

How Secure Are We? A Critical Assessment of the Global Cybersecurity Posture in an Era of Artificial Intelligence, Cloud Dependence and Interconnected Critical Infrastructure

¹*Dimie Nwankwe, ²Boye Azibolelia Frederick

¹Strategic Procurement Department, Oando Energy Resources Nigeria Limited, Port Harcourt, Nigeria

²Faculty of Computing, Department of Computer Science and Informatics, Otuoke, Bayelsa State, Nigeria

*Corresponding Author's E-mail: dimie.nwankwe@gmail.com

²Co-Author's E-mail: boyeaf@fuotuokey.edu.ng

Abstract - Despite record global spending on cybersecurity, the question of how secure modern societies actually have remained unsettled. This paper answers that question through an integrative review of peer-reviewed literature, international standards and the most recent large-scale empirical datasets on breaches, incidents and workforce capacity published between 2024 and 2026. The evidence points to a security paradox. Defensive capability has improved measurably: organisations now detect a larger share of intrusions internally, extensive use of security automation is associated with substantially lower breach costs, and post-quantum cryptographic standards have been finalised. Yet aggregate exposure is rising faster than defence. The global average cost of a data breach reached a record USD 4.99 million in 2026; vulnerability exploitation overtook stolen credentials as the leading initial access vector; ransomware featured in 48% of analysed breaches; third-party involvement rose to 48% of breaches; and the human element remained present in roughly six in ten. Artificial intelligence has moved from a theoretical amplifier to an operational one, with the first publicly documented AI-orchestrated espionage campaign disrupted in 2025. Workforce data show that skills, rather than headcount alone, are now the binding constraint. For Africa and Nigeria, the gap is sharper still: cybercrime accounts for more than 30% of reported crime in West and East Africa, and Nigeria remains in Tier 3 of the ITU Global Cybersecurity Index. The paper argues that security should be understood not as a state but as a dynamic, socio-technical capability whose adequacy is relative to adversary speed, systemic interdependence and institutional capacity. It proposes a five-dimension assessment lens (exposure, detection, resilience, governance and capacity) and offers recommendations for organisations, governments and researchers, with specific

attention to the Nigerian context. The answer to the title question is therefore conditional: we are more capable than ever, but less secure than we need to be.

Keywords: Cybersecurity; cyber resilience; ransomware; supply chain risk; artificial intelligence; post-quantum cryptography; zero trust; Nigeria; Africa; security economics.

I. Introduction

Digital systems now carry the functions on which modern life depends: payments, power, fuel, healthcare, logistics, communication and government. Each wave of digitalisation, from enterprise networks to cloud computing, mobile money, the Internet of Things (IoT) and generative artificial intelligence (AI), has expanded what organisations can do and, at the same time, what adversaries can attack. Cybersecurity, the discipline concerned with protecting the confidentiality, integrity and availability of these systems, has consequently moved from a technical specialism to a matter of corporate governance, economic stability and national security.

The scale of the problem is no longer in dispute. The 2026 edition of the Verizon Data Breach Investigations Report (DBIR), the longest-running multi-source breach dataset, analysed more than 22,000 confirmed breaches across 145 countries, nearly double the prior year's count (Verizon, 2026). IBM and the Ponemon Institute report that the global average cost of a data breach reached a record USD 4.99 million in 2026, a 12% increase on the previous year (IBM, 2026a). The World Economic Forum's Global Cybersecurity Outlook 2026 found that 94% of surveyed leaders regard AI as the most significant driver of change in cybersecurity, and that cyber-enabled fraud has overtaken ransomware as the leading concern of chief executives (World Economic Forum [WEF], 2026).

These figures sit alongside genuine progress. Detection has improved for many organisations; security automation is associated with markedly lower breach costs; national frameworks such as the NIST Cybersecurity Framework 2.0 (National Institute of Standards and Technology [NIST], 2024a) have broadened their scope to governance; and the first post-quantum cryptographic standards were finalised in August 2024 (NIST, 2024b). The co-existence of rising capability and rising loss is the puzzle this paper addresses.

Public and professional discussion of cybersecurity tends to oscillate between two unhelpful positions. The first treats each major incident as proof that “nothing works”, which encourages fatalism and under-investment in basic controls. The second treats compliance certificates, tool deployments or maturity scores as proof of security, which encourages complacency. Neither position answers the question that boards, regulators and citizens actually ask: how secure are we, and is that secure enough? Three features of the current environment make the question harder to answer. First, security is relative: an organisation’s posture is only meaningful against the speed and capability of the adversaries targeting it, and that speed has increased sharply. Mandiant reports that the median time between initial access and hand-off to a second criminal group fell from more than eight hours in 2022 to 22 seconds in 2025 (Mandiant, 2026). Second, risk is increasingly systemic: an organisation can be compromised, or disabled, through suppliers, software dependencies and service providers it does not control, as the July 2024 CrowdStrike outage showed when a faulty update crashed an estimated 8.5 million Windows devices (Microsoft, 2024). Third, capacity is uneven: the skills, institutions and funding needed to defend are concentrated in a small number of economies and large firms, while the attack surface is global. In sub-Saharan Africa, 70% of surveyed chief executives reported lacking the skills to achieve their cybersecurity goals (WEF, 2026). The problem, therefore, is not a shortage of data about cyber threats but a shortage of integrated, critical assessment that converts that data into a defensible answer about the actual state of security, globally and in developing digital economies such as Nigeria.

1.1 Research questions

The paper is organised around four questions:

- i. **RQ1.** What are the dominant threat vectors and adversary behaviours shaping the global cyber risk landscape in 2024 to 2026?
- ii. **RQ2.** What do the best available empirical indicators reveal about the effectiveness of current defences?

- iii. **RQ3.** How are emerging technologies, particularly AI, cloud concentration and quantum computing, altering the balance between attack and defense?
- iv. **RQ4.** What is the specific security position of Africa and Nigeria, and what interventions are most likely to improve it?

1.2 Objectives

Corresponding to these questions, the paper aims to: (a) synthesise current evidence on threat vectors, incident patterns and costs; (b) critically evaluate indicators commonly used to judge security posture; (c) analyse how emerging technologies shift risk; (d) situate the Nigerian and wider African experience within the global picture; and (e) propose an assessment lens and actionable recommendations for practitioners, policymakers and researchers.

1.3 Scope and significance

The review focuses on organisational and national cybersecurity, drawing principally on evidence published between January 2024 and September 2026, supported by foundational literature in security engineering and security economics. Individual consumer security, military cyber operations doctrine and detailed cryptanalysis are discussed only where they bear directly on organisational and national posture. The paper’s significance is threefold. It updates the evidence base with the 2026 editions of the major industry datasets; it offers an explicit, multi-dimensional answer to the question of security adequacy rather than a list of threats; and it gives sustained attention to a West African context that remains under-represented in the international literature.

1.4 Structure of paper

Section 2 sets out the conceptual and theoretical framework. Section 3 describes the review methodology. Section 4 analyses the global threat landscape, and Section 5 examines landmark incidents and their lessons. Section 6 evaluates empirical indicators of security performance. Section 7 discusses emerging frontiers in AI, cloud, operational technology and quantum computing. Section 8 focuses on Africa and Nigeria. Section 9 synthesises the findings into a discussion of the security paradox, and Section 10 presents the contribution to knowledge, recommendations and conclusion.

II. Conceptual and Theoretical Framework

2.1 What does “secure” mean?

Classical definitions frame information security around three properties: confidentiality (information is disclosed only to authorised parties), integrity (information and systems are not altered without authorisation) and availability (systems and data are accessible when needed). Saltzer and Schroeder (1975) translated these goals into enduring design principles, including economy of mechanism, fail-safe defaults, complete mediation, least privilege and psychological acceptability. Half a century later, these principles still describe most of what goes wrong: excessive privilege, unmediated trust between components, insecure defaults and controls that users find too burdensome to follow.

A purely property-based definition, however, cannot answer the question of how secure a system is. Security is not binary. Every real system is vulnerable to some adversary given sufficient resources and time. Anderson (2020) therefore treats security engineering as the discipline of building systems that remain dependable in the face of malice, error or mischance, and that do so at a cost proportionate to the value protected. On this view, “secure” is always shorthand for “secure enough, against a specified adversary, for a specified purpose, over a specified period”. This paper adopts that relative conception throughout: the adequacy of security is judged against threat capability, the consequences of failure and the resources available to defenders.

2.2 Security as an Economic Problem

A second strand of theory explains why systems are often less secure than their owners could afford to make. Anderson (2001) argued that many security failures are better explained by misaligned incentives than by technical shortcomings: the best party to prevent harm frequently does not bear its cost. Anderson and Moore (2006) extended this analysis to show how network externalities, information asymmetries and liability gaps lead to systematic under-investment. Software vendors race to market and ship flaws because customers cannot easily evaluate security before purchase; organisations under-report breaches because disclosure is costly to them while the benefits of shared information accrue to others. Gordon and Loeb (2002) formalised the investment decision, showing that for broad classes of breach probability functions the optimal investment in protecting a given information set does not exceed approximately 37% (1/e) of the expected loss. The model’s practical lesson is not the exact fraction but the principle that security spending should be calibrated to the value at risk and the marginal reduction in vulnerability it

buys. Moore, Clayton and Anderson (2009) applied similar reasoning to online crime, describing an ecosystem in which specialised criminal services such as malware writing, access brokering and money laundering reduce the skill required to attack. The 2025 data showing a 22-second median hand-off between initial access brokers and follow-on groups (Mandiant, 2026) is a striking contemporary confirmation of that specialisation thesis.

