understanding and improving cybersecurity outcomes through compliance in the global South.

3. MATERIALS AND METHODS

Research Design: This study adopts a mixed-methods research design, combining quantitative surveys with qualitative interviews to explore how regulatory compliance influences cybersecurity maturity in emerging economies, particularly Nigeria. This design allows for both broad generalizations from numerical data and in-depth understanding of organizational dynamics [14]. The mixed approach is appropriate given the need to validate and refine the newly proposed Regulatory-Driven Cybersecurity Alignment (RDCA) Theory.

Population and Sampling: The target population comprises IT professionals, data protection officers, cybersecurity heads, and risk managers in public and private sector organizations across finance, healthcare, education, and telecommunications in Nigeria. A purposive sampling technique is employed to ensure that participants have relevant expertise and responsibilities aligned with data privacy and cybersecurity. For the quantitative component, a sample size of approximately 615 participants is targeted. For qualitative interviews, 10–15 key informants are selected for in-depth insights.

Data Collection Instruments: Quantitative data is collected through a structured questionnaire, which includes Likert-scale items on perceived regulatory pressure, cybersecurity practices, compliance levels, and threat experiences. The instrument is adapted from prior validated tools e.g., [15, 16] and aligned with the RDCA Theory constructs. Qualitative data is gathered via semi-structured interviews, enabling participants to elaborate on challenges, motivations, and institutional dynamics related to data privacy and cybersecurity alignment.

Procedure for Data Collection: Surveys are distributed electronically using Google Forms and other online platforms. Interview appointments are scheduled via email and conducted through Zoom or in-person depending on availability and location. Participants are informed of the purpose of the research and assured of confidentiality through informed consent forms. Ethical

clearance is obtained from the relevant institutional review board.

Data Analysis Techniques: Quantitative data was analyzed using SPSS. Descriptive statistics, correlation analysis, and regression models are used to assess the relationship between regulatory compliance and cybersecurity practices. In particular, the analysis seeks to test the core propositions of the RDCA Theory that regulatory pressure leads to operational alignment, which enhances cybersecurity maturity. Qualitative data from interviews are transcribed and analyzed thematically using NVivo, focusing on patterns of institutional adaptation, regulatory influence, and sectoral variations.

Validity and Reliability: To ensure validity, instruments are pilot-tested with a small subset of professionals before full deployment. Feedback is used to improve clarity and relevance. For reliability, internal consistency of the survey instrument is tested using Cronbach’s alpha, targeting a coefficient of 0.70 or higher.

Ethical Considerations: The study adheres to standard ethical guidelines in research involving human subjects. Participation is voluntary, and all data are anonymized. The study avoids any harm, deception, or conflict of interest and complies with data protection standards consistent with NDPR.

4. RESULT AND DISCUSSION

Data were collected from 561 respondents through structured questionnaires and 54 key informant interviews. Respondents were drawn from finance, health, education, and telecommunications sectors in Nigeria. The goal was to assess the relationship between regulatory compliance and cybersecurity outcomes based on the constructs of the Regulatory-Driven Cybersecurity Alignment (RDCA) Theory.

4.1 Descriptive Statistics

i. Demographics of Respondents

Table 1: Distribution of Respondents by Role and Organizational Size

Category	Subcategory	Percentage (%)
Professional Role	IT Professionals	40
	Cybersecurity Officers	25
	Data Protection Officers	20
	Risk Managers	15
Organizational Size	Large Organizations	50
	Small and Medium Enterprises (SMEs)	50

Source: Authors field Survey Results, 2025, computed using SPSS

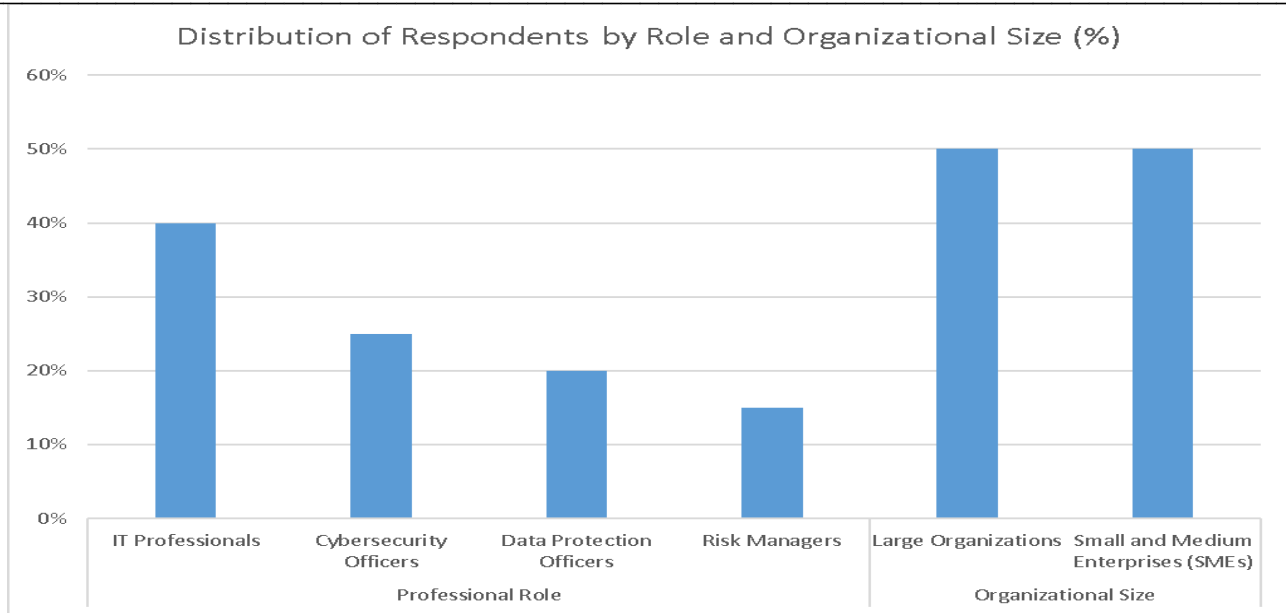


Figure 1: Distribution of Respondents by Role and Organizational Size (%)

