© AUG 2021 | IRE Journals | Volume 5 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV5I2-1722621

Cyber Risk Management Maturity in Nigeria's Insurance Sector: An Assessment Against the NAICOM and NDPR Regulatory Landscape

SAMUEL FADERO[1], STANLEY NWAKAMMA[2], DEMILADE JOODA[3], SERIF OYINDAMOLA OYESIJI[4]

[1]*SanlamAllianz Life Insurance Ltd, Lagos Nigeria*
[2]*Independent Researcher, USA*
[3]*Fasyl Technology Ghana - Accra, Ghana*
[4]*Independent Researcher, Lagos Nigeria*

Abstract- ***This review critically examines the maturity of cyber risk management within Nigeria's insurance sector, with particular attention to the extent to which organisational practices align with prevailing supervisory, data-protection, and resilience expectations. It seeks to determine whether insurers are progressing beyond formal compliance toward embedded, measurable, and adaptive cyber-risk capabilities. The study adopts a structured narrative review approach, synthesising scholarly literature, regulatory instruments, industry guidance, and established cybersecurity maturity frameworks to evaluate governance, threat exposure, privacy protection, incident management, operational resilience, workforce capability, and regulatory alignment. The findings indicate that cyber maturity within the sector is shaped by the quality of board oversight, integration of cyber risk into enterprise risk management, effectiveness of technical and organisational controls, third-party governance, and the ability to detect, respond to, and recover from disruptive events. The review further identifies significant barriers, including fragmented accountability, uneven security investment, skills shortages, weak security cultures, legacy systems, inconsistent control measurement, and gaps between documented compliance and operational effectiveness. It also establishes that regulatory conformity alone is insufficient to demonstrate resilience where controls are not continuously tested, monitored, and improved. The study concludes that a more mature cyber-risk posture requires coordinated governance, risk-based supervision, measurable maturity assessments, stronger privacy-by-design practices, continuous monitoring, and tested incident-response and recovery capabilities. It recommends enhanced board accountability, sector-wide threat intelligence, structured third-party assurance, sustained cybersecurity workforce development, and closer alignment between supervisory expectations and evidence-based resilience metrics. These measures are essential for strengthening policyholder protection, operational continuity, regulatory confidence, and the long-term stability of Nigeria's increasingly digital insurance ecosystem amid increasingly sophisticated cyber threats.***

Keywords: cyber risk management; cyber maturity; nigerian insurance sector; NAICOM; data protection; operational resilience

I. INTRODUCTION

1.1 Digital Transformation and Emerging Cyber Risks

Digital transformation has altered the operating architecture of insurance by shifting customer acquisition, underwriting, claims administration and service delivery toward digital platforms. Cloud computing, mobile applications, advanced analytics, application programming interfaces and automated decision systems compress processing times and expand access, but also enlarge the interfaces through which policyholder and corporate data may be exposed. Digitalisation therefore changes how insurers create value and the location and interconnectedness of operational risk across the insurance value chain (Eling & Lehmann, 2018).

The strategic significance of this transition is evident in insurers' movement from isolated technology projects toward enterprise-wide digital agendas. Such agendas link technology investment with innovation, customer experience and organisational performance,

making cyber resilience inseparable from business strategy. Where transformation proceeds faster than governance, legacy applications, fragmented databases, weak access controls and poorly governed integrations can create vulnerabilities that undermine digital initiatives (Bohnert, Fritzsche & Gregor, 2019).

InsurTech intensifies this transformation by combining data-driven services, platform intermediation and technology-enabled relationships among insurers, intermediaries, customers and external providers. These innovations can improve personalisation and efficiency while extending data flows beyond organisational boundaries. For Nigerian insurers, expanding digital ecosystems consequently require security architectures capable of protecting information across partner interfaces and outsourced technology services rather than concentrating controls within traditional corporate perimeters (Stoeckli, Dremel &Uebernickel, 2018).

African evidence illustrates that this transition is neither uniform nor frictionless. Research on South Africa's short-term insurance sector shows that Internet of Things and InsurTech technologies possess transformational potential, although incumbent insurers may adopt them cautiously because business models and organisational capabilities constrain change. This is relevant to Nigeria because uneven digital maturity can produce hybrid environments where legacy systems coexist with connected technologies, complicating visibility, control standardisation and cyber-risk governance (Moodley, 2019).

Cyber risk is particularly consequential for insurers because digital incidents can generate confidentiality breaches, service interruption, liability, recovery costs and reputational damage while creating underwriting exposure through cyber-insurance products. Empirical analysis demonstrates that cyber losses exhibit characteristics challenging conventional insurability, including dependence, potentially severe losses and information asymmetries. These properties make reliable risk identification, accumulation management and security capability increasingly important as insurers digitise (Biener, Eling & Wirfs, 2015).

The problem extends into underwriting. Cyber insurers frequently assess applicants through information concerning organisational characteristics, security practices and previous incidents, yet underwriting remains constrained by imperfect and heterogeneous information. Digital transformation therefore has a dual effect: it exposes insurance institutions to direct cyber threats while requiring them to evaluate comparable threats within policyholders' digital environments, increasing the importance of credible cybersecurity data and disciplined risk assessment (Romanosky et al., 2019). Evidence from the wider financial sector indicates that perceptions of cyber threats influence how organisations prioritise and manage digital risk. As financial activities become more technology-dependent, decision-makers must interpret changing threat conditions while balancing security investment against operational objectives. Nigerian insurers consequently require cyber-risk approaches that connect technological monitoring with enterprise risk processes, management judgement and business continuity rather than treating cybersecurity as an isolated information-technology function (Varga, Brynielsson & Franke, 2021).

Within Nigeria, blockchain research demonstrates the relevance of decentralised digital architectures, automated transactions and peer-to-peer exchanges. Although this energy-sector study does not directly examine insurance or cybersecurity and should be treated as contextually rather than evidentially aligned, it illustrates how distributed technologies create new governance, trust and systems-integration considerations. Similar architectural shifts in insurance can broaden dependencies and demand stronger authentication, data integrity, access governance and oversight as digital ecosystems expand (Shittu et al., 2021).

1.2 Cybersecurity, Privacy, and Operational Resilience Imperatives

Cybersecurity in insurance must be understood as a strategic capability rather than a narrow information-technology function because insurers depend on

continuous access to policy, claims, actuarial, payment and customer-identification systems. The concentration of sensitive personal and financial information makes disruption, manipulation or unauthorised disclosure capable of affecting service continuity, regulatory compliance and public confidence. In Nigeria, these pressures are intensified by uneven cyber preparedness, infrastructure limitations and persistent digital-crime exposure, making organisational readiness central to protecting digital insurance operations (Iorliam, 2019).

Privacy is inseparable from cybersecurity because the confidentiality, integrity and lawful processing of personal information depend on effective technical and organisational safeguards. European experience under the GDPR demonstrates that data protection increasingly requires accountability, security-by-design, breach responsiveness and stronger governance over personal-data processing. These principles are relevant to Nigerian insurers handling identity records, medical information, beneficiary details and financial data, where privacy failures can create legal, reputational and operational consequences beyond the immediate security incident (Tikkinen-Piri, Rohunen& Markkula, 2018).

African financial-sector experience reinforces this relationship. South Africa's regulatory environment illustrates how expanding digital financial services expose consumers' personal information to cybercrime while compelling institutions to align information-security controls with statutory data-protection obligations. For Nigerian insurers, comparable pressures imply that privacy compliance should not operate as documentation detached from cybersecurity; rather, data inventories, access restrictions, encryption, retention controls and breach-management processes should form part of an integrated risk architecture (Warikandwa, 2021).

Operational resilience extends this architecture beyond prevention. Financial institutions cannot reasonably assume that every intrusion, technology failure or third-party disruption will be prevented; mature organisations must preserve critical services, absorb shocks, recover essential capabilities and adapt after incidents. This resilience perspective is particularly important for insurers because prolonged outages can interrupt premium administration, claims settlement, customer communication and regulatory reporting, transforming a technical event into a business-continuity problem (Dupont, 2019).

The economic consequences of cyber incidents further justify this integrated approach. Evidence on successful cyberattacks shows that security failures can produce reputational penalties and adverse market consequences, particularly where incidents reveal weaknesses in risk governance or compromise sensitive customer information. Accordingly, cyber maturity in insurance should incorporate executive oversight, incident escalation, recovery planning and stakeholder communication alongside preventive controls, because organisational credibility after an attack depends partly on the quality and speed of institutional response (Kamiya et al., 2021).