2.3 The Socio-Technical View

The third strand treats security as a property of socio-technical systems rather than technology alone. Adams and Sasse (1999) showed that users who circumvent password policies are typically responding rationally to poorly designed controls rather than acting carelessly. Herley (2009) went further, arguing that much security advice is rationally rejected because its aggregate cost in user time exceeds the losses it prevents. Bada, Sasse and Nurse (2015) found that awareness campaigns frequently fail to change behaviour because they emphasise fear and compliance rather than enabling practical action. The empirical persistence of the human element in breaches, present in about 60% of breaches in the 2025 DBIR and 62% in the 2026 edition (Verizon, 2025, 2026), should therefore be read carefully. It does not simply mean that people are the “weakest link”. It means that system designs continue to place security-critical decisions on people without giving them the context, tools or time to make those decisions well.

2.4 Systemic Risk and Tight Coupling

Perrow’s (1999) theory of normal accidents holds that in systems that are both interactively complex and tightly coupled, serious failures are inevitable rather than exceptional. Contemporary digital infrastructure displays both features. Cloud platforms, identity providers, endpoint security agents, software libraries and managed service providers are shared across thousands of organisations, so a single fault or compromise propagates rapidly. This lens explains why some of the most disruptive recent events, such as the CrowdStrike update failure, were not attacks at all, and why supply chain compromises such as SolarWinds and MOVEit had consequences far beyond their initial targets.

2.5 The Offence-Defense Balance

A recurrent claim in policy debates is that cyberspace inherently favours the attacker. Slayton (2017) challenged that assumption, arguing that the balance depends not on technology as such but on the relative skill, organisation and cost of the actors involved. An attacker needs to find only one

exploitable weakness, but a capable defender with good visibility can force the attacker to succeed repeatedly across a long intrusion chain. This framing is essential for assessing AI, which lowers costs on both sides. Whether it favours attack or defence is an empirical and organisational question rather than a technological given.

2.6 Defensive Frameworks

Several frameworks structure contemporary defense. Defense-in-depth layers independent controls so that a single failure is not catastrophic. The intrusion kills chain model (Hutchins, Cloppert & Amin, 2011) decomposes attacks into stages, from reconnaissance to actions on objectives, so that defenders can detect and disrupt adversaries at multiple points. MITRE ATT&CK (Strom et al., 2020) catalogues observed adversary tactics and techniques, providing a common language for detection engineering and threat intelligence. Zero trust architecture (Rose et al., 2020) abandons the notion of a trusted internal network, requiring every access request to be authenticated, authorised and continuously evaluated. Finally, the NIST Cybersecurity Framework 2.0 (NIST, 2024a) organises programmes around six functions (Govern, Identify, Protect, Detect, Respond and Recover), adding governance as an explicit function and extending the framework’s applicability beyond critical infrastructure to organisations of all sizes.

2.7 Analytical Lens Adopted in this Paper

Drawing these strands together, this paper assesses “how secure we are” across five dimensions. Each dimension is relative: it is judged against adversary capability and the consequences of failure, consistent with Section 2.1.

Table 1: Five-dimension assessment lens

Dimension	Guiding question	Example indicators used in this paper	Theoretical anchor
Exposure	How large and how accessible is the attack surface?	Initial access vectors, unpatched exploited vulnerabilities, third-party involvement	Saltzer & Schroeder (1975); Anderson (2020)
Detection	How quickly and reliably are intrusions found?	Median dwell time, share of internally detected incidents, breach lifecycle	Hutchins et al. (2011); Strom et al. (2020)
Resilience	How well do	Breach cost,	Perrow (1999);

Dimension	Guiding question	Example indicators used in this paper	Theoretical anchor
	organisations absorb and recover from incidents?	ransomware outcomes, outage impact	NIST (2024a)
Governance	Are incentives, accountability and regulation aligned with risk?	Board oversight, AI governance, regulatory regimes	Anderson & Moore (2006); Gordon & Loeb (2002)
Capacity	Do people and institutions have the skills and resources to defend?	Skills gaps, enforcement capacity, national index tiers	Slayton (2017); Kshetri (2019)

III. Methodology

3.1 Research design

The study adopts an integrative review design. Integrative reviews synthesise heterogeneous sources, including empirical studies, theoretical work and authoritative grey literature, in order to generate new frameworks or perspectives on a topic (Torraco, 2005). Snyder (2019) distinguishes this approach from systematic reviews, which answer narrow questions from homogeneous studies, and recommends it where a field is evolving rapidly and the most current evidence is produced outside academic journals. Both conditions apply to cybersecurity, where the largest incident datasets are compiled by incident response firms, insurers, international organisations and government agencies, and where the threat landscape changes faster than the typical peer-review cycle.

3.2 Sources and Search Strategy

Three categories of source were consulted:

- Peer-reviewed and foundational scholarly literature**, retrieved from IEEE Xplore, the ACM Digital Library, ScienceDirect, Taylor & Francis Online and arXiv, using combinations of the terms “cybersecurity”, “security economics”, “ransomware”, “supply chain attack”, “zero trust”, “post-quantum cryptography”, “large language model security”, “prompt injection” and “cybercrime Africa”.
- Recurring empirical datasets**, selected because they are large, methodologically documented and published annually, allowing comparison over time: the Verizon DBIR (2025 and 2026 editions), the IBM Cost of a Data Breach Report (2025 and 2026), Mandiant M-Trends

(2025 and 2026), the ISC2 Cybersecurity Workforce Study (2024 and 2025), the World Economic Forum Global Cybersecurity Outlook 2026, the ITU Global Cybersecurity Index 2024 and the INTERPOL Africa Cyberthreat Assessment Report 2025.

- iii. **Primary official and legal documents**, including NIST standards and frameworks, regulatory filings, vendor incident statements and Nigerian legislation.

3.3 Inclusion and Exclusion Criteria

Sources were included if they (a) addressed organisational or national cybersecurity posture, threats or governance; (b) were published by a peer-reviewed venue, a standards body, a government or intergovernmental agency, or an organisation that publishes its dataset size and collection method; and (c) could be traced to a stable, publicly accessible record. Empirical figures were restricted, where possible, to publications from January 2024 to September 2026 to reflect the current landscape; foundational theoretical works were included regardless of date. Vendor marketing material without disclosed methodology, unsourced statistics and estimates that could not be traced to an originating study were excluded. Where figures were obtained from secondary reporting, they were cross-checked against the originating organisation's own publication or press release.

3.4 Analytical procedure

Evidence was extracted into a matrix organised by the five dimensions defined in Section 2.7 (exposure, detection, resilience, governance and capacity). Within each dimension, findings were compared across sources and over time, and convergent findings were distinguished from divergent ones. Incident case studies (Section 5) were selected purposively to represent distinct failure modes rather than to be statistically representative. The synthesis in Section 9 then evaluates each dimension qualitatively as improving, stable or deteriorating relative to threat capability.

3.5 Evaluating the Quality of Evidence

No single data source offers an unbiased view of cyber risk. Table 2 summarises the main source types and their known limitations, which inform how findings are interpreted throughout the paper.

Table 2: Evidence sources, strengths and limitations

Source type	Examples	Main strengths	Main limitations
Multi-contributor	Verizon DBIR	Very large samples;	Contributor mix changes

Source type	Examples	Main strengths	Main limitations
breach datasets		consistent taxonomy (VERIS); long time series	between years; skewed toward reported and investigated incidents
Cost surveys	IBM / Ponemon Cost of a Data Breach	Structured cost model; trend data since 2005	Sample of breached organisations only; costs partly estimated by respondents
Incident response casebooks	Mandiant M-Trends	Deep forensic detail; adversary-level insight	Biased toward large, high-severity investigations
Workforce and leadership surveys	ISC2; WEF Global Cybersecurity Outlook	Global reach; captures perceptions and capacity	Self-reported; non-probability samples
National indices and law enforcement reports	ITU GCI; INTERPOL	Cross-country comparability; official data	Measure commitments and reported crime, not outcomes; under-reporting in many jurisdictions

3.6 Limitations

Three limitations should be noted. First, as a review, the study does not generate new primary data; its contribution lies in synthesis and interpretation. Second, the empirical datasets differ in definitions, sampling frames and reporting periods (for example, the 2026 DBIR covers incidents from November 2024 to October 2025, while the 2026 IBM study covers breaches from March 2025 to February 2026), so figures are compared directionally rather than combined statistically. Third, systematic under-reporting means that published data almost certainly understates the true incidence of cybercrime, particularly in developing economies, a point developed in Section 8.

IV. The Global Threat Landscape

This section addresses RQ1. The evidence shows four structural shifts between 2024 and 2026: attackers increasingly enter through software flaws rather than stolen passwords; ransomware has become more common but less lucrative per victim; third parties have become a primary path into organisations; and social engineering has moved from email toward voice, mobile and AI-assisted channels.

4.1 From stolen credentials to exploited systems

For much of the past decade, the use of stolen credentials was the most common way attackers gained initial access. That has changed. The 2025 DBIR reported that exploitation of vulnerabilities grew by 34% and accounted for 20% of breaches (Verizon, 2025). In the 2026 edition, vulnerability exploitation became the leading initial access vector, at 31% of breaches, overtaking stolen credentials for the first time (Verizon, 2026). Mandiant's incident response data point the same way: exploits were the most common initial infection vector for the sixth consecutive year, with highly interactive, voice-based social engineering rising to second place (Mandiant, 2026).