The study drew participation from a diverse group of professionals involved in organizational cybersecurity and data governance in Nigeria. Specifically, 40% of the respondents were IT professionals, 25% were cybersecurity officers, 20% were data protection officers, and the remaining 15% were risk managers. This distribution reflects a balanced representation across roles directly responsible for data security and regulatory compliance. In terms of organizational size, 50% of the participants worked in large organizations, while 50% came from small and medium-sized enterprises (SMEs). This demographic distribution provides a meaningful basis for comparing how organizational capacity and structure influence both awareness and implementation of data privacy regulations.

ii. Awareness of Data Privacy Regulations

The survey revealed a generally high level of awareness of data privacy regulations among respondents. A significant 89% reported familiarity with the Nigeria Data Protection Regulation (NDPR), 77% were aware of the Cybercrime Act, and 54% knew about the more recent E-Privacy Law. Notably, awareness was substantially higher in sectors such as finance and telecommunications, which are typically more regulated and exposed to stricter compliance mandates. This variation suggests that sectoral regulatory pressure may drive heightened institutional engagement with privacy laws and related cybersecurity practices.

4.2 Compliance and Cybersecurity Practice

i. Regulatory Compliance Levels: The data showed a marked disparity in compliance levels between large organizations and SMEs. Approximately 90% of large organizations reported full or near-full compliance with the NDPR, whereas only 35% of SMEs reached similar levels. This gap highlights the influence of organizational resources, technical capacity, and institutional readiness on regulatory adherence. Larger firms often possess dedicated compliance units and better funding, enabling them to implement comprehensive data privacy and cybersecurity programs, unlike many resource-constrained SMEs.

ii. Cybersecurity Investment Trends: In line with the compliance trends, cybersecurity investment patterns also differed significantly based on organizational size. About 85% of large organizations indicated that their cybersecurity investments had increased following the implementation of the NDPR. In contrast, only 30% of SMEs reported a similar increase. This trend underscores how regulatory requirements can stimulate strategic security spending, especially among organizations with the financial capability to scale their operations. However, it also points to a potential vulnerability among SMEs, which may lack the means to upgrade their systems in response to evolving regulatory standards.

4.3 Theoretical Development: Regulatory-Driven Cybersecurity Alignment (RDCA) Theory

This study introduces an original conceptual framework known as the Regulatory-Driven Cybersecurity Alignment (RDCA) Theory. The development of this theory was inspired by recurring patterns observed in Nigerian organizations, where regulatory instruments such as the Nigeria Data Protection Regulation (NDPR) do more than simply enforce legal compliance. Instead, they actively influence how organizations structure, prioritize, and implement cybersecurity measures. The RDCA Theory posits that data privacy regulations act as powerful institutional forces that trigger internal behavioral and operational shifts, leading to alignment with broader cybersecurity best practices. In this theoretical model, data privacy laws are viewed not merely as legal requirements but as external pressures that drive meaningful organizational responses. For instance, the NDPR mandates responsibilities like lawful data processing, incident reporting, data minimization, and third-party data management each of which requires deliberate action from organizations. The resulting pressure from these mandates acts as a stimulus for internal change, compelling leaders to reassess and strengthen their data protection strategies. According to RDCA, this regulatory pressure fosters compliance awareness within organizations, which then sparks operational changes that go beyond compliance extending into broader improvements in information security frameworks.

The RDCA Theory's core contribution lies in its assertion that compliance-driven actions often catalyze wider cybersecurity transformations. While the immediate goal may be to meet regulatory requirements, the resulting measures such as the deployment of access control systems, the formation of incident response teams, and regular staff cybersecurity training contribute to the overall enhancement of an organization's security posture. Thus, RDCA outlines a clear and structured progression: regulatory pressure awareness operational adjustments improved cybersecurity maturity. This sequential model captures the dynamic nature of how external regulatory drivers influence internal organizational resilience. Additionally, the RDCA Theory recognizes that the degree and nature of this transformation are not uniform across all organizations. The model incorporates cultural and sectoral variables such as organizational size, industry standards, regulatory experience, and internal values which shape how effectively compliance is translated into tangible cybersecurity outcomes. For example, financial institutions that are regularly monitored may respond more aggressively than under-resourced public institutions or small businesses. By factoring in these moderating elements, RDCA offers a flexible and context-sensitive approach that accommodates the varied realities within Nigeria's organizational landscape.

Ultimately, the RDCA Theory re-conceptualizes data privacy regulation as a strategic enabler of cybersecurity growth, rather than a regulatory burden. It bridges the often-separated domains of legal compliance and cybersecurity development by demonstrating that regulatory alignment can act as a pathway to improved security behavior, infrastructure, and organizational awareness. This perspective is especially relevant in Nigeria, where cybersecurity frameworks are still maturing and regulatory compliance is becoming a central driver of institutional change. As such, RDCA provides both a theoretical and practical lens for understanding how data protection laws contribute to long-term cybersecurity advancement in emerging digital economies.

4.4 Theoretical Foundations

The **Regulatory-Driven Cybersecurity Alignment (RDCA) Theory** is underpinned by insights drawn from three foundational theoretical frameworks: Institutional Theory, the Technology-Organization-Environment (TOE) Framework, and Protection Motivation Theory. Together, these perspectives offer a multidimensional understanding of how organizations respond to regulatory demands and technological pressures.