Cybersecurity and privacy also require dynamic assessment rather than periodic compliance checks. Automated risk-management approaches can combine information about assets, vulnerabilities, threats, processing activities and personally identifiable information to support responsive control decisions. Such integration is pertinent to Nigerian insurers operating interconnected systems because it enables risk prioritisation to reflect both cyber exposure and privacy consequences, strengthening alignment between technical safeguards, data-governance duties and operational priorities. Gonzalez-Granadillo et al. (2021) therefore provide a basis for treating cyber and privacy risks as interdependent and continuously changing.

A comparable resilience principle appears in engineering research on grounding-system optimisation, where protection is strengthened through performance-oriented design, monitoring, context-sensitive assessment and adaptation rather than reliance on static requirements. Although this study does not examine cybersecurity, privacy or insurance and should not be treated as direct evidence for the sector, its systems-resilience logic is transferable: Nigerian insurers similarly require controls that are tested, monitored and adjusted as

conditions change rather than installed for formal compliance (Shittu et al., 2020).

1.3 Regulatory Context and Cyber Maturity Challenges

Nigeria's insurance sector operates within a regulatory environment in which cybersecurity maturity is increasingly shaped by overlapping obligations relating to data protection, corporate governance, information security and operational risk. The Nigeria Data Protection Regulation (NDPR) established an important compliance baseline by imposing duties concerning lawful processing, accountability, security safeguards and breach-related responsibilities. Yet weaknesses in regulatory design and enforcement can limit the extent to which formal compliance translates into demonstrable organisational capability, creating uncertainty around how insurers operationalise privacy requirements within broader cyber-risk programmes (Omotubora, 2021).

This challenge is not unique to Nigeria. South Africa's experience shows that cybersecurity governance depends not only on legislation but also on institutional coordination, implementation capacity and clear assignment of responsibility across public and private actors. Fragmented mandates, delayed implementation and shortages of specialist expertise can weaken otherwise credible regulatory frameworks. For Nigerian insurers, this implies that compliance with NAICOM expectations and the NDPR should be evaluated alongside governance effectiveness, technical capability and institutional preparedness rather than through documentary conformity alone (Sutherland, 2017).

Cyber maturity therefore requires a structured means of determining whether regulatory controls are embedded, repeatable and measurable. Holistic maturity frameworks demonstrate the value of integrating multiple security and privacy requirements into a unified assessment architecture, enabling organisations to identify gaps across governance, technical protection, awareness, incident management and assurance functions. Such approaches are relevant to insurers because fragmented compliance programmes can obscure systemic weaknesses that cut across regulatory domains (Aliyu et al., 2020).

Regulatory alignment also benefits from maturity models that translate legal obligations into graded organisational capabilities. The NIS Directive-compliant Cybersecurity Maturity Assessment Framework, for example, links regulatory expectations with progressively developed controls and measurable performance levels. Its underlying logic is pertinent to the Nigerian insurance context, where maturity assessment should distinguish between controls that merely exist and those that are institutionalised, monitored, tested and continuously improved (Drivas et al., 2020).

The governance dimension remains equally significant. Evidence from the United States indicates that executive-level information-technology expertise is associated with lower incidence of reported data-security breaches, underscoring the importance of leadership competence in converting policy into effective oversight. Nigerian insurers therefore require boards and senior executives capable of interpreting cyber risk, challenging management assumptions and integrating security considerations into strategic and operational decision-making (Haislip, Lim & Pinsker, 2021).

Financial-sector evidence from Peru further demonstrates that cyber maturity can be assessed through staged progression from initial practices to managed and optimised capabilities, incorporating cloud security and privacy alongside conventional controls. This is particularly relevant to Nigeria's insurance industry, where differences in organisational size, technological sophistication and investment capacity may produce uneven maturity across firms. A defensible regulatory assessment should therefore examine not only compliance status but also the depth, consistency and sustainability of cybersecurity capabilities across critical business processes under rapidly evolving regulatory and technological conditions nationwide (Alayo et al., 2021).

1.4 Aim, Scope, Objectives, and Review Approach

This review aims to critically examine the maturity of cyber risk management practices within Nigeria's insurance sector and to assess the extent to which prevailing organisational capabilities align with the regulatory expectations established by the National Insurance Commission and the Nigeria Data Protection Regulation. The study is concerned not merely with formal compliance, but with the depth, consistency, and institutionalisation of cybersecurity governance, privacy protection, operational resilience, and risk-based control practices across insurance organisations.

The scope encompasses cyber risk governance, board oversight, enterprise risk integration, data protection, threat identification, preventive and detective controls, incident response, business continuity, third-party risk management, workforce capability, and continuous improvement. Particular attention is given to the relationship between regulatory obligations and actual organisational maturity, recognising that documented policies do not necessarily demonstrate effective cyber resilience.

The review pursues four objectives: to clarify the conceptual foundations of cyber risk maturity in insurance; to identify the principal cybersecurity and privacy obligations relevant to Nigerian insurers; to evaluate common maturity gaps and institutional constraints that may inhibit effective implementation; and to develop strategic pathways for strengthening regulatory alignment and sector resilience.

Methodologically, the study adopts a structured narrative review approach, drawing together scholarly literature, regulatory instruments, industry guidance, and established cyber maturity frameworks. Evidence is synthesised thematically to compare governance, technical, operational, and compliance dimensions. This approach supports a contextual assessment of Nigeria's insurance environment while enabling comparison with recognised international practices and providing a coherent basis for subsequent analysis of regulatory benchmarks and maturity challenges in practice.

II. FOUNDATIONS OF CYBER RISK MANAGEMENT MATURITY

2.1 Cyber Threats and Insurance Sector Exposure

The insurance sector occupies a distinctive position within the contemporary cyber-threat landscape because it is simultaneously a custodian of sensitive personal and financial information, a digitally dependent service provider, and a potential risk carrier for losses generated by cyber incidents. Core activities such as underwriting, premium administration, claims processing, actuarial modelling and customer servicing rely on interconnected platforms, creating multiple points through which malicious actors may compromise confidentiality, integrity or availability. Cyber incidents therefore expose insurers to direct operational disruption and cascading economic, reputational and customer-related harms that persist beyond initial compromise (Agrafiotis et al., 2018).

Threat exposure is intensified by the diversity of attack vectors confronting digital organisations. Phishing, credential theft, malware, ransomware, denial-of-service attacks, data exfiltration and exploitation of vulnerable applications can interrupt critical insurance processes or facilitate unauthorised access to policyholder records. Evidence from South Africa demonstrates that expanding technological dependence has enlarged organisational attack surfaces, with data exposure, system intrusion and criminally motivated attacks recurring across major sectors. These patterns are instructive for Nigerian insurers operating within digitising African environments (Pieterse, 2021).

From an insurance perspective, cyber risk is unusually difficult to evaluate because threat frequency, vulnerability and loss severity evolve rapidly and may be interdependent across firms. Cyber-insurance scholarship identifies limited historical data, information asymmetry, correlated losses and changing technologies as persistent constraints on underwriting and accumulation analysis. Nigerian insurers considering cyber coverage must therefore manage the dual exposure of defending their own information assets while evaluating the security posture and potential losses of

organisations seeking risk transfer (Marotta et al., 2017).

The quality of security assessment is consequently central to understanding exposure. Analysis of cyber-insurance proposal forms has shown that insurer assessments do not invariably capture all controls contained in established information-security frameworks. Reliance on incomplete self-assessment may therefore generate adverse selection or underestimate material vulnerabilities. Within Nigeria, where organisational cyber maturity may differ across prospective policyholders, insurers require granular evidence concerning access control, patching, backups, incident response, network security and governance before accepting cyber liabilities (Woods et al., 2017).

Cyber exposure also raises an economic allocation problem. Organisations must determine whether particular risks should be mitigated internally, transferred through insurance, retained, or addressed through combinations of security investment and coverage. Decision models demonstrate that insurance choices depend on vulnerabilities, expected losses, security safeguards and the price of risk transfer. Such reasoning is relevant to Nigerian insurers both as corporate entities purchasing protection and as underwriters seeking to differentiate insurable cyber exposure from risks requiring stronger controls before coverage (Mukhopadhyay et al., 2013).