The shift reflects both supply and demand. On the supply side, the volume of disclosed vulnerabilities continues to grow, and perimeter technologies such as VPN concentrators, firewalls and file transfer appliances are attractive because they are internet-facing, privileged and frequently lack endpoint telemetry. On the demand side, wider adoption of multi-factor authentication has raised the cost of credential-only attacks, pushing adversaries toward technical exploitation. The defensive bottleneck is remediation speed. The 2025 DBIR found that only about 54% of edge-device vulnerabilities were fully remediated during the year (Verizon, 2025), and the 2026 DBIR reports that only 26% of critical vulnerabilities listed in CISA's Known Exploited Vulnerabilities catalogue were fully remediated by the organisations studied, down from 38% the previous year (Verizon, 2026).

Two episodes illustrate the stakes. The Log4Shell vulnerability (CVE-2021-44228) in the ubiquitous Apache Log4j library allowed remote code execution in an enormous range of products, many of whose owners did not know the library was present (NIST National Vulnerability Database [NVD], 2021). In March 2024, a deliberately inserted backdoor was discovered in the XZ Utils compression library (CVE-2024-3094) shortly before it would have propagated into mainstream Linux distributions (GitHub Advisory Database, 2024). The XZ case is notable because the attacker spent an extended period building trust as a contributor to an under-resourced open-source project, an attack on the social infrastructure of software rather than on code alone.

4.2 Ransomware and Extortion

There are several diverse types of cyber-attacks and security threats on several industries outside oil and gas. The most popular cyber security threats are among is Ransomware etc. (Boye & Onate, 2023). Ransomware remains the most

operationally damaging form of cybercrime for most organisations. The 2025 DBIR found ransomware present in 44% of breaches, a 37% increase on the previous report, while the median ransom paid fell (Verizon, 2025). By the 2026 edition, ransomware was involved in 48% of breaches (Verizon, 2026). At the same time, victims are increasingly refusing to pay: the share of ransomware victims who did not pay rose from 64% in the 2025 DBIR to 69% in the 2026 edition, although the median payment among those who did pay was USD 139,875, compared with USD 115,000 a year earlier (Verizon, 2025, 2026). IBM found that extortion or ransomware incidents disclosed by the attacker cost an average of USD 5.08 million in 2025 (IBM, 2025). These figures describe a maturing criminal industry rather than a declining one. As payment rates fall, operators compensate through volume, through data theft and public leak sites ("double extortion") and through targeting of organisations least able to resist. Small and medium-sized businesses are disproportionately affected; in the 2025 DBIR, ransomware was present in 88% of breaches at small and medium-sized organisations, compared with 39% at large organisations (Verizon, 2025). The February 2024 attack on Change Healthcare (Section 5) demonstrated that ransomware against a single intermediary can disrupt an entire national sector.

4.3 Third parties and the software supply chain

The most significant structural change in the data is the rise of third-party risk. The share of breaches involving a third party doubled from 15% to 30% in the 2025 DBIR (Verizon, 2025), and the 2026 edition reports that third parties featured in 48% of breaches, a 60% increase on the previous year (Verizon, 2026). Third-party exposure includes compromised software vendors, managed service providers, cloud tenants with weak configurations and credentials reused across partner environments. Remediation in third-party environments is slow. The 2026 DBIR found that only 23% of third-party organisations fully remediated missing or improperly configured multi-factor authentication on cloud accounts, and that it took a median of about eight months to resolve half of the findings on weak passwords and permission misconfigurations (Verizon, 2026). The 2025 DBIR similarly noted that leaked secrets discovered in public GitHub repositories took a median of 94 days to remediate (Verizon, 2025). For procurement and supply chain functions, the implication is direct: vendor selection, contracting and ongoing supplier assurance have become security controls in their own right.

4.4 The human element and the evolution of social engineering

The human element was involved in roughly 60% of breaches in the 2025 DBIR and 62% in 2026 (Verizon, 2025, 2026). What has changed is the channel. Verizon reports click rates on mobile-based social engineering about 40% higher than on traditional email phishing (Verizon, 2026), and Mandiant reports that voice phishing rose to 11% of initial infection vectors in 2025, becoming the second most common vector, while email phishing fell to 6% (Mandiant, 2026). Infostealer malware, which harvests browser-stored credentials and session tokens from personal and unmanaged devices, now feeds a supply chain of stolen access that links consumer-grade compromises to enterprise ransomware (Verizon, 2025). The World Economic Forum found that 73% of surveyed leaders had been, or knew someone who had been, directly affected by cyber-enabled fraud in 2025, and that such fraud has overtaken ransomware as the leading concern of chief executives (WEF, 2026). In the United States alone, the FBI's Internet Crime Complaint Center received 859,532 complaints in 2024 with reported losses exceeding USD 16.6 billion (Federal Bureau of Investigation [FBI], 2025). Fraud of this kind rarely requires technical sophistication; it exploits trust, urgency and authority, and it is precisely the category most easily scaled by generative AI (Section 7).

4.5 Nation-state operations and geopolitics

State-sponsored actors pursue espionage, pre-positioning in critical infrastructure and, occasionally, destructive effects. Stuxnet, which sabotaged Iranian uranium enrichment centrifuges, demonstrated that code could cause physical damage to industrial processes (Langner, 2011). The Russian military intelligence unit known as Sandworm subsequently disrupted Ukrainian power distribution in 2015 and 2016 and released the destructive NotPetya malware in 2017, which spread far beyond its intended targets (Greenberg, 2019). Recent data show espionage becoming more patient. Mandiant attributes the rise in global median dwell time from 11 days in 2024 to 14 days in 2025 largely to long-running espionage intrusions and North Korean IT worker schemes, both of which had a median dwell time of 122 days (Mandiant, 2026). The WEF reports that 64% of organisations now factor geopolitically motivated attacks into their risk strategies and that 91% of the largest organisations have changed their cybersecurity strategies because of geopolitical volatility (WEF, 2026). Geopolitics has thus become a permanent input to enterprise risk management rather than a concern confined to governments.

4.6 IoT and operational technology

The expansion of connected devices extends the attack surface into physical systems. The Mirai botnet, which in 2016 conscripted hundreds of thousands of poorly secured cameras and routers into some of the largest distributed denial-of-service attacks then recorded, showed how default credentials on cheap devices can become a systemic risk to internet infrastructure (Antonakakis *et al.*, 2017). In industrial settings, including oil and gas production, power and water, operational technology (OT) was historically designed for reliability and isolation rather than security. As OT is connected to enterprise networks and cloud analytics for efficiency, vulnerabilities in legacy controllers and remote access paths become routes to safety-critical processes.

4.7 Summary of key trends

Table 3: Key indicators from the Verizon DBIR, 2025 and 2026 editions

Indicator (Verizon DBIR)	2025 edition	2026 edition	Direction
Confirmed breaches analysed	12,195	More than 22,000	Larger dataset
Vulnerability exploitation as initial access	20%	31% (top vector)	Worsening
Breaches involving ransomware	44%	48%	Worsening
Breaches involving a third party	30%	48%	Worsening
Human element involved	About 60%	62%	Persistent
Ransomware victims not paying	64%	69%	Improving for defenders
Median ransom paid (where paid)	USD 115,000	USD 139,875	Higher

Sources: Verizon (2025, 2026).

V. Case Evidence: Landmark Incidents, 2017 to 2025

Aggregate statistics show frequency; individual incidents reveal mechanism. The cases in Table 4 were selected purposively to represent distinct failure modes: unpatched systems, supply chain compromise, single points of failure in critical services, open-source fragility, systemic dependency and AI-enabled operations. They are listed newest first.

Table 4: Landmark incidents and their lessons

Date	Incident	Primary failure mode	Consequence and lesson
Sep 2025	AI-orchestrated espionage campaign (GTG-1002)	Misuse of an agentic AI coding tool to automate intrusion	About 30 organisations targeted; a small number of intrusions succeeded; AI performed an estimated 80 to 90% of the campaign. Adversary tempo is no longer bounded by human operators (Anthropic, 2025).
Jul 2024	CrowdStrike Falcon content update failure	Faulty update to a privileged, widely deployed security agent (not an attack)	About 8.5 million Windows devices crashed, disrupting airlines, banks and hospitals. Concentration of trusted software creates systemic availability risk (Microsoft, 2024; CISA, 2024).
Mar 2024	XZ Utils backdoor (CVE-2024-3094)	Long-term social engineering of an open-source maintainer	Backdoor discovered shortly before wide distribution. Critical infrastructure depends on under-resourced volunteer projects (GitHub Advisory Database, 2024).
Feb 2024	Change Healthcare ransomware	Stolen credentials used on a Citrix remote access service that lacked multi-factor authentication	Data of an estimated 192.7 million people affected; prolonged disruption to claims and payments; a USD 22 million ransom paid. A single intermediary can be a sector-wide point of failure (HIPAA Journal, 2025).
May to Jun 2023	MOVEit Transfer mass exploitation (CVE-2023-34362)	Zero-day SQL injection in a managed file transfer product, exploited by the CL0P group	Large-scale data theft from organisations and their downstream clients. One product flaw cascades through supply chains (CISA & FBI, 2023).
Dec 2021	Log4Shell (CVE-2021-44228)	Remote code execution in a ubiquitous logging library	Organisations struggled to locate affected software. Lack of software inventory turns one flaw into a global emergency (NVD, 2021).
May 2021	Colonial Pipeline ransomware	Legacy VPN profile that was no longer meant to be in use	Proactive shutdown of the 5,500-mile fuel pipeline; about USD 2.3 million of the ransom later seized by US authorities. IT compromise can halt OT operations (Blount, 2021; US Department of Justice, 2021).
Dec 2020	SolarWinds Orion supply chain compromise	Trojanised software updates from a trusted vendor	Fewer than 18,000 customers received the malicious update; selected government and corporate networks were targeted for espionage. Trusted update channels are high-value targets (CISA, 2020; SolarWinds Corporation, 2020).
Jun 2017	NotPetya	Destructive malware spread through a compromised accounting software update	Global disruption to shipping, logistics and manufacturing far beyond the intended targets. State operations generate uncontrollable collateral damage (Greenberg, 2019).
May 2017	WannaCry	Self-propagating ransomware exploiting an unpatched Windows SMB flaw	Widespread disruption, including to the UK National Health Service. Basic patching and asset management remain decisive (National Audit Office, 2017).