To begin with, Institutional Theory (DiMaggio & Powell, 1983) argues that organizations are shaped by the norms, rules, and expectations of their broader institutional environment. Organizations often adopt practices not purely for operational efficiency or financial gain but to maintain legitimacy, conform to societal expectations, and avoid sanctions. Within the RDCA framework, the Nigeria Data Protection Regulation (NDPR) is interpreted as a coercive institutional force that drives organizations to modify their operations to comply with emerging standards in data privacy and cybersecurity. Next, the Technology-Organization-Environment (TOE) Framework (Tornatzky & Fleischer, 1990) explains the adoption of new technologies as a function of three key dimensions: technological capability, organizational preparedness, and environmental influences. In the context of RDCA, the NDPR is seen as an environmental driver that compels organizations to enhance their technical infrastructure such as implementing encryption protocols, access management systems, and threat detection technologies while also revising internal policies to support compliance. This framework helps explain the structural and strategic changes that organizations in Nigeria undertake in response to privacy regulation.

The third lens, Protection Motivation Theory (Rogers, 1975), brings a psychological perspective, focusing on how individuals and organizations assess threats and the perceived effectiveness of coping strategies.

Within the RDCA model, organizations that perceive significant risks such as cyberattacks or legal penalties are more likely to adopt protective cybersecurity measures if they believe those measures will be effective. This theory helps account for the motivational factors behind proactive compliance and cybersecurity investment. While each of these theories contributes critical insights, the RDCA Theory advances beyond them by establishing a direct and contextualized link between regulatory pressure and cybersecurity outcomes. Unlike the foundational frameworks, which either focus on legitimacy, innovation adoption, or threat response in isolation, RDCA traces a complete pathway: from regulatory influence, through awareness and operational adaptation, to sustained cybersecurity maturity. This progression is particularly relevant in Nigeria's evolving regulatory landscape, where enforcement is increasingly shaping organizational behavior. As such, RDCA not only builds upon established theories but also extends and localizes them, offering a holistic model for understanding how data privacy regulation drives cybersecurity transformation in emerging economies.

4.5 Theory Justification Based on Findings

i. Justification Based on Findings

Based on the in-depth findings of this study, the development and application of the Regulatory-Driven Cybersecurity Alignment (RDCA) Theory are both appropriate and timely. The empirical evidence strongly reinforces the central claim of RDCA: that data privacy regulations particularly the Nigeria Data Protection Regulation (NDPR) act as external institutional forces that significantly shape and enhance cybersecurity practices in Nigerian organizations. While existing theoretical models often focus on regulatory compliance or risk management independently, RDCA offers a more integrated view by demonstrating that data protection laws not only enforce compliance but actively influence organizational behavior, technology investment, and security culture. These dynamics collectively contribute to the development of cybersecurity maturity. The findings also reveal that Nigeria has made notable strides in establishing a regulatory framework for data privacy through the implementation of the NDPR, the Cybercrime Act, and the E-Privacy Law. These regulations reflect international standards and provide a solid legal basis for advancing cybersecurity. However, their impact is uneven across organizational types. Larger organizations are more likely to comply and increase investment in cybersecurity, while small and medium-sized enterprises (SMEs) face resource limitations that hinder full regulatory alignment. This disparity supports RDCA's argument that regulatory influence is mediated by internal organizational factors such as size, capacity, and readiness.

A key element of RDCA the concept of regulatory awareness is also strongly validated by the data. High levels of awareness among IT professionals (95%) and risk managers (85%) suggest that knowledge of regulatory obligations is a crucial driver of cybersecurity behavior. Organizations that understand the implications of non-compliance are more likely to take proactive measures, as evidenced by the higher investment and compliance rates observed among larger firms. This supports RDCA's proposition that awareness is not merely informational it acts as a motivator for operational and strategic change. Furthermore, the study found a clear link between regulatory compliance and a reduction in cybersecurity incidents. Organizations that reported full compliance also experienced fewer threats, while those with low compliance levels were more exposed. This correlation reinforces RDCA's core assumption that aligning with data privacy regulations serves not just as a legal requirement, but as an effective cybersecurity risk mitigation strategy. RDCA uniquely captures the influence of external regulation on internal behavior, an area often overlooked by traditional frameworks.

The importance of training and awareness initiatives further supports the theoretical underpinnings of RDCA. The data showed that organizations conducting regular staff training achieved better compliance outcomes and stronger cybersecurity performance. SMEs, however, often lacked the resources to implement such initiatives, which impacted their alignment efforts. RDCA accounts for this by emphasizing that regulatory outcomes are mediated through internal practices like education, awareness, and employee preparedness not just through policy adherence. Although cybersecurity incidents have declined since the introduction of privacy regulations, the reduction has not been as substantial as anticipated. This reinforces one of RDCA's key insights: regulation alone is not sufficient to combat complex and evolving cybersecurity threats. To be effective, regulatory compliance must be supported by investments in advanced technologies, human capital development, and strategic threat intelligence. RDCA extends beyond conventional compliance frameworks by promoting a continuous alignment process, where organizations evolve alongside regulatory and threat landscapes rather than relying on one-off compliance efforts.

Additionally, the data shows that organizations compliant with the NDPR benefit from increased consumer trust. Seventy-five percent of respondents reported a rise in customer confidence following compliance, highlighting the broader organizational gains that stem from regulatory alignment. This supports RDCA's broader view that compliance not only reduces risk but also enhances corporate reputation and stakeholder engagement.