Risk transfer should therefore complement rather than substitute for cybersecurity. A structured cyber-risk management process requires organisations to identify exposures, quantify probable consequences, evaluate control options and determine the residual risk suitable for insurance. This is particularly pertinent to insurers because excessive reliance on contractual transfer without corresponding security investment can leave operational vulnerabilities unresolved and increase the possibility of losses affecting policyholders, shareholders and counterparties simultaneously (Gordon, Loeb & Sohail, 2003).

The supplied Nigerian engineering study does not directly examine cybersecurity or insurance and should not be interpreted as sector-specific evidence. Its treatment of integrating a secondary energy carrier into an interconnected national grid nevertheless illustrates a limited systems principle: introducing new components into complex infrastructures creates dependencies that must be modelled and governed. Applied cautiously, this analogy underscores why Nigerian insurers should consider third-party connections and external service dependencies when mapping cyber exposure in practice (Shittu et al., 2019).

2.2 Cyber Risk Maturity Models and Dimensions

Cyber risk maturity models provide a structured means of determining whether cybersecurity capabilities are merely ad hoc or have become governed, repeatable, measurable and continuously improved. Their value for Nigeria's insurance sector lies in converting broad security expectations into observable organisational capabilities that can be benchmarked over time. Comparative research shows that maturity models differ in scope, assessment depth, intended users and domain specificity, meaning that insurers should avoid adopting any framework mechanically without considering regulatory obligations, organisational scale and risk exposure (Garba et al., 2020).

A mature assessment architecture should therefore distinguish between capability domains and maturity levels. Core dimensions normally encompass governance, risk identification, asset management, access control, vulnerability management, security monitoring, incident response, recovery, workforce competence and assurance. Comparative analysis of established cybersecurity capability models demonstrates that staged maturity structures enable organisations to establish baselines, identify deficiencies and prioritise improvement pathways rather than treating cybersecurity as a binary state of compliance or non-compliance (Rea-Guaman et al., 2017).

The concept is especially relevant in regulated sectors because maturity models can provide a common language for management, technical teams and

supervisors. For critical infrastructure providers, capability models help organisations communicate preparedness, evaluate control effectiveness and identify weaknesses arising from interdependent systems. Nigerian insurers similarly require a model that captures dependencies among digital platforms, outsourced services, customer databases and payment infrastructures (Miron & Muita, 2014).

Maturity must also reflect adaptability. A dynamic capability perspective treats cybersecurity as an evolving organisational competence in which controls, processes and decision structures must change as threats, technologies and business conditions change. This is particularly important for insurers whose digital channels and third-party ecosystems continuously alter the underlying risk environment (Adler, 2013).

African conditions further require contextualisation. A maturity model developed around the African Union cybersecurity framework illustrates how staged assessments can connect policy, institutional capability, partnerships and cybersecurity capacity-building, highlighting the importance of regional realities rather than relying exclusively on externally developed benchmarks (von Solms, 2015).

The requested Nigerian engineering source is not a cybersecurity or insurance study and should not be treated as direct maturity evidence. Its relevance is limited to the transferable principle that performance improves through systematic measurement, control and optimisation. Applied cautiously, this principle reinforces the need for Nigerian insurers to measure control effectiveness and progressively refine cyber-risk processes instead of equating the existence of controls with maturity (Sunday et al., 2019).

2.3 Cyber Governance, Risk Management, and Board Accountability

Cyber governance in insurance requires cybersecurity to be positioned within corporate governance rather than confined to information-technology administration. This distinction is particularly consequential in Nigeria, where insurers hold sensitive identity, financial, health and claims information while depending on increasingly interconnected platforms. Evidence from Nigerian financial institutions indicates that enterprise risk management, board risk committee activism, board independence and the centrality of the chief risk officer are materially associated with cybercrime outcomes, demonstrating that cyber exposure is partly a governance problem requiring direct board engagement (Erin, Kolawole & Noah, 2020).

A mature governance structure establishes clear decision rights, accountability and reporting relationships across the board, executive management, risk functions, internal audit and operational units. Information-security governance research in South Africa similarly stresses that security objectives should be integrated with corporate governance, strategic direction, policies, organisational structures and performance monitoring rather than managed through isolated technical controls (Da Veiga & Eloff, 2007).

Board accountability is especially important where technology constitutes a strategic dependency. Effective board-level IT governance improves the alignment of technology resources with organisational priorities and strengthens oversight of technology-related opportunities and risks. For Nigerian insurers, this implies that directors should interrogate cyber-risk appetite, major security investments, critical third-party dependencies, incident readiness and remediation performance instead of delegating the entire subject to technology specialists (Turel & Bart, 2014).

Cyber governance must also evolve from operational security management toward enterprise-wide digital security governance. A systematic review of information-security governance literature identifies this movement from technically isolated security toward boardroom-level strategic oversight. Consequently, insurer governance should connect cyber metrics with business objectives, regulatory obligations and executive accountability (Schinagl& Shahim, 2020).

Table 1: Illustrative Cyber Governance and Accountability Structure for Nigerian Insurers

Governance level	Core cyber responsibilities	Illustrative maturity evidence
Board of Directors	Approve cyber strategy, appetite and oversight	Regular cyber reporting and challenge
Board Risk Committee	Review exposures, incidents and remediation	Risk indicators tracked against thresholds
Executive Management	Translate strategy into funded controls	Defined ownership and resource allocation
CRO/ERM Function	Integrate cyber risk into enterprise risks	Cyber exposure within ERM registers
CISO/Security Function	Coordinate protection, detection and response	Tested controls and incident capabilities
Internal Audit	Provide independent assurance	Periodic control and governance reviews
Business Units	Own operational cyber exposures	Risk ownership embedded in processes

Within this structure, the CISO or equivalent security leader provides specialist coordination, but accountability cannot rest with one office. Research examining breached organisations shows considerable variation in CISO reporting arrangements and highlights the importance of authority, organisational positioning and post-incident strategic involvement. Nigerian insurers therefore require reporting lines that permit security concerns to reach senior management and the board without distortion or undue delay (Karanja, 2017).

Enterprise risk management provides the integrative mechanism through which cyber risk can be considered alongside underwriting, market, liquidity, operational, compliance and reputational risks. ERM creates value when organisations evaluate risks collectively, allocate risk ownership and align risk-taking with strategic objectives rather than managing exposures independently (Nocco & Stulz, 2006).

This integrated perspective has particular relevance for insurance. Empirical evidence suggests that ERM adoption is associated with higher firm value among insurers, indicating that systematic risk governance can generate benefits extending beyond regulatory conformity. Cybersecurity should therefore be incorporated into risk appetite statements, capital considerations and strategic planning rather than treated as an episodic compliance exercise (Hoyt & Liebenberg, 2011).

Insurance-specific evidence further indicates that ERM can improve risk reduction efficiency and lower volatility by enabling firms to recognise interactions among exposures and prioritise mitigation resources. Applied to cyber risk, boards should demand risk-based investment decisions supported by exposure assessments, control effectiveness indicators and residual-risk reporting (Eckles, Hoyt & Miller, 2014).

International insurance evidence also shows that ERM effectiveness depends on organisational implementation rather than the mere existence of formal frameworks. Findings from China's insurance industry reinforce the relevance of integrated risk structures to firm value and governance quality, offering a useful comparative lens for assessing whether Nigerian insurers have progressed from policy-based compliance toward embedded cyber-risk accountability (Li et al., 2014). This also allows supervisors to distinguish substantive governance capacity from nominal compliance structures in practice.

2.4 Data Protection, Security, and Cyber Resilience

Data protection, information security and cyber resilience are mutually reinforcing components of cyber-risk maturity in insurance. Nigerian insurers process identity records, financial details, claims histories, health information and beneficiary data whose compromise can produce regulatory and reputational consequences. Effective protection therefore requires governance of the full data lifecycle, including collection, classification, storage, access, sharing, retention and secure disposal. Comparative regulatory analysis demonstrates that contemporary data-protection and cybersecurity regimes increasingly converge around risk-based

safeguards, security-by-design, incident reporting, resilience and assurance mechanisms (Mantelero et al., 2020).