5.1 Lessons across the cases

Lesson 1: Basic hygiene failures remain the dominant root cause. WannaCry was, in the words of the UK National Audit Office, a relatively unsophisticated attack that could have been prevented by following basic IT security best practice; the infected organisations had unpatched or unsupported Windows systems (National Audit Office, 2017). Colonial Pipeline and Change Healthcare both began with weakly protected remote access: an unused legacy VPN profile in one case and a remote access portal without multi-factor authentication in the other (Blount, 2021; HIPAA Journal, 2025). The persistence of these root causes across almost a decade, despite large increases in security spending, supports the economic explanation in Section 2.2: organisations under-invest in unglamorous controls such as asset inventory,

patching and access management because their benefits are invisible until they fail.

Lesson 2: Trust is the new perimeter, and it is being attacked directly. SolarWinds, NotPetya, XZ Utils and MOVEit all exploited the trust organisations place in software suppliers and update mechanisms. Zero trust principles (Rose et al., 2020) are usually applied to users and devices; these cases show they must also be applied to software, vendors and service providers.

Lesson 3: Availability risk is now systemic. The CrowdStrike outage was not malicious, yet it produced disruption on a scale comparable to the largest attacks. Change Healthcare similarly showed that concentration of critical functions in a single intermediary converts an organisational

incident into a sectoral one. Consistent with Perrow's (1999) theory, tight coupling turns local faults into system-wide failures.

Lesson 4: The boundary between IT and physical operations is porous. Colonial Pipeline's operational shutdown was a precautionary response to an IT compromise, not the result of attackers reaching control systems. For energy and industrial firms, this means that business continuity planning must assume that IT incidents can force operational decisions even when OT is technically intact.

Lesson 5: Adversary speed and scale are changing qualitatively. The GTG-1002 campaign is significant less for its outcomes, which were limited, than for its operating model. Anthropic (2025) reports that human operators intervened only at roughly four to six critical decision points per campaign, while the AI system carried out reconnaissance, exploitation, credential harvesting and data analysis at request rates no human team could sustain. Defensive processes calibrated to human-speed adversaries will need to adapt (Section 7).

VI. Measuring Security: What the Indicators Reveal

This section addresses RQ2. It examines four families of indicators: fiscal impact, detection performance, workforce capacity and governance maturity. Taken together they show that defense is improving in speed and sophistication, but that losses continue to rise because exposure and adversary capability are growing faster.

6.1 The financial impact of breaches

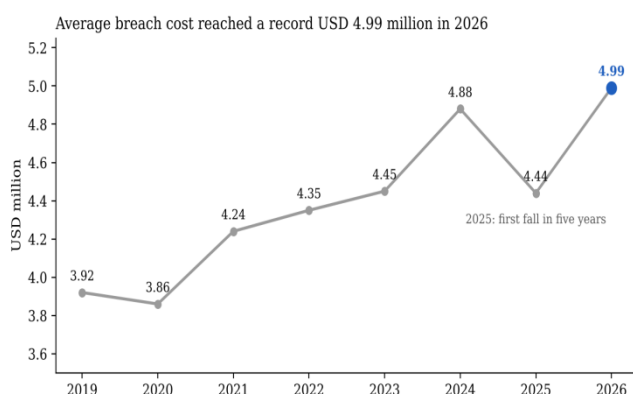


Figure 1: Global average total cost of a data breach, USD million, by report year. Source: IBM / Ponemon Institute, Cost of a Data Breach Reports (IBM, 2023, 2025, 2026a)

The IBM and Ponemon Institute series is the longest-running estimate of breach costs. The global average fell 9% in 2025, to USD 4.44 million, the first decline in five years, which IBM attributed largely to faster identification and

containment (IBM, 2025). The improvement did not last. Across 602 organisations breached between March 2025 and February 2026, the average rose 12% to a record USD 4.99 million (IBM, 2026a, 2026b). Detection and escalation costs plus lost business accounted for 63% of the total, which indicates that the dominant cost of a breach is operational disruption and customer loss rather than fines or notification (Security Boulevard, 2026). Averages conceal large variation. The United States recorded an average of USD 11.5 million in 2026, more than twice the global figure, and healthcare remained the most expensive sector for the thirteenth consecutive year, at USD 6.64 million (Baker Donelson, 2026; HIPAA Journal, 2026). Of greater analytical interest is the effect of defensive investment. In 2025, organisations that used security AI and automation extensively saved an average of USD 1.9 million per breach and shortened the breach lifecycle by about 80 days (IBM, 2025). In 2026, organisations making extensive use of AI and automation in security saved USD 1.93 million on average compared with those using none, yet only about a quarter of organisations had adopted such tools in security operations (IBM, 2026a, 2026b). These findings are among the clearest available evidence that well-implemented defenses change outcomes.

6.2 Detection and dwell time

Dwell time, the period between initial compromise and detection, is a direct measure of defensive visibility. Mandiant's global median fell from 205 days in 2014 to 10 days in 2023, one of the largest measurable improvements in the history of the field (Mandiant, 2025). It then rose to 11 days in 2024 and to 14 days in 2025 (Mandiant, 2026). The recent increase does not mean that ordinary detection has deteriorated: organisations that detected intrusions themselves did so in a median of about nine days in 2025, and 52% of intrusions were detected internally, up from 43% (Help Net Security, 2026; Mandiant, 2026). The rise is driven by externally notified cases, whose median rose to 25 days, and particularly by espionage and insider-style operations with median dwell times of 122 days (Help Net Security, 2026; Mandiant, 2026). IBM's data show a similar pattern. The mean breach lifecycle (time to identify and contain) fell to 241 days in 2025, a nine-year low (IBM, 2025), before edging up to about 247 days in 2026 (HIPAA Journal, 2026). The gap between Mandiant's median of two weeks and IBM's mean of eight months is itself instructive: most intrusions are now found relatively quickly, but a long tail of stealthy compromises persists for many months. Detection must also be judged against adversary speed. If initial access can be handed to a ransomware affiliate in a median of 22 seconds (Mandiant, 2026), then a two-week detection window,

however improved, leaves ample time for damage. Speed, not merely eventual detection, is now the operative standard.

6.3 Workforce and skills capacity

The 2024 ISC2 Cybersecurity Workforce Study estimated an active global workforce of about 5.5 million, essentially unchanged from the previous year, and a workforce gap of 4.8 million, an increase of 19% (ISC2, 2024). In its 2025 study, based on more than 16,000 respondents, ISC2 chose not to publish a headline gap estimate, explaining that respondents increasingly emphasised specific skills needs over headcount (ISC2, 2025). The 2025 findings are nonetheless stark: 95% of respondents reported at least one skill need, 59% described their skills gaps as critical or significant (up from 44% in 2024), and 88% reported at least one significant cybersecurity consequence attributable to a skills shortage (ISC2, 2025). The WEF reinforces the link between skills and resilience: among organisations reporting insufficient cyber resilience, 85% also lacked critical skills and people (WEF, 2026). The constraint is therefore not simply the number of professionals but the match between their skills and the technologies, notably AI and cloud that organisations are adopting.

6.4 Governance of innovative technology

Governance indicators show adoption outpacing control. In the 2025 IBM study, 63% of breached organisations lacked AI governance policies, and 97% of organisations reporting an AI-related security incident lacked proper AI access controls (IBM, 2025). By 2026, “shadow AI” (staff use of unsanctioned AI tools) was involved in 43% of security incidents, up from 20%, and such incidents cost an average of USD 5.39 million (HIPAA Journal, 2026; Baker Donelson, 2026). Verizon similarly found that frequent employee use of AI tools rose from 15% to 45% in a year, and that 67% of users accessing AI services on corporate devices did so through non-corporate accounts (Verizon, 2026). There are signs of response: the share of organisations with a process to assess the security of AI tools before deployment rose from 37% in 2025 to 64% in 2026 (WEF, 2026).

6.5 Interpreting the indicators

Three cautions apply when using these indicators to answer the question “how secure are we?”. First, cost and incident counts measure realised losses, not prevented ones; a successful security programme is largely invisible in these datasets. Second, several indicators are composition-sensitive: a rise in median dwell time can reflect a shift in which incidents are investigated rather than a decline in capability.

Third, compliance and maturity indicators measure inputs. Organisations can score well on frameworks while remaining exposed to the specific vectors, such as unpatched edge devices or vendor credentials, that adversaries actually use. A credible assessment must therefore triangulate across exposure, detection, resilience, governance and capacity, as Section 9 does.

VII. Emerging Frontiers: AI, Cloud, Operational Technology and Quantum

This section addresses RQ3. Each technology examined here lowers costs for both attackers and defenders. Consistent with Slayton (2017), whether it shifts the balance depends on how quickly and competently each side adopts it, not on the technology alone.