The study identified several systemic challenges including high compliance costs, limited awareness among smaller firms, and insufficient government support that limit the effectiveness of existing regulations. These barriers highlight the relevance of the RDCA Theory within the Nigerian context, where resource constraints and uneven enforcement are common. By focusing on alignment rather than static compliance, RDCA provides a flexible and realistic model for achieving cybersecurity advancement in resource-limited environments.

In summary, the findings of this study provide strong empirical support for the RDCA Theory. They demonstrate that data privacy regulations influence cybersecurity not just through mandatory compliance, but by fostering organizational transformation across multiple dimensions. RDCA offers a holistic, theoretically grounded, and contextually appropriate explanation of how regulatory forces drive sustainable improvements in cybersecurity. It is a valuable framework for understanding the interplay between regulation and institutional behavior in emerging economies like Nigeria.

Table 2: Theory Constructs and Propositions

Construct	Definition	Proposition
Regulatory Pressure	The degree to which organizations are influenced or obligated to adhere to GDPR and related regulations.	P1: Increased regulatory pressure encourages stronger implementation of cybersecurity safeguards.
Compliance Awareness	The extent to which organizations comprehend and internalize their responsibilities under data privacy laws.	P2: Enhanced awareness of compliance obligations leads to improved cybersecurity practices.
Operational Adjustment	The modification of internal procedures, policies, and technical systems in response to regulatory demands.	P3: Organizations that adapt their operations to meet privacy requirements tend to strengthen cybersecurity resilience.
Cybersecurity Maturity	The depth, effectiveness, and advancement of an organization's cybersecurity infrastructure and practices.	P4: Reforms driven by regulatory compliance contribute significantly to advancing cybersecurity maturity.
Cultural and Sectoral Context	The impact of organizational values and industry characteristics on regulatory adoption and implementation.	P5: The influence of data privacy regulations on cybersecurity outcomes differs across sectors and cultures.

ii. Conceptual Model Diagram:

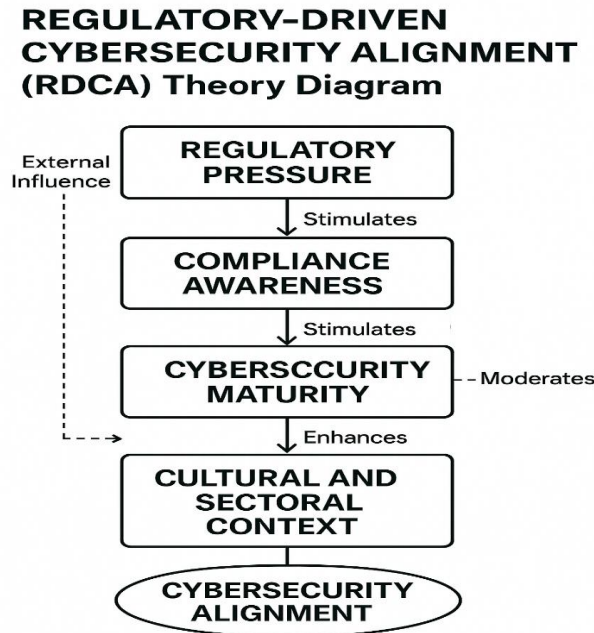


Figure 2: Regulatory-Driven Cybersecurity Alignment (RDCA) Theory Conceptual Model Diagram

The Regulatory-Driven Cybersecurity Alignment (RDCA) Theory Diagram provides a visual representation of how data privacy regulations influence cybersecurity practices in Nigerian organizations. At its foundation, the diagram begins with "Data Privacy Regulations", which encompass key legal instruments such as the Nigeria Data Protection Regulation (NDPR), the Cybercrime Act, and other related legislative policies. These regulations function as external institutional drivers, establishing expectations and compliance requirements for safeguarding personal data and securing organizational digital infrastructures. These legal mandates lead to the emergence of "Perceived Regulatory Pressure", a core construct within the RDCA framework. This concept captures how organizations perceive and interpret regulatory requirements whether through the lens of avoiding sanctions, achieving legitimacy, or conforming to global data protection standards. This perceived pressure becomes a key motivational force, shaping organizational behavior and decision-making related to cybersecurity.

In reaction to this pressure, organizations initiate a range of "Organizational Responses". These responses may include the development of formal compliance strategies, adoption of cybersecurity technologies, staff training programs, and updates to internal policies and procedures. These actions represent a pivotal transition

point, where external regulatory demands are translated into tangible internal changes. Crucially, these responses do more than satisfy legal requirements they serve to enhance the overall security posture of the organization. The culmination of these efforts is reflected in "Cybersecurity Maturity" a state marked by improved threat detection and response, reduced incidence of cyberattacks, stronger data protection capabilities, and greater resilience against emerging digital threats. The RDCA Theory suggests that regulatory compliance is not simply about meeting minimum standards; rather, it acts as a strategic catalyst for broader and deeper improvements in cybersecurity infrastructure and culture.

A notable feature of the RDCA diagram is the inclusion of "Institutional Context" as a moderating factor. This accounts for variables such as the organization's size, industry sector, and available resources, which significantly influence how well an organization can respond to regulatory demands. For example, large enterprises with better funding and technical capacity are often more capable of adopting advanced cybersecurity measures than small or medium-sized enterprises (SMEs). This recognition of contextual variability highlights that the pathway from regulation to cybersecurity advancement is not linear or uniform but shaped by situational realities.

In sum, the RDCA Theory Diagram presents a dynamic and context-sensitive model. It illustrates how regulatory frameworks exert influence on organizational perceptions, which then drive specific internal actions, ultimately leading to improved cybersecurity outcomes. By highlighting the interplay between regulation, organizational response, and contextual factors, the RDCA Theory offers a comprehensive and adaptable approach for understanding the regulatory impact on cybersecurity development in Nigeria.

iii. Derived formulae for Regulatory-Driven Cybersecurity Alignment (RDCA) Theory

To derive a formulaic representation of the Regulatory-Driven Cybersecurity Alignment (RDCA) Theory, we will express the relationships between its key constructs using a structural equation modeling (SEM) or regression-inspired approach. This helps make the theory analytically testable.