Privacy-by-design strengthens this integration by requiring privacy requirements to influence systems before deployment rather than being retrofitted after vulnerabilities emerge. For insurance organisations, this principle is relevant to customer portals, mobile applications, automated underwriting and claims platforms, where excessive collection or poorly configured access can increase exposure. Privacy engineering translates abstract obligations into technical choices such as data minimisation, purpose limitation and controlled disclosure (Spiekermann& Cranor, 2009).

The same logic extends to data-protection-by-design within cybersecurity architecture. Legal privacy principles can be operationalised through technical controls during development, allowing security functions to protect individuals without generating unnecessary privacy risks. Nigerian insurers should consequently incorporate privacy considerations into authentication, monitoring, threat-intelligence and analytics systems (Gkotsopoulou et al., 2019).

Resilience adds a further dimension because protection cannot guarantee that incidents will never occur. Cyber-resilient organisations must anticipate disruption, absorb its effects, restore critical functions and adapt controls after recovery. Metrics spanning informational, cognitive and organisational domains can assist management in determining whether recovery capabilities are measurable rather than merely assumed (Linkov et al., 2013).

Table 2: Illustrative Data Protection and Cyber-Resilience Control Matrix

Control domain	Insurance-sector application	Maturity evidence
Data governance	Classify policyholder and claims data	Current inventory and assigned ownership
Access security	Restrict sensitive and privileged access	MFA, reviews and least privilege
Privacy-by-design	Embed privacy within digital services	Documented privacy impact assessments
Incident management	Detect and contain data compromise	Tested escalation and response plans
Recovery	Restore critical insurance services	Verified backups and recovery exercises
Third-party security	Govern processors and technology vendors	Due diligence and continuing assurance

Cyber resilience is also an organisational capability. Analysis of firms and wider systems shows that resilience requires balancing preventive investment, insurance, response resources and recovery mechanisms, reinforcing the need for Nigerian insurers to integrate security expenditure with operational-risk planning (Hausken, 2020). Cyber insurance may complement this architecture, but risk transfer cannot substitute for substantive cybersecurity controls and institutional preparedness (Markopoulou, 2021).

African evidence further demonstrates why technical safeguards must be reinforced by organisational awareness. Research in Ghana identified limitations in corporate cybersecurity awareness and the integration of legal considerations into information-security policies, underscoring the importance of training, coherent policies and specialist expertise in preventing data loss (Adu & Adjei, 2018). Privacy-by-design scholarship similarly emphasises proactive safeguards in environments processing sensitive information because remedial measures cannot fully reverse privacy harms after disclosure has occurred (Romanou, 2018).

The requested Nigerian engineering study is not cybersecurity or insurance research. Its relevance is

limited to the systems principle that resilient infrastructure benefits from integrated design and continuity-oriented investment. Applied cautiously, this principle supports treating security, redundancy and continuity as interconnected capabilities rather than isolated technical initiatives within insurance operations (Sunday &Omoegun, 2018).

III. NAICOM AND NDPR CYBER RISK BENCHMARKS

Assessing cyber-risk maturity within Nigeria's insurance sector requires a benchmark that integrates sector-specific supervisory expectations with the privacy, security and accountability obligations applicable to organisations processing personal information. NAICOM's supervisory orientation places considerable emphasis on sound corporate governance, effective risk oversight, internal controls, compliance and board accountability. Within listed Nigerian insurance companies, governance attributes have been shown to influence organisational outcomes, reinforcing the importance of treating cyber risk as an enterprise-level exposure requiring board attention rather than as an exclusively technical responsibility delegated to information-technology personnel (Mohammed &Kurawa, 2021).

The Nigeria Data Protection Regulation provides a complementary benchmark because insurers routinely collect and process highly sensitive categories of information, including identification records, financial details, medical information, beneficiary data and claims histories. Regulatory maturity therefore requires more than the existence of privacy policies. It entails demonstrable capability in lawful processing, transparency, accountability, data-subject rights, appropriate security safeguards and responsible management of data processors. A mature insurer should be able to show that these obligations are embedded within operational processes and supported by documented evidence (Udoh, 2021).

Cyber maturity must also be assessed against the risks arising from misuse, unauthorised disclosure and unlawful exploitation of personal data. Nigeria's evolving data-protection environment has historically faced concerns regarding enforcement, institutional capability and the adequacy of protective mechanisms. For insurers, these concerns translate into practical requirements for data classification, access control, secure transmission, encryption, retention management, breach escalation and disciplined handling of policyholder information across its lifecycle (Odusote, 2021).

An effective NAICOM–NDPR benchmark should consequently examine several interconnected capability areas. At governance level, boards should approve cyber-risk policies, define accountability and receive regular reports on material exposures. At enterprise-risk level, cyber threats should appear within formal risk registers, risk appetite statements and key risk indicators. Data-governance maturity should be evidenced through inventories, classification standards and assigned ownership. Technical maturity should include identity management, multifactor authentication, vulnerability remediation, monitoring and secure configuration. Incident-response maturity should be demonstrated through tested escalation arrangements, while operational resilience should include verified backups, recovery procedures and business-continuity exercises.

African regulatory experience further indicates that cross-border privacy governance can become complex where national legal frameworks and enforcement capabilities differ. This is relevant to Nigerian insurers increasingly dependent on multinational cloud providers, reinsurers, payment processors and technology vendors. Mature institutions should therefore maintain traceability of data flows, conduct appropriate due diligence and establish contractual controls over third parties without assuming that outsourcing transfers regulatory accountability (Makulilo, 2015).

Financial-sector cyber supervision should additionally move beyond checklist-based compliance toward risk-sensitive assessment. Quantitative approaches can strengthen maturity evaluation by linking vulnerabilities, operational dependencies and potential financial losses to control priorities. For Nigerian insurers, this implies

developing measurable exposure indicators and scenario-based assessments capable of informing both management decisions and supervisory scrutiny (Bouveret, 2018).

Regulation must also address interconnected risks that may produce consequences beyond an individual institution. Cyber incidents can generate externalities through shared infrastructure, service providers ands financial networks, making minimum standards, information sharing and credible testing important supervisory instruments (Kashyap & Wetherilt, 2019). As digital architectures continue to evolve, benchmark design should equally support standardised terminology, measurable risk categories and adaptive assessment practices. This enables NAICOM and data-protection expectations to be translated into evidence-based maturity indicators that distinguish nominal compliance from institutionalised, continuously improving cyber-risk capability (Radanliev et al., 2020).

IV. CYBER RISK MATURITY IN NIGERIAN INSURANCE

Cyber-risk maturity in Nigerian insurance should be assessed as the degree to which security practices are institutionalised, measurable, risk-driven and capable of sustaining critical services under evolving threats. In the absence of a public maturity survey covering the industry, a defensible assessment is capability-based rather than numerical. A Nigerian-African resilience framework emphasises the existence, effectiveness and efficiency of controls across protection, detection, response and recovery, providing a lens for distinguishing basic compliance from operationalised resilience (Mbanaso, Abrahams &Apene, 2019).

At the governance level, maturity is demonstrated when cyber risk is incorporated into enterprise risk registers, risk appetite, board reporting and investment decisions. Insurers operating with fragmented security ownership or reactive technology controls would occupy lower maturity positions, whereas institutions that align security objectives with business capabilities, allocate accountable ownership and continually optimise controls exhibit stronger capability. Security maturity research shows that organisational context, resources, management structures, talent and technology must be considered together rather than through isolated safeguards (Al-Matari et al., 2021).

Measurement quality is equally important. Assessments based solely on policy existence or self-reported compliance may overstate capability because practitioners can interpret maturity levels inconsistently. Empirical evidence indicates that maturity evaluation requires clearly defined criteria, repeatable evidence and disciplined judgement. For Nigerian insurers, this implies validating stated controls through configuration reviews, testing, audit findings, vulnerability remediation records and management follow-through (Schmitz et al., 2021).

A practical maturity profile should examine the five operational functions of identifying assets and risks, protecting systems, detecting abnormal activity, responding to incidents and recovering services. Assessment tools structured around these functions demonstrate how organisations can convert broad cybersecurity expectations into observable indicators and prioritised improvement actions. Such an approach is useful where firms differ in size, digital dependence and available security resources (Benz & Chatterjee, 2020).