7.1 AI as an offensive amplifier

Until recently, discussion of AI-enabled attacks was largely speculative. The evidence base has now changed. Fang, Bindu, Gupta and Kang (2024) showed that a large language model (LLM) agent equipped with simple tools could autonomously exploit a majority of a benchmark set of real one-day vulnerabilities when given their public descriptions. In September 2025, Anthropic detected and disrupted a campaign it attributed with high confidence to a Chinese state-sponsored group, designated GTG-1002, which used an agentic AI coding tool within an automated framework to target about 30 organisations in technology, finance, chemical manufacturing and government. Anthropic estimated that the attackers used AI to perform 80 to 90% of the campaign, with human intervention needed at only about four to six critical decision points; a small number of intrusions succeeded before the activity was stopped (Anthropic, 2025). Anthropic also noted that the model occasionally hallucinated credentials or claimed to have extracted secret information that was in fact publicly available, a reminder that AI-enabled attacks are powerful but not flawless. Industry data indicates that such capabilities are diffusing. IBM reported that attackers used AI in about one in six breaches in 2025, mostly to scale phishing and impersonation (IBM, 2025). In the 2026 study, AI-enabled breaches rose by 56%, accounted for one in four malicious breaches and cost about USD 6 million on average, roughly USD 1 million more than the overall average (IBM, 2026b). Verizon similarly reports that generative AI now supports 15 distinct attack techniques, helping threat actors work faster at every stage from identifying security gaps to writing malware (Verizon, 2026). The most immediate effect is on fraud: convincing, personalised and multilingual phishing, voice

cloning and deepfake video reduce the cues that people and filters have traditionally relied on.

7.2 AI as a Defensive Force

AI also offers the most promising route to close the speed gap identified in Section 6.2. The IBM findings on security automation (USD 1.9 million savings and about 80 fewer days of breach lifecycle in 2025) represent the clearest quantitative evidence that machine-speed defense changes outcomes (IBM, 2025). Defensive applications include alert triage, correlation of telemetry across sources, malware analysis, detection rule generation, vulnerability discovery in source code and incident investigation. Notably, Anthropic reported using its own models to analyse the large volume of data generated during its GTG-1002 investigation (Anthropic, 2025). Some caution is warranted. Sommer and Paxson (2010) showed that machine learning for intrusion detection faces structural obstacles, including the excessive cost of false positives, the scarcity of representative attack data and the difficulty of interpreting model outputs. These problems have not disappeared; they reappear whenever AI-generated alerts or summaries are trusted without verification. Defensive AI is most valuable when it accelerates skilled analysts rather than replacing them, which links its effectiveness back to the skills constraint described in Section 6.3.

7.3 Securing AI Systems Themselves

AI systems introduce new attack surfaces. Goodfellow, Shlens and Szegedy (2015) demonstrated that imperceptible input perturbations can cause neural networks to misclassify with high confidence. So, while artificial intelligence (AI) brings significant benefits to the energy sector, it also introduces challenges, but few challenges on the integrating of artificial intelligence (AI) into energy systems (IEPL, 2019). Carlini et al. (2021) showed that large language models can be induced to reproduce verbatim fragments of their training data, including personal information. Greshake et al. (2023) introduced indirect prompt injections, in which malicious instructions embedded in web pages, documents or emails are processed by an LLM-integrated application and executed with the user's privileges. As organisations deploy AI agents that can read email, browse the web and call internal tools, prompt injections become analogous to a remote code execution vulnerability. The cost data confirm that these are no longer theoretical concerns: the 2026 IBM study recorded an average cost of about USD 6.07 million for model inversion attacks, well above the global average (Baker Donelson, 2026; IBM, 2026a). Securing AI therefore requires the same disciplines as securing any other privileged system: least privilege for agents and their tools, separation of trusted

instructions from untrusted content, logging and review of agent actions, and governance of which AI services staff may use (Section 6.4).

7.4 Cloud Concentration and Identity

Cloud computing has improved baseline security for many organisations by shifting patching, physical security and much infrastructure hardening large providers with deep expertise. It also concentrated on risk. Under the shared responsibility model, customers remain responsible for identity, configuration and data, and the DBIR evidence on weak or missing multi-factor authentication in third-party cloud environments shows how often that responsibility is not met (Verizon, 2026). Identity has effectively become the perimeter: the same credentials and session tokens grant access to email, file storage, enterprise applications and administrative consoles. The CrowdStrike outage (Microsoft, 2024) illustrates the complementary availability risk, in which a fault at a single trusted provider propagates instantly across its customer base. Zero trust architecture (Rose *et al.*, 2020) and concentration-aware resilience planning are the principal responses.

7.5 Operational Technology in Energy and Critical Infrastructure

For oil and gas, power and water operators, the convergence of information technology (IT) and OT is the frontier with the highest physical stakes. Remote monitoring, predictive maintenance and IoT-based production optimisation deliver real efficiency gains, but they create network paths between internet-facing systems and safety-critical control processes. Legacy controllers often lack authentication, cannot be patched without production downtime and remain in service for decades. Stuxnet (Langner, 2011) demonstrated the feasibility of manipulating industrial processes, and Colonial Pipeline showed that an IT-only compromise can still halt operations (Section 5). Effective practice combines network segmentation between IT and OT, strict control of remote access, asset inventories that include field devices, and incident response plans that integrate engineering and safety teams.

7.6 Quantum computing and cryptographic transition

Shor (1997) showed that a sufficiently large quantum computer could factor integers and compute discrete logarithms in polynomial time, which would break the RSA and elliptic-curve public-key cryptography that protects most internet traffic and digital signatures. Although such machines do not yet exist, two features make the threat current. First,

adversaries can record encrypted data today and decrypt it later (“harvest now, decrypt later”). Second, cryptographic migration across large estates takes many years. Mosca (2018) captured the resulting decision rule: if x is the number of years data must remain confidential, y is the time required to migrate to quantum-safe cryptography, and z is the time until a cryptographically relevant quantum computer exists, then an organisation is already at risk whenever:

$$x + y > z$$

The defensive response is now concrete. On 13 August 2024, NIST published its first three post-quantum cryptography standards: FIPS 203 (ML-KEM, for key encapsulation), FIPS 204 (ML-DSA, for digital signatures) and FIPS 205 (SLH-DSA, a hash-based signature scheme) (NIST, 2024b, 2024c, 2024d). These build on decades of research into problems believed to be hard for both classical and quantum computers (Bernstein & Lange, 2017). In the WEF survey, 37% of respondents expected quantum technologies to affect cybersecurity within the next 12 months (WEF, 2026). The practical priority for most organisations is not quantum computing itself but cryptographic inventory and agility: knowing where public-key cryptography is used and being able to replace it.

7.7 Summary assessment

Table 5: Net effect of emerging technologies on security posture

Technology	Main benefit to attackers	Main benefit to defenders	Net effect on security posture (2026)
Generative and agentic AI	Scaled fraud and phishing; automated reconnaissance and exploitation	Machine-speed triage, detection and investigation; code analysis	Currently favours attackers in fraud; favours well-resourced defenders in detection
AI systems as targets	Prompt injection; data extraction; model abuse	Governed, least-privilege deployment	New exposure largely ungoverned in many organisations
Cloud and identity platforms	Credential theft yields broad access; concentration multiplies impact	Strong baseline controls; centralised logging	Improves average security; raises systemic tail risk
IT/OT convergence	Paths from internet-facing systems to physical	Better monitoring and asset visibility	Exposure growing faster than OT security maturity

Technology	Main benefit to attackers	Main benefit to defenders	Net effect on security posture (2026)
	processes		
Quantum computing	Future decryption of today's harvested data	Standardised post-quantum algorithms	Manageable if migration starts now; costly if delayed

VIII. The African and Nigerian Perspective

This section addresses RQ4. Africa combines one of the world's fastest rates of digital adoption with some of its thinnest defensive capacity. The result is a widening gap between exposure and capability, although recent legal and institutional reforms, including in Nigeria, show measurable progress.

8.1 The continental picture

Kshetri (2019) described Africa as among the fastest-growing regions for cybercrime, driven by rapid internet and mobile money adoption, weak legal frameworks and limited enforcement capacity, while noting that governments and private firms had begun to respond. The INTERPOL Africa Cyberthreat Assessment Report 2025 confirms and sharpens that picture. Two-thirds of surveyed African member countries reported that cyber-related offences make up a medium-to-high share of all crime, and in West and East Africa cybercrime accounts for more than 30% of all reported crime (INTERPOL, 2025a). Online scams, particularly phishing, were the most frequently reported offences, while ransomware, business email compromise (BEC) and digital sextortion remained widespread. In West Africa, BEC fraud has supported highly organised, multi-million-dollar criminal enterprises (INTERPOL, 2025a). Between 2019 and 2025, cyber incidents across the continent caused estimated losses exceeding USD 3 billion, with finance, healthcare, energy and government among the hardest-hit sectors (INTERPOL, 2025a). Enforcement capacity is the critical weakness. Ninety per cent of African countries reported needing significant improvement in law enforcement or prosecution capacity; only 30% had an incident reporting system, 29% a digital evidence repository and 19% a cyber threat intelligence database (INTERPOL, 2025a). Regional cooperation is improving: INTERPOL's Operation Sentinel, conducted across 19 countries in late 2025, led to 574 arrests and the recovery of about USD 3 million, with linked losses exceeding USD 21 million (INTERPOL, 2025b). INTERPOL's 2026 assessment, drawing on data from 36 African member countries, found that AI now enables 55% of reported cybercrimes across Africa (INTERPOL, 2026), a development consistent with the

global evidence in Section 7.1. Skills constraints are more severe than elsewhere. In the WEF survey, 70% of chief executives in sub-Saharan Africa reported lacking the skills needed to meet their current cybersecurity goals, the highest of any region (WEF, 2026). On the positive side, the ITU Global Cybersecurity Index 2024 found that Africa was the region that had advanced the most in cybersecurity commitments since 2021 (ITU, 2024b), and several African states, including Ghana, reached Tier 1, the highest tier (Ministry of Communications and Digitalisation, Ghana, 2024).