RDCA Theory Constructs Recap

Let the theory be grounded on the following latent constructs:

1. **RP** = Regulatory Pressure (e.g., NDPR, Cybercrime Act)
2. **RA** = Regulatory Awareness (awareness level in the organization)
3. **OA** = Operational Alignment (alignment of policies, practices, training)
4. **CM** = Cybersecurity Maturity (investment, incident reduction, capabilities)
5. **CT** = Compliance Threshold (level of compliance with data privacy laws)

RDCA Theoretical Pathways (Sequential Influence)

We hypothesize a causal path as:

$$RP \rightarrow RA \rightarrow OA \rightarrow CM$$

This means:

Regulatory Pressure (RP) leads to Awareness (RA),

Awareness leads to Operational Alignment (OA),

Operational Alignment leads to improved Cybersecurity Maturity (CM).

Derived Formulae

I. Awareness Equation (RA)

Let awareness be a function of regulatory pressure:

$$RA = \alpha_1 \cdot RP + \epsilon_1 \text{ --- (Equation 1)}$$

Where:

α_1 = strength of regulatory influence on awareness

ϵ_1 = error term

II. Operational Alignment Equation (OA)

Operational alignment is influenced by awareness:

$$OA = \alpha_2 \cdot RA + \epsilon_2 \text{ ---- (Equation 2)}$$

Where:

α_2 = coefficient for awareness to alignment translation

ϵ_2 = error term

III. Cybersecurity Maturity Equation (CM)

Cybersecurity maturity depends on operational alignment and indirectly on prior constructs:

$$CM = \alpha_3 \cdot OA + \epsilon_3 \text{ ----- (Equation 3)}$$

Where:

α_3 = coefficient showing how operational alignment leads to maturity

ϵ_3 = error term

IV. Extended Composite Equation

Substitute to create a single formula expressing how Regulatory Pressure ultimately leads to Cybersecurity Maturity:

$$CM = \alpha_3(\alpha_2(\alpha_1 \cdot RP + \epsilon_1) + \epsilon_2) + \epsilon_3 \text{ ----- (Equation 4)}$$

This unfolds the full theoretical process in a functional form.

V. Optional Extension: Compliance Threshold as a Moderator

Let's define a moderator variable for compliance level (CT), which adjusts the strength of OA:

$$CM = (\alpha_3 + \gamma_1 \cdot CT) \cdot OA + \epsilon_4 \text{ ----- (Equation 5)}$$

Where:

γ_1 = moderation coefficient of compliance threshold on cybersecurity outcomes

Summarily, the formulae allow the RDCA Theory to be empirically tested using statistical modeling (e.g., multiple regression, PLS-SEM). You can collect data on RP, RA, OA, CT, and CM and estimate coefficients using software like SPSS, SmartPLS, or AMOS.

iv. Application of the RDCA Theory in Research

The Regulatory-Driven Cybersecurity Alignment (RDCA) Theory offers a valuable framework for empirical investigation into the relationship between data privacy regulations and cybersecurity practices in Nigerian organizations. Researchers can apply this theory through both qualitative and quantitative approaches, such as structured surveys and in-depth interviews, targeting key informants like Data Protection Officers (DPOs), Heads of IT Governance, and Cybersecurity Managers across diverse industries.

These individuals occupy roles that give them direct insight into how regulatory mandates shape internal security behaviors and decision-making processes. By collecting data on how organizations interpret and respond to laws like the Nigeria Data Protection Regulation (NDPR), the Cybercrime Act, and sector-specific privacy guidelines, researchers can examine the connection between perceived regulatory pressure and actual cybersecurity practices. Key areas of investigation might include investments in cybersecurity infrastructure, implementation of technical measures (such as firewalls, encryption, and access controls), staff awareness programs, and preparedness for cyber incidents. This approach enables validation of RDCA's central premise that compliance-driven efforts extend beyond legal adherence and contribute to broader cybersecurity maturity.

The RDCA Theory is also well-suited to comparative sectoral studies that explore how contextual variables influence the regulatory-cybersecurity relationship. For instance, researchers can compare outcomes in tightly regulated sectors like banking and telecommunications with those in less regulated fields such as education or

healthcare. This comparative analysis can reveal how factors like regulatory intensity, organizational resources, and industry-specific risks moderate the impact of data privacy regulations on cybersecurity outcomes. Such insights are valuable for tailoring policy interventions and compliance strategies to specific industry contexts. In essence, using the RDCA Theory as a research framework offers a systematic way to explore the causal pathways between regulation and cybersecurity behavior. It facilitates a deeper understanding of sectoral nuances, organizational responses, and the effectiveness of regulatory mechanisms. Ultimately, RDCA provides a robust foundation for advancing empirical research, informing evidence-based policymaking, and enhancing cybersecurity strategies in Nigeria's evolving digital ecosystem.