Incident-management capability separates nominal preparedness from operational maturity. Mature insurers require documented escalation routes, post-incident learning, evidence preservation and tested coordination with business-continuity functions. Research on incident-management practice shows that formal procedures are insufficient unless organisations can execute, review and improve them consistently across the incident lifecycle (Tøndel, Line &Jaatun, 2014).

Insurance maturity must also account for the sector's dual position as both a target of cyber events and a potential underwriter of cyber losses. Challenges surrounding data scarcity, accumulation, pricing and changing losses mean that stronger internal cybersecurity should be complemented by disciplined cyber-risk modelling and underwriting expertise

where cyber coverage is offered (Eling & Schnell, 2016).

The supplied Nigerian biomedical study does not examine insurance or cybersecurity and therefore cannot substantiate sector maturity directly. Its automated template-matching approach is relevant only as an illustration of rule-based detection and systematic pattern identification. Applied cautiously, it reinforces the principle that mature digital environments depend on repeatable detection mechanisms, but it should not be treated as empirical evidence about Nigerian insurers' cyber capabilities (Ejofodomi et al., 2014).

V. COMPLIANCE GAPS AND CYBER MATURITY BARRIERS

Compliance gaps within Nigeria's insurance sector should be understood as the distance between regulatory expectations and the extent to which those expectations are embedded in repeatable, measurable, and continuously improved cyber-risk practices. A review-based assessment suggests that the principal challenge is unlikely to be the absence of policy alone, but the uneven translation of governance requirements into operational capability. Earlier analysis of Nigeria's national cybersecurity policy environment similarly identified implementation weaknesses despite comprehensive strategic content, illustrating how sound regulatory design can coexist with institutional gaps in execution, coordination, monitoring, and capacity development (Osho & Onoja, 2015).

One major barrier is the persistence of fragmented information-security management. Cybersecurity can remain divided among information technology, compliance, risk, legal, and audit functions without an integrated operating model linking accountability, control ownership, and escalation. Research on information-security management demonstrates that effective protection requires a holistic combination of policy execution, training, enterprise architecture, infrastructure management, human-resource practices, and business–technology alignment (Soomro, Shah & Ahmed, 2016). For Nigerian insurers, fragmentation can weaken the conversion of NAICOM and data-protection expectations into controls across underwriting, claims, portals, payments, and outsourced services.

Policy existence also does not guarantee behavioural compliance. Organisational security policies can be ambiguous, inconsistently enforced, poorly communicated, or detached from actual work practices, thereby encouraging ceremonial rather than substantive compliance. A broad review of organisational information-security policies shows that policy effectiveness depends on contextual factors including enforcement, employee interpretation, organisational culture, and management support (Cram, Proudfoot & D'Arcy, 2017). This creates a maturity barrier where insurers possess documented procedures but lack evidence that employees and managers apply them consistently.

Human factors further constrain maturity. South African evidence shows that a strong information-security culture depends on management commitment, awareness, training, communication, policy understanding, responsibility, and employee behaviour. Weakness in any of these elements can sustain risky practices even where technical safeguards exist (Nel & Drevin, 2019). For Nigerian insurers, cyber awareness should therefore extend beyond periodic compliance training toward embedded behavioural expectations covering phishing, privileged access, data handling, incident reporting, and third-party interaction.

Moving beyond minimum compliance also requires deliberate cultural change. Practical evidence indicates that cybersecurity champions, coordinated awareness initiatives, visible security leadership, and organisation-wide engagement can help institutions progress from rule-following toward functional cybersecurity cultures (Alshaikh, 2020). Without such mechanisms, compliance may remain reactive, driven primarily by audits, incidents, or regulatory inspections rather than by continuous risk ownership.
Resource constraints are equally material. Cybersecurity functions require expertise spanning governance, cloud security, identity management, incident response, privacy, threat analysis, and

business resilience. International research identifies persistent shortages of skilled personnel and stresses that cybersecurity capability cannot be reduced to a narrow technical specialism (Furnell & Bishop, 2020). Insurers with constrained budgets or weak retention capacity may consequently struggle to sustain specialised functions, test controls rigorously, and remediate vulnerabilities promptly.

Cyber maturity is also shaped by the interaction between technology, organisational conditions, and the external environment. Empirical evidence from Bahrain shows that cybersecurity readiness positively influences security performance and, indirectly, organisational performance, while readiness itself depends on multiple technological and organisational factors (Hasan et al., 2021). This implies that Nigerian insurers cannot close compliance gaps solely through security products; progress requires coordinated governance, resources, processes, skills, and oversight.

Workforce development consequently becomes a strategic capability issue. Although the supplied study concerns distributed supply chains rather than cybersecurity or insurance, its emphasis on competency mapping, continuous learning, leadership readiness, and technology-enabled talent development provides a limited but transferable insight. Applied cautiously, it suggests that insurers should treat cybersecurity skills as an evolving institutional capability requiring structured development rather than episodic recruitment or training (Falemi, Akhigbe & Akin-Oluyomi, 2020).

VI. ADVANCING CYBER MATURITY AND REGULATORY ALIGNMENT

Advancing cyber maturity within Nigeria's insurance sector requires a deliberate shift from minimum regulatory compliance toward an integrated capability model in which governance, technology, people, and resilience are continuously strengthened. The most immediate priority is to translate NAICOM and NDPR obligations into measurable control outcomes, supported by clear ownership, evidence-based assurance, and periodic maturity assessment. Regulatory effectiveness in insurance depends on requirements being sufficiently flexible, proportionate, transparent, and timely to remain relevant as operational technologies and threat conditions evolve (Grima & Marano, 2021).

At the organisational level, insurers should institutionalise cyber governance through board-approved risk appetite, defined executive accountability, funded security programmes, and recurring reporting against key risk and control indicators. A maturity dashboard can help directors distinguish policy existence from actual capability by showing whether governance practices are ad hoc, repeatable, defined, measured, or optimised. Governance-maturity research demonstrates the value of combining multiple assessment dimensions into an executive view that supports prioritisation and sustained oversight rather than episodic compliance activity (De Bruin & Von Solms, 2016).

Risk management should likewise become more dynamic and evidence-led. Nigerian insurers require recurring assessment of information assets, business services, vulnerabilities, threat likelihood, control effectiveness, and potential operational or privacy impacts. Mature assessment should also capture dependencies among cloud platforms, payment channels, outsourced administrators, brokers, reinsurers, and other service providers. A structured risk taxonomy improves the selection of appropriate assessment methods and enables scarce resources to be directed toward exposures with the greatest business significance (Shameli-Sendi et al., 2016).

Operational maturity further depends on strengthening detection and response. Insurers should progressively develop security operations capabilities that integrate logging, behavioural monitoring, threat intelligence, incident triage, escalation, and post-incident learning. Intelligence-driven maturity models show that security operations become more effective when external threat information is systematically integrated with internal telemetry and response processes, enabling organisations to move from reactive detection toward anticipatory and context-aware defence (Schlette, Vielberth&Pernul, 2021).

Incident response should also be connected directly to business decision-making. Mature financial organisations develop situation awareness by combining technical indicators with knowledge of business processes, stakeholders, regulatory obligations, and potential service consequences. Nigerian insurers should therefore conduct scenario exercises covering ransomware, data compromise, cloud outages, privileged-account abuse, and third-party disruption, while ensuring that response teams can rapidly communicate material implications to senior management and regulators (Ahmad et al., 2021).

Regulatory alignment would be strengthened further through common standards, supervisory guidance, and credible assurance mechanisms. Cybersecurity regulation is most effective when policy requirements are reinforced through recognised standards, incident-management structures, verification practices, and coordinated national response arrangements. For NAICOM, this supports a supervisory approach that combines baseline requirements with risk-sensitive examinations, thematic reviews, remediation tracking, and proportionate escalation where material weaknesses persist. This enables supervisory attention to concentrate on institutions whose control weaknesses, outsourcing dependencies, data exposure, or recovery limitations create disproportionate risks to policyholders and wider market confidence over time consistently (Srinivas, Das & Kumar, 2019).

Sector-wide maturity also requires structured collaboration beyond individual insurers. Information sharing among insurers, regulators, technology providers, law-enforcement bodies, and other financial institutions can improve threat visibility and reduce duplicated defensive effort. International financial-sector experience shows that public-private partnerships can strengthen cyber protection when participants establish trusted channels, governance arrangements, and practical mechanisms for exchanging timely threat information. Nigeria could adapt such collaboration to sector-specific incident patterns while preserving confidentiality and regulatory responsibilities (Pomerleau & Lowery, 2020).