8.2 Nigeria's legal and institutional framework

Nigeria has built a substantial legal framework over the past decade. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 created the country's first comprehensive cybercrime offences and established a National Cyber Security Fund. The Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024, signed into law on 28 February 2024, updated offences, strengthened enforcement provisions and clarified, in Section 44(2)(a), a levy of 0.5% on the value of electronic transactions by specified businesses to finance the Fund under the administration of the Office of the National Security Adviser (Mondaq, 2024; Nairametrics, 2024a). When the Central Bank of Nigeria directed banks on 6 May 2024 to begin collecting the levy (Nairametrics, 2024a), public objection centered on whether the burden would fall on customers rather than on the businesses named in the Act. The House of Representatives directed the Central Bank to suspend implementation (TechHive Advisory, 2024), and on 14 May 2024 the Federal Executive Council announced that the levy had been suspended pending review (Nairametrics, 2024c). The episode illustrates the governance dimension of cybersecurity: sustainable funding mechanisms require public legitimacy as well as legal authority. Data protection was placed on a statutory footing by the Nigeria Data Protection Act 2023, signed on 12 June 2023, which established the Nigeria Data Protection Commission (NDPC) and imposed security, breach notification and accountability obligations on data controllers and processors (Nigeria Data Protection Commission [NDPC], n.d.; KPMG Nigeria, 2023). Strategic direction is provided by the National Cybersecurity Policy and Strategy 2021, coordinated by the Office of the National Security Adviser, while the Nigeria Computer Emergency Response Team (ngCERT) provides national incident coordination. In the ITU Global Cybersecurity Index 2024, Nigeria was placed in Tier 3 ("establishing"), alongside countries such as Cameroon (ITU, 2024a; Ministry of Communications and Digitalisation, Ghana, 2024; Nairametrics, 2024b). Tier 3 indicates meaningful commitments across the five GCI pillars (legal, technical,

organisational, capacity development and cooperation) but significant remaining gaps; the ITU notes that, globally, the capacity development and technical pillars are where countries are typically weakest (ITU, 2024a).

8.3 Sectoral exposure

Three Nigerian sectors deserve particular attention. Financial services have digitised rapidly through mobile banking, payment platforms and fintech, creating large volumes of electronic transactions that are attractive to fraudsters and that depend on the integrity of identity verification. Telecommunications underpin both mobile money and national identity linkage, making SIM-swap fraud and account takeover persistent risks. Oil and gas, the country's principal source of export revenue, increasingly relies on remote monitoring, IoT sensors and digital supply chains across onshore, swamp and offshore operations. In this sector the IT/OT convergence risks described in Section 7.5 coincide with geographically dispersed assets, extensive use of contractors and service companies, and long procurement chains for imported technology. For energy companies, supplier cybersecurity assurance is therefore as much a procurement discipline as a technical one.

8.4 Structural constraints

Several constraints shape Nigeria's posture beyond formal law and policy:

- i. **Under-reporting and limited data.** Few organisations publicly disclose incidents, and national statistics on cyber incidents are sparse, making it difficult to measure progress or allocate resources by risk.
- ii. **Enforcement and forensic capacity.** The continental gaps in digital evidence handling and threat intelligence identified by INTERPOL (2025a) apply to Nigeria, limiting deterrence.
- iii. **Skills and retention.** Demand for experienced security professionals far exceeds local supply, and skilled practitioners are frequently recruited by foreign employers.
- iv. **Cost and dependency.** Most security technology is imported and priced in foreign currency, so exchange-rate pressure directly affects the affordability of licences, cloud services and training.
- v. **Reputational externalities.** The international association of Nigeria with online fraud imposes costs on legitimate Nigerian businesses and individuals, including heightened scrutiny of transactions and reduced trust.

8.5 How secure is Nigeria?

Applying the five-dimension lens from Section 2.7 yields a mixed assessment (Table 6).

Table 6: Nigeria's cybersecurity posture across the five dimensions

Dimension	Assessment	Evidence
Exposure	High and rising	Rapid growth in digital financial services and connected industrial assets; West African prevalence of BEC and online fraud (INTERPOL, 2025a)
Detection	Limited visibility	Sparse incident reporting and threat intelligence infrastructure across the region (INTERPOL, 2025a)
Resilience	Uneven	Strong in large banks and multinational operators; weak in SMEs and public agencies
Governance	Improving	Cybercrimes Act 2015 and 2024 amendment; Nigeria Data Protection Act 2023; national policy and strategy; Tier 3 in ITU GCI 2024
Capacity	Binding constraint	Regional skills shortfalls (WEF, 2026); enforcement and prosecution gaps (INTERPOL, 2025a)

Nigeria is therefore better governed in cybersecurity than at any point in its history, but its operational capacity to detect, investigate and recover from attacks has not kept pace with its digital exposure.

IX. Discussion: The Security Paradox

9.1 Synthesis across the five dimensions

Bringing the evidence together, the global position in 2026 can be summarised as in Table 7.

Table 7: Global synthesis across the five dimensions

Dimension	Trend relative to threat capability	Principal evidence
Exposure	Deteriorating	Exploitation now the top initial access vector (31%); third parties in 48% of breaches; low remediation of known exploited vulnerabilities; rapid AI adoption without governance (Verizon, 2026)
Detection	Improving in absolute terms, lagging adversary speed	Dwell time down from 205 days (2014) to 9 days for internal detection (2025), but a 22-second access hand-off and a

Dimension	Trend relative to threat capability	Principal evidence
		long tail of 122-day espionage intrusions (Mandiant, 2025, 2026)
Resilience	Mixed	Record breach costs, yet large savings for organisations with extensive security automation; more victims refusing ransom (IBM, 2026a; Verizon, 2026)
Governance	Improving	NIST CSF 2.0 adds a Govern function; post-quantum standards finalised; AI security assessment rising from 37% to 64% of organisations (NIST, 2024a, 2024b; WEF, 2026)
Capacity	Binding constraint	95% of security teams report skills needs; 88% report a significant incident linked to skills shortages; 70% of sub-Saharan African CEOs lack needed skills (ISC2, 2025; WEF, 2026)

The pattern is consistent: the dimensions that organisations directly control (detection tooling, governance frameworks) are improving, while the dimensions shaped by the wider ecosystem (exposure through suppliers and software, the speed of adversaries, and the availability of skills) are deteriorating or constrained.

9.2 Why better defense has not produced less loss

Four mechanisms explain the paradox of rising capability alongside rising losses.

First, a “Red Queen” dynamic. Adversaries adapt to defensive improvements. Wider use of multi-factor authentication pushed attackers toward exploiting software vulnerabilities and session tokens; improved email filtering pushed them toward voice and mobile channels; falling ransom payment rates pushed them toward data theft and higher volume. Defense must improve merely to hold its position.

Second, misaligned incentives persist. As Anderson (2001) and Anderson and Moore (2006) predicted, the parties best placed to reduce risk, such as software vendors, open-source consumers and large platform providers, do not bear its full cost. The low remediation rates for known exploited vulnerabilities and third-party misconfigurations reported in the 2025 and 2026 DBIRs reflect this externality. Individual

organisations rationally invest in protecting the ecosystem they depend on.

Third, systemic coupling has increased. Each organisation now relies on many more external software components and service providers than a decade ago. Following Perrow (1999), as coupling tightens, failures increasingly originate outside the organisation and propagate faster than local controls can contain them. The CrowdStrike and Change Healthcare cases demonstrate that even organisations with strong internal security can be disrupted through dependencies.

Fourth, capacity is unevenly distributed. The benefits of security automation and AI-enabled defense accrue mainly to organisations with the budget and skills to deploy them well. Small and medium-sized enterprises, public agencies and developing economies face the same adversaries with far fewer resources, as the disproportionate impact of ransomware on SMEs (Verizon, 2025) and the regional skills data (WEF, 2026) show. Cyber inequity thus becomes a source of systemic risk, because weakly defended organisations are often suppliers to, or partners of, better-defended ones.

9.3 So, how secure are we?

The evidence supports a conditional answer rather than a single verdict. For well-resourced organisations that have invested in identity security, rapid patching, extensive monitoring and automation, the answer is: more secure than at any previous time, but not secure against sophisticated, patient adversaries or against failures in their own supply chains. Their residual risk is increasingly systemic rather than local. For the majority of organisations, including most SMEs and many public bodies, the answer is: insufficiently secure against commodity threats. Their dominant risks remain the basic hygiene failures (unpatched systems, weak credentials, unmanaged suppliers) that have caused major incidents since WannaCry, now exploited at greater speed and scale with AI assistance. For developing digital economies such as Nigeria, the answer is: increasingly well governed on paper, but under-equipped in operational capacity relative to rapidly expanding exposure. The gap is most acute in detection, enforcement and skills. Across all three groups, a common conclusion is held. Security should be understood not as a state that can be achieved and certified but as a dynamic capability, the continuing ability to anticipate, withstand, detect, respond to and recover from adverse events at a pace that matches adversaries. By that standard, collective security is improving, but more slowly than the threat.