V. Comparison of RDCA with Existing Theories

Below is a comparative table that contrasts the Regulatory-Driven Cybersecurity Alignment (RDCA) Theory with key existing theories that relate to data privacy regulations and cybersecurity practices, particularly in the Nigerian context:

Table 3: Comparison of RDCA with Existing Theories

Theory	Core Focus	Application to Cybersecurity and Data Privacy	Limitations in Nigerian Context	How RDCA Theory Improves Upon It
Institutional Theory (DiMaggio & Powell, 1983)	How organizations conform to institutional pressures for legitimacy	Emphasizes coercive pressure from regulations (e.g., NDPR) as drivers of compliance behavior	Does not explain how compliance leads to technical cybersecurity improvements	RDCA integrates institutional pressure with operational responses and cybersecurity maturity outcomes
Technology-Organization-Environment (TOE) Framework (Tornatzky & Fleischer, 1990)	Adoption of innovation influenced by tech capacity, organizational factors, and environment	Useful in explaining why some firms adopt data privacy tools and practices	Lacks focus on regulatory influence as a primary driver of cybersecurity behavior	RDCA builds on TOE by making regulation the central external driver and linking it directly to cybersecurity transformation
Protection Motivation Theory (PMT) (Rogers, 1975)	Motivation to act based on threat appraisal and coping efficacy	Explains individual/organizational motivation to adopt protective measures (e.g., against cyber threats)	Focuses primarily on psychological aspects; lacks systemic view of compliance dynamics	RDCA incorporates PMT concepts (e.g., perceived threat) into a broader organizational model that includes structural change
Deterrence Theory	Behavior influenced by fear of punishment or sanctions	Applicable to understanding NDPR enforcement and compliance behavior	Overemphasizes punitive aspect, ignoring positive transformation outcomes	RDCA reframes regulation as both deterrent and developmental trigger for cybersecurity growth
General Compliance Models	Adherence to rules due to legal or normative expectations	Explains why organizations obey laws and policies	Often treat compliance as the end goal rather than a means to strategic improvement	RDCA sees compliance as a pathway to cybersecurity advancement, not just legal adherence

Theory	Core Focus	Application to Cybersecurity and Data Privacy	Limitations in Nigerian Context	How RDCA Theory Improves Upon It
Regulatory Compliance Model (RCM)	Frameworks that encourage legal and regulatory conformity	Basis for many audit/checklist-based compliance programs	Often static, lacking a feedback loop for continuous improvement	RDCA emphasizes continuous alignment, adaptation, and capacity building—especially relevant in dynamic threat landscapes
Cybersecurity Capability Maturity Models (e.g., CMMI, NIST)	Assessment of cybersecurity maturity based on practices and capabilities	Provide benchmarking and structured growth pathways	Do not factor in regulatory context or how compliance efforts begin transformation	RDCA uniquely connects regulatory pressure to maturity outcomes, explaining <i>why</i> and <i>how</i> growth occurs under regulation
RDCA Theory (New)	Regulation-driven alignment between compliance and cybersecurity improvement	Synthesizes regulation, organizational response, and maturity within Nigerian realities	Designed specifically for developing contexts; considers sector, size, and capacity disparities	Provides a holistic, context-aware, and empirically validated framework to guide regulatory impact and policy development

The Regulatory-Driven Cybersecurity Alignment (RDCA) Theory builds upon and extends several established theoretical frameworks by explicitly linking data privacy regulation to cybersecurity outcomes, especially within developing economies like Nigeria. One of the foundational theories RDCA draws from is Institutional Theory (DiMaggio & Powell, 1983), which suggests that organizations conform to external pressures such as legal mandates or societal expectations in order to gain legitimacy. While Institutional Theory provides a useful explanation for why organizations may comply with regulations like the Nigeria Data Protection Regulation (NDPR), it does not clarify how such compliance translates into improved cybersecurity practices. RDCA addresses this gap by not only acknowledging coercive regulatory forces but also demonstrating how they catalyze operational, technical, and cultural shifts that enhance cybersecurity maturity.

Similarly, the Technology-Organization-Environment (TOE) Framework [5] explains the adoption of innovations based on an organization’s technological capabilities, internal readiness, and external environment. This framework is valuable for understanding how firms adopt tools such as encryption or data protection software. However, TOE does not centralize regulatory influence as a driver of behavior change. RDCA advances TOE by positioning regulation especially in the form of external legal pressure as the core trigger for technology adoption, policy restructuring, and workforce development in cybersecurity. Protection Motivation Theory (PMT) [6] adds a psychological perspective, focusing on how threat perception and belief in protective strategies drive action. This theory is applicable when considering how

Nigerian organizations react to perceived threats of cyberattacks or regulatory penalties. Nevertheless, PMT primarily targets individual behavior and lacks a comprehensive organizational systems view. RDCA incorporates PMT’s motivational constructs but embeds them within a broader organizational context, explaining how psychological drivers interact with structural and resource-based factors to shape cybersecurity responses. Furthermore, Deterrence Theory and general Regulatory Compliance Models provide insights into how fear of sanctions or legal penalties influence behavior. While these models help explain why organizations may initially conform to regulations like the NDPR, they often treat compliance as a static goal. RDCA distinguishes itself by reframing regulatory compliance as a means not an end to achieving higher cybersecurity maturity. It emphasizes that true regulatory impact comes not only from compliance checklists, but from sustained organizational transformation driven by compliance efforts.

Comparatively, Cybersecurity Capability Maturity Models (such as NIST or CMMI) offer detailed assessments of an organization’s cybersecurity development over time. These models are useful for benchmarking practices but typically overlook the role of regulatory pressure as a developmental catalyst. RDCA fills this void by directly linking compliance-driven reforms to maturity progression, especially in environments where regulation is a key driver of security investment and policy change. Unlike these existing theories, RDCA is uniquely suited to resource-constrained and institutionally evolving environments like-Nigeria.

It takes into account institutional context such as sector-specific challenges, organizational size, and access to resources which significantly influence how regulations are interpreted and implemented. By doing so, RDCA offers a practical, adaptive, and empirically grounded model for understanding how external regulatory forces are internalized and translated into cybersecurity improvements. It bridges theoretical gaps and reflects the real-world dynamics of regulatory influence on digital security in developing economies.

vi. Implications of the RDCA Theory

The Regulatory-Driven Cybersecurity Alignment (RDCA) Theory offers significant implications across policy formulation, managerial decision-making, and academic research. These implications provide a practical bridge between theoretical understanding and real-world action, supporting stakeholders in leveraging data privacy regulations to drive cybersecurity improvements.