Finally, cyber investment should be prioritised according to risk, operational criticality, and measurable performance rather than technology acquisition alone. The supplied Nigerian engineering study does not address cybersecurity, insurance, NAICOM, or the NDPR and therefore cannot substantiate sector-specific cyber claims. Its relevance is limited to the transferable principle that optimisation requires balancing resources, system constraints, reliability objectives, and changing demand. Applied cautiously, this supports a maturity pathway in which Nigerian insurers continuously evaluate control performance, allocate resources to critical exposures, and recalibrate safeguards as regulatory expectations and threat conditions change (Sunday &Omoegun, 2019).

VII. CONCLUSION

This review has critically examined the maturity of cyber risk management within Nigeria's insurance sector by integrating conceptual, regulatory, governance, technological, and organisational perspectives. The study achieved its objectives by clarifying the dimensions of cyber maturity, identifying the distinctive threat exposure of insurance institutions, evaluating the relevance of NAICOM and data-protection requirements, and assessing the institutional conditions that influence the transition from basic compliance to sustainable cyber resilience. The analysis demonstrates that cyber maturity cannot be inferred from the existence of policies, security technologies, or regulatory reporting alone; rather, it depends on the extent to which governance, risk assessment, privacy protection, incident response, recovery, workforce capability, and continuous assurance are embedded across organisational processes.

A central finding is that Nigerian insurers operate within an increasingly complex digital environment in which interconnected platforms, third-party dependencies, sensitive policyholder information, and evolving cyber threats intensify operational and regulatory exposure. Although NAICOM governance

expectations and the NDPR provide important foundations for accountability and data protection, significant maturity barriers may arise from fragmented governance, limited specialist expertise, inconsistent control measurement, weak security cultures, constrained resources, and insufficient integration of cyber risk into enterprise-wide decision-making. The review further establishes that regulatory compliance and cyber resilience are related but fundamentally distinct outcomes.

Accordingly, insurers should adopt structured maturity assessments, strengthen board-level cyber oversight, integrate cyber risk into enterprise risk management, expand continuous monitoring, improve third-party assurance, and institutionalise tested incident-response and recovery capabilities. Regulators should complement prescriptive requirements with risk-based supervision, maturity benchmarking, sector-wide threat intelligence, and proportionate remediation monitoring. Greater investment in cybersecurity skills, privacy-by-design, measurable resilience indicators, and collaborative information sharing is also recommended. Collectively, these measures would enable the sector to progress from reactive and compliance-centred practices toward adaptive, evidence-driven, and continuously improving cyber-risk governance capable of protecting policyholders, sustaining operational continuity, and reinforcing confidence in Nigeria's increasingly digital insurance market.

REFERENCES

[1] Adler, R.M. (2013) 'A dynamic capability maturity model for improving cyber security', in 2013 IEEE International Conference on Technologies for Homeland Security (HST). IEEE, pp. 230–235. DOI: 10.1109/THS.2013.6699005. (Science Publishing Corporation)

[2] Adu, K.K. and Adjei, E. (2018) 'The phenomenon of data loss and cyber security issues in Ghana', Foresight, 20(2), pp. 150–161. DOI: 10.1108/FS-08-2017-0043. (Emerald Publishing)

[3] Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S. and Upton, D. (2018) 'A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate', Journal of Cybersecurity, 4(1), tyy006. DOI: 10.1093/cybsec/tyy006. (OUP Academic)

[4] Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M.T. and Baskerville, R.L. (2021) 'How can organizations develop situation awareness for incident response: A case study of management practice', Computers & Security, 101, 102122. DOI: 10.1016/j.cose.2020.102122. (Monash University)

[5] Alayo, J.G., Mendoza, P.N., Armas-Aguirre, J. and Molina, J.M. (2021) 'Cybersecurity maturity model for providing services in the financial sector in Peru', in 2021 7th Congreso Internacional de Innovación y Tendenciasen Ingeniería (CONIITI). IEEE, pp. 1–4. DOI: 10.1109/CONIITI53815.2021.9619733. (UPC)

[6] Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A. and Janicke, H. (2020) 'A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom', Applied Sciences, 10(10), p. 3660. DOI: 10.3390/app10103660. (ResearchGate)

[7] Al-Matari, O.M.M., Helal, I.M.A., Mazen, S.A. and Elhennawy, S. (2021) 'Adopting security maturity model to the organizations' capability model', Egyptian Informatics Journal, 22(2), pp. 193–199. DOI: 10.1016/j.eij.2020.08.001. (ScienceDirect)

[8] Alshaikh, M. (2020) 'Developing cybersecurity culture to influence employee behavior: A practice perspective', Computers & Security, 98, 102003. DOI: 10.1016/j.cose.2020.102003. (ScienceDirect)

[9] Benz, M. and Chatterjee, D. (2020) 'Calculated risk? A cybersecurity evaluation tool for SMEs', Business Horizons, 63(4), pp. 531–540. DOI: 10.1016/j.bushor.2020.03.010. (ScienceDirect)

[10] Biener, C., Eling, M. and Wirfs, J.H. (2015) 'Insurability of cyber risk: An empirical analysis', The Geneva Papers on Risk and Insurance—Issues and Practice, 40(1), pp. 131–158. DOI: 10.1057/gpp.2014.19. (Springer)

[11] Bohnert, A., Fritzsche, A. and Gregor, S. (2019) 'Digital agendas in the insurance industry: The importance of comprehensive approaches', The Geneva Papers on Risk and Insurance—Issues and Practice, 44(1), pp. 1–19. DOI: 10.1057/s41288-018-0109-0. (Springer)

[12] Bouveret, A. (2018) 'Cyber risk for the financial sector: A framework for quantitative assessment', IMF Working Papers, 2018(143), pp. 1–29. DOI: 10.5089/9781484360750.001.

[13] Cram, W.A., Proudfoot, J.G. and D'Arcy, J. (2017) 'Organizational information security policies: A review and research framework', European Journal of Information Systems, 26(6), pp. 605–641. DOI: 10.1057/s41303-017-0059-9. (Taylor & Francis Online)

[14] Da Veiga, A. and Eloff, J.H.P. (2007) 'An information security governance framework', Information Systems Management, 24(4), pp. 361–372. DOI: 10.1080/10580530701586136. (ACM Digital Library)

[15] De Bruin, R. and Von Solms, S.H. (2016) 'Modelling cyber security governance maturity', in 2015 IEEE International Symposium on Technology and Society (ISTAS). IEEE, Article 7439415. DOI: 10.1109/ISTAS.2015.7439415. (University of Johannesburg)

[16] Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinoudakis, C., Cook, A. and Janicke, H. (2020) 'A NIS Directive compliant cybersecurity maturity assessment framework', in 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, pp. 1641–1646. DOI: 10.1109/COMPSAC48688.2020.00-20. (CONCORDIA)

[17] Dupont, B. (2019) 'The cyber-resilience of financial institutions: Significance and applicability', Journal of Cybersecurity, 5(1), tyz013. DOI: 10.1093/cybsec/tyz013. (OUP Academic)

[18] Eckles, D.L., Hoyt, R.E. and Miller, S.M. (2014) 'The impact of enterprise risk management on the marginal cost of reducing risk: Evidence from the insurance industry', Journal of Banking & Finance, 43, pp. 247–261. DOI: 10.1016/j.jbankfin.2014.02.007. (IDEAS/RePEc)

[19] Ejofodomi, O.A., Gideon, E.N., Oladipo, G.O. and Oshomah, E.R. (2014) 'Automated detection of architectural detection in mammograms using template matching', International Journal of Biomedical Science and Engineering, 2(1), pp. 1–6. DOI: 10.11648/j.ijbse.20140201.11. (Science Publishing Group)

[20] Eling, M. and Lehmann, M. (2018) 'The impact of digitalization on the insurance value chain and the insurability of risks', The Geneva Papers on Risk and Insurance—Issues and Practice, 43(3), pp. 359–396. DOI: 10.1057/s41288-017-0073-0. (EconPapers)

[21] Eling, M. and Schnell, W. (2016) 'What do we know about cyber risk and cyber risk insurance?', The Journal of Risk Finance, 17(5), pp. 474–491. DOI: 10.1108/JRF-09-2016-0122. (IDEAS/RePEc)