9.4 Implications for theory

The findings support and extend the theoretical framework in Section 2. They confirm the explanatory power of security economics: the most persistent failures are those where incentives are misaligned. They support Slayton's (2017) argument that the offence-defense balance is organisational rather than technological, since the same AI capabilities produce large defensive gains for some organisations and large offensive gains for adversaries targeting others. And they suggest an extension of Perrow's (1999) normal accident theory to digital ecosystems: as dependency on shared providers grows, the unit of analysis for security must shift from the individual organisation to the ecosystem of which it is part.

X. Contribution to Knowledge, Recommendations and Conclusion

10.1 Contribution to knowledge

This paper makes four contributions. First, it provides an up-to-date integrative synthesis of the principal global cybersecurity datasets, including the 2026 editions of the Verizon DBIR, the IBM Cost of a Data Breach Report and Mandiant M-Trends, together with foundational theory. Second, it proposes a five-dimension assessment lens (exposure, detection, resilience, governance and capacity) that converts disparate indicators into an explicit, relative judgement of security adequacy, and that can be applied at organisational, sectoral and national levels. Third, it articulates and explains the "security paradox" of rising defensive capability alongside rising losses through four mechanisms: adversarial adaptation, misaligned incentives, systemic coupling and uneven capacity. Fourth, it extends the analysis to Nigeria and Africa, applying the lens to a context that is under-represented in international scholarship and identifying operational capacity, rather than legislation, as the binding constraint.

10.2 Recommendations for organisations

- i. **Prioritise exposure reduction on the vectors adversaries actually use.** Maintain a complete inventory of internet-facing assets; patch or isolate vulnerabilities listed in the CISA Known Exploited Vulnerabilities catalogue within days rather than months; and retire or harden legacy remote access.
- ii. **Treat identity as the primary perimeter.** Enforce phishing-resistant multi-factor authentication, manage session tokens and privileged accounts, and apply zero

trust principles to users, devices, workloads and AI agents (Rose et al., 2020).

- iii. **Make supplier security a procurement control.** Embed cybersecurity requirements in vendor selection, contracts and performance reviews; require software bills of materials and incident notification clauses; verify multi-factor authentication and configuration hygiene in supplier environments; and tier suppliers by criticality and access. The doubling and subsequent rise of third-party involvement in breaches (Verizon, 2025, 2026) makes this one of the highest-return interventions available.
- iv. **Invest in machine-speed detection and response.** The evidence on security automation (IBM, 2025, 2026a) justifies investment in integrated telemetry, automated triage and pre-approved containment actions, paired with analysts trained to verify AI outputs.
- v. **Govern AI before scaling it.** Establish an inventory of AI tools in use, approved services and data handling rules; assess AI applications for prompt injection and excessive agency before deployment; and monitor for shadow AI.
- vi. **Plan for systemic failures.** Test business continuity against the loss of key providers, including cloud platforms, identity services and security agents, and ensure that recovery does not depend on the systems that have failed.
- vii. **Segment and secure operational technology.** For energy and industrial operators, separate IT and OT networks, strictly control remote access to field systems, and integrate engineering and safety teams into incident response.
- viii. **Begin post-quantum preparation.** Inventory cryptographic dependencies, prioritise long-lived sensitive data, and require cryptographic agility and support for FIPS 203, 204 and 205 in new procurements (NIST, 2024b, 2024c, 2024d).
- ix. **Invest in skills, not only headcount.** Fund continuous training in cloud, identity and AI security, and design controls that support rather than burden staff (Adams & Sasse, 1999; Herley, 2009).

10.3 Recommendations for government and regulators, with reference to Nigeria

- i. **Build operational capacity alongside legislation.** Prioritise digital forensics laboratories, specialised prosecutors and judges, and sustained funding for ngCERT and sectoral computer emergency response teams, addressing the enforcement gaps identified by INTERPOL (2025a).

- ii. **Establish trusted incident reporting.** Introduce confidential, proportionate mandatory reporting for significant incidents in critical sectors, with aggregated statistics published regularly to inform policy and investment.
- iii. **Resolve the cybersecurity levy transparently.** Clarify the incidence of Section 44 levy consistent with the text of the Act, publish allocations from the National Cyber Security Fund, and link spending to measurable capacity outcomes to secure public legitimacy.
- iv. **Harmonise data protection and cybersecurity obligations.** Align NDPC breach notification requirements with sectoral regulators (CBN, NCC, NUPRC and others) to reduce duplication and improve compliance.
- v. **Develop the national skills pipeline.** Expand university and vocational programmes in cybersecurity, support professional certification, and create incentives to retain skilled practitioners locally.
- vi. **Strengthen critical infrastructure protection for energy.** Issue OT security baselines for oil, gas and power operators, and require supplier assurance for contractors with remote access to production systems.
- vii. **Deepen regional and international cooperation.** Continue participation in INTERPOL and AFRIPOL operations and pursue mutual legal assistance arrangements to address cross-border fraud networks.

10.4 Recommendations for technology providers

Software vendors and platform providers should adopt secure-by-design and secure-by-default practices, staged and reversible update mechanisms for privileged software (a direct lesson of the CrowdStrike outage), sustained funding for critical open-source dependencies (a lesson of XZ Utils), and robust abuse monitoring for AI services capable of being used in offensive operations, as demonstrated by the GTG-1002 case (Anthropic, 2025).

10.5 Directions for future research

Future work should (a) develop validated, outcome-based metrics of security that capture prevented as well as realised losses; (b) collect primary incident and cost data in African economies, where published evidence remains scarce; (c) evaluate empirically whether AI-enabled defence narrows or widens the capability gap between large and small organisations; (d) model systemic cyber risk arising from provider concentration, drawing on methods from financial stability analysis; and (e) study the effectiveness of procurement-based supplier security controls in reducing third-party breaches.

10.6 Conclusion

This paper asked how secure we are. The evidence from the most comprehensive datasets available in 2026 shows that defenders have become faster, better governed and better equipped than ever before. Organisations that invest in automation, identity security and secure development achieve markedly better outcomes, and the cryptographic foundations for a post-quantum future are in place. Yet losses continue to rise because exposure is expanding through software, suppliers and AI adoption; because adversaries, now assisted by AI, operate at machine speed; because incentives across the digital ecosystem remain misaligned; and because the skills and institutions needed for defense are unevenly distributed. In Nigeria and across Africa, substantial legal progress has not yet been matched by operational capacity. The answer to the title question is therefore conditional: we are more capable than ever, but less secure than we need to be. Closing that gap will depend less on any single technology than on sustained attention to fundamentals, on treating suppliers and ecosystems as part of the security perimeter, and on building human and institutional capacity at the same pace as digital adoption. Security is not a destination to be reached but a capability to be maintained, and in an environment where adversaries learn continuously, so must defenders.

REFERENCES

- [1] Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40–46. <https://doi.org/10.1145/322796.322806>
- [2] Anderson, R. (2001). Why information security is hard: An economic perspective. In *Proceedings of the 17th Annual Computer Security Applications Conference* (pp. 358–365). IEEE. <https://doi.org/10.1109/ACSAC.2001.991552>
- [3] Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). Wiley.
- [4] Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610–613. <https://doi.org/10.1126/science.1130992>
- [5] Anthropic. (2025, November 13). Disrupting the first reported AI-orchestrated cyber espionage campaign. <https://www.anthropic.com/news/disrupting-AI-espionage>
- [6] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017). Understanding the Mirai botnet. In *Proceedings of the 26th USENIX Security Symposium* (pp. 1093–1110). USENIX Association.
- [7] Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*. <https://doi.org/10.48550/arXiv.1901.02672>
- [8] Baker Donelson. (2026). Ten takeaways from IBM's 2026 Cost of a Data Breach Report. <https://www.bakerdonelson.com/ten-takeaways-from-ibms-2026-cost-of-a-data-breach-report>
- [9] Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), 188–194. <https://doi.org/10.1038/nature23461>
- [10] Blount, J. (2021, June 8). Testimony of Joseph Blount, President and Chief Executive Officer, Colonial Pipeline Company, before the United States Senate Committee on Homeland Security and Governmental Affairs. <https://www.hsgac.senate.gov/imo/media/doc/Testimony-Blount-2021-06-08.pdf>
- [11] Boye Azibole, Frederick, Onate Egerton Taylor. Analysis on Cybersecurity Control and Monitoring Techniques in Industrial IoT: Industrial Control Systems. *Internet of Things and Cloud Computing*. Vol. 11, No. 1, 2023, pp. 1-17. doi: 10.11648/j.iotcc.20231101.11
- [12] Carlini, N., Tramèr, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., Roberts, A., Brown, T., Song, D., Erlingsson, Ú., Oprea, A., & Raffel, C. (2021). Extracting training data from large language models. In *Proceedings of the 30th USENIX Security Symposium* (pp. 2633–2650). USENIX Association.
- [13] Cybersecurity and Infrastructure Security Agency. (2020, December 13). Emergency Directive 21-01: Mitigate Solar Winds Orion code compromise. <https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise>
- [14] Cybersecurity and Infrastructure Security Agency. (2024, July 19). Widespread IT outage due to CrowdStrike update. <https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update>
- [15] Cybersecurity and Infrastructure Security Agency & Federal Bureau of Investigation. (2023). #StopRansomware: CL0P ransomware gang exploits CVE-2023-34362 MOVEit vulnerability (Advisory AA23-158A). <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a>
- [16] Fang, R., Bindu, R., Gupta, A., & Kang, D. (2024). LLM agents can autonomously exploit one-day