- **Policy Implications:** From a policymaking standpoint, the RDCA Theory highlights the transformative potential of strict enforcement of data privacy laws such as the NDPR, Cybercrime Act, and E-Privacy Law beyond simply ensuring legal adherence. It suggests that more rigorous implementation of these laws can act as a lever to enhance national cybersecurity posture. By applying the RDCA framework, policymakers can design focused strategies such as sector-specific compliance assistance programs, awareness campaigns, and enforcement mechanisms that encourage organizations, especially small and medium-sized enterprises (SMEs), to improve their cybersecurity practices. The theory also stresses the importance of providing technical and financial support to under-resourced organizations, ensuring equitable participation in the national cybersecurity landscape.
- **Managerial Implications:** At the organizational level, RDCA shifts the traditional perspective of regulatory compliance from a burdensome obligation to a strategic enabler. Business leaders are encouraged to view compliance initiatives not as mere legal requirements, but as opportunities to strengthen their cybersecurity capabilities. Activities such as risk assessments, security audits, employee training, and the implementation of access controls and encryption protocols often driven by privacy laws can directly enhance an organization's cyber resilience. This reframing

supports the cultivation of a proactive security culture, embedding cybersecurity considerations into daily operations and long-term planning. Ultimately, this approach improves not only regulatory compliance but also customer trust and operational stability.

- **Research Implications:** For scholars and researchers, RDCA offers a fresh theoretical model that links regulatory compliance to concrete cybersecurity outcomes a connection that has been underexplored in previous studies. It invites new lines of inquiry into how external regulatory forces shape internal organizational behavior and technological adaptations. Researchers can use RDCA to investigate these dynamics across different sectors, regions, or regulatory environments, thereby testing its generalizability and refining its theoretical components. The framework also opens pathways for longitudinal studies that track how regulatory pressures evolve and impact cybersecurity maturity over time, contributing valuable knowledge to the fields of information systems, policy studies, and cybersecurity management.

Overall, the RDCA Theory extends beyond theoretical contribution to influence national policy, corporate governance, and academic discourse. By promoting a holistic and integrative approach, it serves as a practical guide for transforming regulatory compliance into a driver of sustainable cybersecurity improvement at both organizational and national levels.

vii. Why the RDCA Theory Is the Most Suitable Framework

The Regulatory-Driven Cybersecurity Alignment (RDCA) Theory emerges as the most suitable and effective framework for analyzing the impact of data privacy regulations on cybersecurity practices in Nigeria. Its strength lies in its ability to address the shortcomings of conventional models by framing compliance not as a static achievement, but as a dynamic process that fosters ongoing cybersecurity improvement. Unlike traditional approaches that focus solely on whether organizations meet legal requirements, RDCA presents a developmental pathway: regulatory pressure heightens organizational awareness, which in turn prompts concrete operational responses such as policy reforms, staff training, and technology investments. These responses, over time, lead to enhanced cybersecurity maturity. This progression-oriented perspective captures how regulatory mandates can catalyze long-term security evolution rather than short-term legal conformity.

Another reason RDCA stands out is its practical recognition of organizational diversity and constraints. It acknowledges that Nigerian organizations vary widely in their capacity to comply with data privacy laws. Factors such as inconsistent enforcement, limited technical skills, financial constraints, and cultural resistance can significantly influence how regulation is received and implemented. By embedding these contextual realities into its structure, RDCA provides a more accurate reflection of the Nigerian regulatory landscape, particularly for resource-constrained sectors like SMEs and public institutions that are often overlooked by global models.

Furthermore, the RDCA Theory emphasizes strategic alignment over mere regulatory adherence. Traditional compliance frameworks typically assess outcomes in binary terms compliant or non-compliant. RDCA, however, reframes regulation as a driver of internal alignment, encouraging organizations to integrate privacy mandates into broader cybersecurity strategies. This shift in focus helps organizations move beyond treating regulations as checklists and instead view them as opportunities to enhance resilience, build stakeholder trust, and support organizational integrity.

In sum, RDCA's flexibility and scalability make it applicable across different sectors and organizational sizes. Whether in finance, healthcare, education, or government, the model can be adapted to fit varying levels of regulatory enforcement, awareness, and cybersecurity capabilities. From large financial institutions with formal compliance infrastructures to smaller organizations with limited IT resources, RDCA provides a practical and inclusive framework that can guide cybersecurity advancement under Nigeria's evolving data privacy regime. This makes it not only a theoretically sound model but also a pragmatic tool for driving security transformation in emerging economies.

5. CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

This study introduced and validated the Regulatory-Driven Cybersecurity Alignment (RDCA) Theory, a novel framework designed to explain the influence of data privacy regulations on cybersecurity practices within Nigerian organizations. Through empirical analysis, the research confirmed that compliance with regulations such as the Nigeria Data Protection Regulation (NDPR), the Cybercrime Act, and sectoral data privacy guidelines acts not only as a legal requirement but also as a strategic driver of cybersecurity maturity. The RDCA Theory illustrates a stepwise transformation where regulatory pressure stimulates awareness, prompts operational adjustments,

and ultimately enhances cybersecurity outcomes. Findings show that larger organizations tend to comply more fully and exhibit higher cybersecurity maturity, while small and medium-sized enterprises (SMEs) face significant limitations due to resource and capacity constraints. The theory's inclusion of contextual factors such as organizational size, sector, and internal culture offers a realistic lens for understanding these disparities. Unlike traditional compliance models, RDCA emphasizes alignment rather than mere conformity, encouraging organizations to integrate regulatory obligations into broader risk management and security strategies. Ultimately, the study contributes a practical and adaptable model for both scholars and practitioners. It not only enriches academic discourse by bridging compliance theory with cybersecurity outcomes but also provides actionable insights for improving national cybersecurity resilience through regulatory means.