[22] Erin, O.A., Kolawole, A.D. and Noah, A.O. (2020) 'Risk governance and cybercrime: The hierarchical regression approach', Future Business Journal, 6, Article 12. DOI: 10.1186/s43093-020-00020-1. (Springer)

[23] Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2020) 'A conceptual supply chain talent development model for capability building across distributed operations', International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), pp. 439–456. DOI: 10.54660/.IJMRGE.2020.1.5.439-456. (All Multidisciplinary Journal)

[24] Furnell, S. and Bishop, M. (2020) 'Addressing cyber security skills: The spectrum, not the silo', Computer Fraud & Security, 2020(2), pp. 6–11. DOI: 10.1016/S1361-3723(20)30017-8. (ScienceDirect)

[25] Garba, A.A., Bade, A.M., Yahuza, M. and Nuhu, Y. (2020) 'Cybersecurity capability maturity models review and application domain', International Journal of Engineering & Technology, 9(3), pp. 779–784. DOI: 10.14419/ijet.v9i3.30719. (Science Publishing Corporation)

[26] Gkotsopoulou, O., Charalambous, E., Limniotis, K., Quinn, P., Kavallieros, D., Sargsyan, G., Shiaeles, S. and Kolokotronis, N. (2019) 'Data protection by design for cybersecurity systems in a smart home environment', in Proceedings of the 2019 IEEE Conference on Network Softwarization (NetSoft). IEEE, pp. 101–109. DOI: 10.1109/NETSOFT.2019.8806694. (University of Portsmouth)

[27] Gonzalez-Granadillo, G., Menesidou, S.A., Papamartzivanos, D., Romeu, R., Navarro-Llobet, D., Okoh, C., Nifakos, S., Xenakis, C. and Panaousis, E. (2021) 'Automated cyber and privacy risk management toolkit', Sensors, 21(16), p. 5493. DOI: 10.3390/s21165493. (MDPI)

[28] Gordon, L.A., Loeb, M.P. and Sohail, T. (2003) 'A framework for using insurance for cyber-risk management', Communications of the ACM, 46(3), pp. 81–85. DOI: 10.1145/636772.636774. (ACM Digital Library)

[29] Grima, S. and Marano, P. (2021) 'Designing a model for testing the effectiveness of a regulation: The case of DORA for insurance undertakings', Risks, 9(11), Article 206, pp. 1–12. DOI: 10.3390/risks9110206. (University of Latvia)

[30] Haislip, J., Lim, J.H. and Pinsker, R. (2021) 'The impact of executives' IT expertise on reported data security breaches', Information Systems Research, 32(2), pp. 318–334. DOI: 10.1287/isre.2020.0986. (PubsOnline)

[31] Hasan, S., Ali, M., Kurnia, S. and Thurasamy, R. (2021) 'Evaluating the cyber security readiness of organizations and its influence on performance', Journal of Information Security and Applications, 58, 102726. DOI: 10.1016/j.jisa.2020.102726. (ScienceDirect)

[32] Hausken, K. (2020) 'Cyber resilience in firms, organizations and societies', Internet of Things, 11, 100204. DOI: 10.1016/j.iot.2020.100204. (ScienceDirect)

[33] Hoyt, R.E. and Liebenberg, A.P. (2011) 'The value of enterprise risk management', Journal of Risk and Insurance, 78(4), pp. 795–822. DOI: 10.1111/j.1539-6975.2011.01413.x. (Wiley Online Library)

[34] Iorliam, A. (2019) Cybersecurity in Nigeria: A Case Study of Surveillance and Prevention of Digital Crime. Cham: Springer. DOI: 10.1007/978-3-030-15210-9. (Springer)

[35] Kamiya, S., Kang, J.K., Kim, J., Milidonis, A. and Stulz, R.M. (2021) 'Risk management, firm reputation, and the impact of successful cyberattacks on target firms', Journal of Financial Economics, 139(3), pp. 719–749. DOI: 10.1016/j.jfineco.2019.05.019. (PolyU Scholars Hub)

[36] Karanja, E. (2017) 'The role of the chief information security officer in the management of IT security', Information and Computer Security, 25(3), pp. 300–329. DOI: 10.1108/ICS-02-2016-0013. (Emerald Publishing)

[37] Kashyap, A.K. and Wetherilt, A. (2019) 'Some principles for regulating cyber risk', AEA Papers and Proceedings, 109, pp. 482–487. DOI: 10.1257/pandp.20191058.

[38] Li, Q., Wu, Y., Ojiako, U., Marshall, A. and Chipulu, M. (2014) 'Enterprise risk management and firm value within China's insurance industry', Acta Commercii, 14(1), Article 198, pp. 1–10. DOI: 10.4102/ac.v14i1.198. (Acta Commercii)

[39] Linkov, I., Eisenberg, D.A., Plourde, K., Seager, T.P., Allen, J. and Kott, A. (2013) 'Resilience metrics for cyber systems', Environment Systems and Decisions, 33(4), pp. 471–476. DOI: 10.1007/s10669-013-9485-y. (ResearchGate)

[40] Makulilo, A.B. (2015) 'Myth and reality of harmonisation of data privacy policies in Africa', Computer Law & Security Review, 31(1), pp. 78–89. DOI: 10.1016/j.clsr.2014.11.005.

[41] Mantelero, A., Vaciago, G., Esposito, M.S. and Monte, N. (2020) 'The common EU approach to personal data and cybersecurity regulation', International Journal of Law and Information Technology, 28(4), pp. 297–328. DOI: 10.1093/ijlit/eaaa021. (OUP Academic)

[42] Markopoulou, D. (2021) 'Cyber-insurance in EU policy-making: Regulatory options, the market's challenges and the US example', Computer Law & Security Review, 43, 105627. DOI: 10.1016/j.clsr.2021.105627. (Vrije Universiteit Brussel)

[43] Marotta, A., Martinelli, F., Nanni, S., Orlando, A. and Yautsiukhin, A. (2017) 'Cyber-insurance survey', Computer Science Review, 24, pp. 35–61. DOI: 10.1016/j.cosrev.2017.01.001. (ScienceDirect)

[44] Mbanaso, U.M., Abrahams, L. and Apene, O.Z. (2019) 'Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework', The African Journal of Information and Communication, 23, pp. 1–26. DOI: 10.23962/10539/27535. (SciELO)

[45] Miron, W. and Muita, K. (2014) 'Cybersecurity capability maturity models for providers of critical infrastructure', Technology Innovation Management Review, 4(10), pp. 33–39. DOI: 10.22215/timreview/837. (TIM Review)

[46] Mohammed, S. and Kurawa, J.M. (2021) 'Board attributes and value of listed insurance companies in Nigeria: The mediating effect of earnings quality', International Journal of Management Science and Business Administration, 8(1), pp. 7–23. DOI: 10.18775/ijmsba.1849-5664-5419.2014.81.1001.

[47] Moodley, A.J. (2019) 'Digital transformation in South Africa's short-term insurance sector: Traditional insurers' responses to the Internet of Things (IoT) and Insurtech', The African Journal of Information and Communication, 24, pp. 1–16. DOI: 10.23962/10539/28657. (AJIC)

[48] Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukhan, S.K. (2013) 'Cyber-risk decision models: To insure IT or not?', Decision Support Systems, 56, pp. 11–26. DOI: 10.1016/j.dss.2013.04.004. (ScienceDirect)

[49] Nel, F. and Drevin, L. (2019) 'Key elements of an information security culture in organisations', Information & Computer Security, 27(2), pp. 146–164. DOI: 10.1108/ICS-12-2016-0095. (ScienceDirect)

[50] Nocco, B.W. and Stulz, R.M. (2006) 'Enterprise risk management: Theory and practice', Journal of Applied Corporate Finance, 18(4), pp. 8–20. DOI: 10.1111/j.1745-6622.2006.00106.x. (Wiley Online Library)

[51] Odusote, A. (2021) 'Data misuse, data theft and data protection in Nigeria: A call for a more robust and more effective legislation', Beijing Law Review, 12(4), pp. 1284–1298. DOI: 10.4236/blr.2021.124066.