5.2 Recommendations

For Policymakers

- **Strengthen Regulatory Enforcement:** Government agencies, such as the Nigeria Data Protection Commission (NDPC), should intensify monitoring and enforcement of data privacy laws to ensure consistent compliance across sectors.
- **Support for SMEs:** Develop targeted initiatives such as financial incentives, training programs, and technical toolkits to support SMEs in overcoming barriers to compliance and cybersecurity improvement.
- **Sector-Specific Guidelines:** Issue tailored data protection and cybersecurity guidelines for different sectors (e.g., health, education, fintech) to accommodate unique risk profiles and operational challenges.

For Organizational Leaders

- **Integrate Compliance into Strategy:** Treat data privacy obligations as part of a broader cybersecurity strategy, rather than as isolated legal requirements.
- **Invest in Capacity Building:** Allocate resources toward staff training, awareness campaigns, and IT system upgrades that support both compliance and cyber resilience.
- **Foster a Security Culture:** Promote a culture of security from top leadership down, ensuring that employees at all levels understand and uphold data protection and cybersecurity responsibilities.

For Researchers and Academics

- **Further Empirical Testing of RDCA:** Apply the RDCA framework to additional contexts such as other African nations or specific industries to validate its generalizability and refine its constructs.
- **Longitudinal Studies:** Conduct long-term studies to examine how regulatory pressures and organizational responses evolve over time, offering deeper insights into sustainability and effectiveness.
- **Cross-Theory Integration:** Explore how RDCA can be integrated with other theories such as the TOE Framework, Institutional Theory, or Diffusion of Innovation, to build a more comprehensive understanding of regulatory-driven change.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the growing academic and professional interest in the subject matter explored in this study titled *"Compliance as a Catalyst: Proposing the RDCA Theory for Institutional Cybersecurity Growth in Emerging Economies."* The development of the Regulatory-Driven Cybersecurity Alignment (RDCA) Theory was inspired by the increasing relevance of regulatory compliance frameworks and their transformative potential in strengthening institutional cybersecurity practices across developing nations. This work responds to a recognized need within both academic and policy-making circles to bridge the gap between regulatory obligations and cybersecurity implementation. The author appreciates the supportive interest from scholars, practitioners, and stakeholders in cybersecurity governance, whose feedback and engagement continue to shape the relevance of this theoretical contribution.

The acknowledgement of interest is made in recognition of the broader community of researchers and professionals whose insights and concerns helped guide the direction and refinement of this work. Their interest is not only appreciated but is also seen as a catalyst for future research and collaboration in this critical area of study.

DECLARATION OF INTEREST STATEMENT

The authors declare that there is no conflict of interest regarding the publication of this research titled *"Compliance as a Catalyst: Proposing the RDCA Theory for Institutional Cybersecurity Growth in Emerging Economies."* This study was independently

conducted and developed without any financial, institutional, or personal relationships that could be perceived to influence the findings, interpretations, or conclusions presented. The proposed RDCA (Regulatory-Driven Cybersecurity Alignment) Theory was conceptualized solely for academic and policy-oriented purposes. No external party influenced the formulation of the theory or the analysis of data used in support of the research. Any references to institutions, regulations, or frameworks are made strictly for scholarly examination and do not imply endorsement or criticism. The research is purely for educational, scientific, and policy development contributions to the fields of cybersecurity, regulatory compliance, and information systems governance in emerging economies.

REFERENCES

- [1].World Bank. (2021). World Development Report 2021: Data for Better Lives. <https://www.worldbank.org/en/publication/wdr2021>
- [2].Parker, C., & Nielsen, V. L. (2011). Explaining compliance: Business responses to regulation. Edward Elgar Publishing.
- [3].ENISA. (2020). Cybersecurity Special Report: Emerging Challenges for SMEs. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu>
- [4].DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. <https://doi.org/10.2307/2095101>
- [5].Tornatzky, L. G., & Fleischer, M. (1990). The processes of technological innovation. Lexington Books.
- [6].Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
- [7].NITDA. (2022). Nigeria Data Protection Regulation (NDPR) Implementation Framework. National Information Technology Development Agency.
- [8].Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46(5), 267–270. <https://doi.org/10.1016/j.im.2009.03.010>
- [9].Renaud, K., & Goucher, W. (2013). The curious incidence of security breaches by knowledgeable employees and the pivotal role a configuration management system plays in a system's security. Proceedings of the 12th European Conference on Information Warfare and Security, 410–418.

[10].OECD. (2020). Digital transformation in the age of COVID-19: Building resilience and bridging divides. Organisation for Economic Co-operation and Development. <https://www.oecd.org/digital/>

[11].Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, 18(2), 106–125. <https://doi.org/10.1057/ejis.2009.6>

[12].Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83–95. <https://doi.org/10.1016/j.cose.2011.10.007>

[13].Alkalbani, A., Deng, H., & Kam, B. (2017). A review of the information security maturity models. *International Journal of Computer Science and Information Security*, 15(6), 244–256.

[14].Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

[15].Bada, A., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672. <https://arxiv.org/abs/1901.02672>

[16].Ayoade, G. O., & Adebisin, F. (2021). Evaluating cybersecurity governance practices in Nigerian organizations. *African Journal of Information and Communication*, 27, 1–18. <https://doi.org/10.23962/10539/31202>