[52] Omotubora, A. (2021) 'How (not) to regulate data processing: Assessing Nigeria's Data Protection Regulation 2019 (NDPR)', Global Privacy Law Review, 2(3), pp. 186–199. DOI: 10.54648/GPLR2021024. (ResearchGate)

[53] Osho, O. and Onoja, A.D. (2015) 'National cyber security policy and strategy of Nigeria: A qualitative analysis', International Journal of Cyber Criminology, 9(1), pp. 120–143. DOI: 10.5281/zenodo.22390. (Zenodo)

[54] Pieterse, H. (2021) 'The cyber threat landscape in South Africa: A 10-year review', The African Journal of Information and Communication, 28, pp. 1–21. DOI: 10.23962/10539/32213. (AJIC)

[55] Pomerleau, P.-L. and Lowery, D.L. (2020) Countering Cyber Threats to Financial Institutions: A Private and Public Partnership Approach to Critical Infrastructure Protection. Cham: Palgrave Macmillan. DOI: 10.1007/978-3-030-54054-8. (Springer)

[56] Radanliev, P., De Roure, D., Nurse, J.R.C., Montalvo, R.M., Cannady, S. and Santos, O. (2020) 'Future developments in standardisation of cyber risk in the Internet of Things (IoT)', SN Applied Sciences, 2, Article 169. DOI: 10.1007/s42452-019-1931-0.

[57] Rea-Guaman, A.M., San Feliu, T., Calvo-Manzano, J.A. and Sanchez-Garcia, I.D. (2017) 'Comparative study of cybersecurity capability maturity models', in Mas, A., Mesquida, A., O'Connor, R.V., Rout, T. and Dorling, A. (eds.) Software Process Improvement and Capability Determination. Communications in Computer and Information Science, Vol. 770. Cham: Springer, pp. 100–113. DOI: 10.1007/978-3-319-67383-7_8. (OUCI)

[58] Romanosky, S., Ablon, L., Kuehn, A. and Jones, T. (2019) 'Content analysis of cyber insurance policies: How do carriers price cyber risk?', Journal of Cybersecurity, 5(1), tyz002. DOI: 10.1093/cybsec/tyz002. (OUP Academic)

[59] Romanou, A. (2018) 'The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise', Computer Law & Security Review, 34(1), pp. 99–110. DOI: 10.1016/j.clsr.2017.05.021. (ScienceDirect)

[60] Schinagl, S. and Shahim, A. (2020) 'What do we know about information security governance? "From the basement to the boardroom": Towards digital security governance', Information and Computer Security, 28(2), pp. 261–292. DOI: 10.1108/ICS-02-2019-0033. (Emerald Publishing)

[61] Schlette, D., Vielberth, M. and Pernul, G. (2021) 'CTI-SOC2M2 – The quest for mature, intelligence-driven security operations and incident response capabilities', Computers & Security, 111, 102482. DOI: 10.1016/j.cose.2021.102482. (University of Regensburg)

[62] Schmitz, C., Schmid, M., Harborth, D. and Pape, S. (2021) 'Maturity level assessments of information security controls: An empirical analysis of practitioners' assessment capabilities', Computers & Security, 108, 102306. DOI: 10.1016/j.cose.2021.102306. (ACM Digital Library)

[63] Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. (2016) 'Taxonomy of information security risk assessment (ISRA)', Computers & Security, 57, pp. 14–30. DOI: 10.1016/j.cose.2015.11.001. (DBLP)

[64] Shittu, H., Opara, I.S., Elumilade, R.A. and Adeniji, I.O. (2019) 'Hydrogen as a secondary energy carrier: Modeling its integration in national grids', Iconic Research and Engineering Journals, 3(1), pp. 628–643. DOI: 10.64388/IREV3I1-1713909. (IRE Journals)

[65] Shittu, H.A., Shittu, M.A., Adeleke, O.J. and Adedokun, O.J. (2021) 'Blockchain-based energy trading models for peer-to-peer renewable microgrids', International Journal of Research in Electrical and Electronics Engineering, 4(3), pp. 1–19. DOI: 10.34218/IJREEE_04_03_001. (IAEME Publication)

[66] Shittu, M.A., Adeniji, I.O., Shittu, H. and Opara, I.S. (2020) 'Grounding system design optimization for medium-voltage distribution networks in emerging power markets', IRE Journal, 3, pp. 11–19. DOI: 10.64388/IREV3I11-1714040.

[67] Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016) 'Information security management needs more holistic approach: A literature review', International Journal of Information Management, 36(2), pp. 215–225. DOI: 10.1016/j.ijinfomgt.2015.11.009. (ScienceDirect)

[68] Spiekermann, S. and Cranor, L.F. (2009) 'Engineering privacy', IEEE Transactions on Software Engineering, 35(1), pp. 67–82. DOI: 10.1109/TSE.2008.88. (ACM Digital Library)

[69] Srinivas, J., Das, A.K. and Kumar, N. (2019) 'Government regulations in cyber security: Framework, standards and recommendations', Future Generation Computer Systems, 92, pp. 178–188. DOI: 10.1016/j.future.2018.09.063. (Publications Repository)

[70] Stoeckli, E., Dremel, C. and Uebernickel, F. (2018) 'Exploring characteristics and transformational capabilities of InsurTech innovations to understand insurance value creation in a digital world', Electronic Markets, 28(3), pp. 287–305. DOI: 10.1007/s12525-018-0304-7. (Springer)

[71] Sunday, E.A. and Omoegun, G.O. (2018) 'Integrating solar power solutions in small-scale manufacturing industries in Nigeria', International Journal of Scientific Research in Science, Engineering and Technology, 4(8), pp. 832–853. DOI: 10.32628/IJSRSET23102175. (IJRSET)

[72] Sunday, E.A. and Omoegun, G.O. (2019) 'Optimizing electrical load distribution for hybrid solar installations in developing economies', International Journal of Scientific

Research in Mechanical and Materials Engineering, 3(6), pp. 27–47.

[73] Sunday, E.A., Omoegun, G.O., Essien, M.A. and Oluokun, O.A. (2019) 'Thermodynamic efficiency and control strategies in residential air conditioning systems', International Journal of Scientific Research in Civil Engineering, 3(3), pp. 52–76. DOI: 10.32628/IJSRCE19339. (IJRCE)

[74] Sutherland, E. (2017) 'Governance of cybersecurity – the case of South Africa', The African Journal of Information and Communication, 20, pp. 83–112. DOI: 10.23962/10539/23574. (SciELO)

[75] Tikkinen-Piri, C., Rohunen, A. and Markkula, J. (2018) 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies', Computer Law & Security Review, 34(1), pp. 134–153. DOI: 10.1016/j.clsr.2017.05.015. (ScienceDirect)

[76] Tøndel, I.A., Line, M.B. and Jaatun, M.G. (2014) 'Information security incident management: Current practice as reported in the literature', Computers & Security, 45, pp. 42–57. DOI: 10.1016/j.cose.2014.05.003. (ScienceDirect)

[77] Turel, O. and Bart, C. (2014) 'Board-level IT governance and organizational performance', European Journal of Information Systems, 23(2), pp. 223–239. DOI: 10.1057/ejis.2012.61. (Taylor & Francis Online)

[78] Udoh, V. (2021) 'Data protection in Nigeria: A review of the Nigerian Data Protection Regulation 2019', SSRN Electronic Journal. DOI: 10.2139/ssrn.3766819.

[79] Varga, S., Brynielsson, J. and Franke, U. (2021) 'Cyber-threat perception and risk management in the Swedish financial sector', Computers & Security, 105, 102239. DOI: 10.1016/j.cose.2021.102239. (ScienceDirect)

[80] von Solms, S.H.B. (2015) 'A maturity model for part of the African Union Convention on Cyber Security', in 2015 Science and Information Conference (SAI). IEEE, pp. 1316–1320. DOI: 10.1109/SAI.2015.7237313. (IEEE Xplore)

[81] Warikandwa, T.V. (2021) 'Personal data security in South Africa's financial services market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation compared', Potchefstroom Electronic Law Journal, 24, pp. 1–32. DOI: 10.17159/1727-3781/2021/v24i0a10727. (Per Journal)

[82] Woods, D., Agrafiotis, I., Nurse, J.R.C. and Creese, S. (2017) 'Mapping the coverage of security controls in cyber insurance proposal forms', Journal of Internet Services and Applications, 8, Article 8, pp. 1–13. DOI: 10.1186/s13174-017-0059-y. (Springer)