- vulnerabilities (arXiv:2404.08144). <https://doi.org/10.48550/arXiv.2404.08144>
- [17] Federal Bureau of Investigation. (2025). Internet Crime Report 2024. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2024_IC3_Report.pdf
- [18] GitHub Advisory Database. (2024, March 29). CVE-2024-3094: Malicious code was discovered in the upstream tarballs of xz (GHSA-rxwq-x6h5-x525). <https://github.com/advisories/GHSA-rxwq-x6h5-x525>
- [19] Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. In *International Conference on Learning Representations (ICLR 2015)*. <https://doi.org/10.48550/arXiv.1412.6572>
- [20] Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), 438–457. <https://doi.org/10.1145/581271.581274>
- [21] Greenberg, A. (2019). Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. *Doubleday*.
- [22] Greshake, K., Abdelnabi, S., Mishra, S., Endres, C., Holz, T., & Fritz, M. (2023). Not what you've signed up for: Compromising real-world LLM-integrated applications with indirect prompt injection. In *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security (AISec '23)* (pp. 79–90). <https://doi.org/10.1145/3605764.3623985>
- [23] Help Net Security. (2026, March 24). Attackers are handing off access in 22 seconds, *Mandiant finds*. <https://www.helpnetsecurity.com/2026/03/24/mandiant-m-trends-2026-report/>
- [24] Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the 2009 New Security Paradigms Workshop* (pp. 133–144). ACM. <https://doi.org/10.1145/1719030.1719050>
- [25] HIPAA Journal. (2025). Change Healthcare responding to cyberattack [Continuously updated report]. <https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/>
- [26] HIPAA Journal. (2026). Global data breach cost rises 12% to almost \$5 million. <https://www.hipaajournal.com/2026-cost-data-breach-study-ibm/>
- [27] Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains [White paper]. *Lockheed Martin Corporation*. [https://www.lockheedmartin.com/content/dam/lockheed](https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf)
- [28] IEPL Corporate Communication, Indorama-Nigeria, *Impact In-House Magazine*, 2019, www.indorama.com
- [29] IBM Security. (2023). Cost of a Data Breach Report 2023 (with the Ponemon Institute). *IBM Corporation*.
- [30] IBM. (2025, July 30). IBM report: 13% of organizations reported breaches of AI models or applications, 97% of which reported lacking proper AI access controls [Press release; Cost of a Data Breach Report 2025]. <https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls>
- [31] IBM. (2026a). Cost of a Data Breach Report 2026 (with the Ponemon Institute). <https://www.ibm.com/reports/data-breach>
- [32] IBM. (2026b, July 29). IBM study: One in four malicious breaches are AI-enabled, costing companies \$6 million on average [Press release]. <https://newsroom.ibm.com/2026-07-29-ibm-study-one-in-four-malicious-breaches-are-ai-enabled,-costing-companies-6-million-on-average>
- [33] International Telecommunication Union. (2024a). Global Cybersecurity Index 2024 (5th ed.). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf
- [34] International Telecommunication Union. (2024b, September 12). Countries strengthening cybersecurity efforts, but increased action still required [Press release]. <https://www.itu.int/en/mediacentre/Pages/PR-2024-09-10-Global-Cybersecurity-Index.aspx>
- [35] INTERPOL. (2025a). Africa Cyberthreat Assessment Report 2025 (4th ed.). https://www.interpol.int/content/download/23094/file/INTERPOL_Africa_Cyberthreat_Assessment_Report_2025.pdf
- [36] INTERPOL. (2025b, December 19). 574 arrests and USD 3 million recovered in coordinated cybercrime operation across Africa. <https://www.interpol.int/en/News-and-Events/News/2025/574-arrests-and-USD-3-million-recovered-in-coordinated-cybercrime-operation-across-Africa>
- [37] INTERPOL. (2026, August 3). INTERPOL report finds AI linked to more than half of cybercrime in Africa. <https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-finds-AI-linked-to-more-than-half-of-cybercrime-in-Africa>

- [38] ISC2. (2024, September 11). Growth of cybersecurity workforce slows in 2024 as economic uncertainty persists [2024 ISC2 Cybersecurity Workforce Study]. <https://www.isc2.org/Insights/2024/09/ISC2-Publishes-2024-Cybersecurity-Workforce-Study-First-Look>
- [39] ISC2. (2025). 2025 ISC2 Cybersecurity Workforce Study. <https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study>
- [40] KPMG Nigeria. (2023). The Nigeria Data Protection Act 2023. <https://kpmg.com/ng/en/home/insights/2023/09/the-nigeria-data-protection-act-2023.html>
- [41] Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77–81. <https://doi.org/10.1080/1097198X.2019.1603527>
- [42] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3), 49–51. <https://doi.org/10.1109/MSP.2011.67>
- [43] Mandiant. (2025). M-Trends 2025. Google Cloud. <https://services.google.com/fh/files/misc/m-trends-2025-en.pdf>
- [44] Mandiant. (2026). M-Trends 2026: Executive edition. Google Cloud. <https://services.google.com/fh/files/misc/m-trends-2026-executive-edition-en.pdf>
- [45] Microsoft. (2024, July 20). Helping our customers through the CrowdStrike outage. <https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/>
- [46] Ministry of Communications and Digitalisation, Ghana. (2024, September 16). Ghana ranked Tier 1 status in latest ITU Global Cybersecurity Index. <https://moc.gov.gh/2024/09/16/ghana-ranked-tier-1-status-in-latest-itu-global-cybersecurity-index/>
- [47] Mondaq. (2024). The National Assembly amends the Cybercrimes (Prohibition, Prevention, etc.) Act. <https://www.mondaq.com/nigeria/security/1466724/the-national-assembly-amends-the-cybercrimes-prohibition-prevention-etc-act>
- [48] Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *Journal of Economic Perspectives*, 23(3), 3–20. <https://doi.org/10.1257/jep.23.3.3>
- [49] Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5), 38–41. <https://doi.org/10.1109/MSP.2018.3761723>
- [50] Nairametrics. (2024a, May 8). Explainer: Is CBN’s cybersecurity levy 0.5% or 0.005%? <https://nairametrics.com/2024/05/08/is-cbns-cybersecurity-levy-0-5-or-0-005/>
- [51] Nairametrics. (2024b, September 13). ITU lists Nigeria among tier-3 countries in Global Cybersecurity Index 2024. <https://nairametrics.com/2024/09/13/itu-lists-nigeria-among-tier-3-countries-in-global-cybersecurity-index-2024/>
- [52] Nairametrics. (2024c, May 14). Federal Executive Council suspends cyber security levy, to undergo “some form of review”. <https://nairametrics.com/2024/05/14/federal-executive-council-suspends-cyber-security-levy/>
- [53] National Audit Office. (2017, October 27). Investigation: WannaCry cyber attack and the NHS. <https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/>
- [54] National Institute of Standards and Technology. (2024a). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). <https://doi.org/10.6028/NIST.CSWP.29>
- [55] National Institute of Standards and Technology. (2024b). Module-lattice-based key-encapsulation mechanism standard (FIPS 203). <https://doi.org/10.6028/NIST.FIPS.203>
- [56] National Institute of Standards and Technology. (2024c). Module-lattice-based digital signature standard (FIPS 204). <https://doi.org/10.6028/NIST.FIPS.204>
- [57] National Institute of Standards and Technology. (2024d). Stateless hash-based digital signature standard (FIPS 205). <https://doi.org/10.6028/NIST.FIPS.205>
- [58] National Vulnerability Database. (2021). CVE-2021-44228. NIST. <https://nvd.nist.gov/vuln/detail/CVE-2021-44228>
- [59] Nigeria Data Protection Commission. (n.d.). About us. <https://ndpc.gov.ng/about-us/>
- [60] Perrow, C. (1999). Normal accidents: Living with high-risk technologies (Updated ed.). Princeton University Press.
- [61] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). *National Institute of Standards and Technology*. <https://doi.org/10.6028/NIST.SP.800-207>
- [62] Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, 63(9), 1278–1308. <https://doi.org/10.1109/PROC.1975.9939>
- [63] Security Boulevard. (2026, August). How much does a data breach cost? *IBM’s 2026 report puts the US average at \$11.5 million.*

- <https://securityboulevard.com/2026/08/how-much-does-a-data-breach-cost-ibms-2026-report-puts-the-us-average-at-11-5-million/>
- [64] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509. <https://doi.org/10.1137/S0097539795293172>
- [65] Slayton, R. (2017). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security*, 41(3), 72–109. https://doi.org/10.1162/ISEC_a_00267
- [66] Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- [67] SolarWinds Corporation. (2020, December 14). Form 8-K: Current report. *U.S. Securities and Exchange Commission*. <https://www.sec.gov/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm>
- [68] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *2010 IEEE Symposium on Security and Privacy* (pp. 305–316). *IEEE*. <https://doi.org/10.1109/SP.2010.25>
- [69] Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2020). MITRE ATT&CK: Design and philosophy (Revised ed.). *The MITRE Corporation*. <https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy>
- [70] TechHive Advisory. (2024). Nigeria Cybercrimes (Prohibition, Prevention, etc.) Act amendment: Charting future direction. <https://www.techhiveadvisory.africa/insights/nigeria-cybercrimes-prohibition-prevention-etc-act-amendment-charting-future-direction>
- [71] Torracco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, 4(3), 356–367. <https://doi.org/10.1177/1534484305278283>
- [72] United States Department of Justice. (2021, June 7). Department of Justice seizes \$2.3 million in cryptocurrency paid to the ransomware extortionists Darkside. <https://www.justice.gov/opa/pr/departments-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>
- [73] Verizon. (2025). 2025 Data Breach Investigations Report: Executive summary. <https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf>
- [74] Verizon. (2026). 2026 Data Breach Investigations Report. <https://www.verizon.com/business/resources/Td15/reports/2026-dbir-data-breach-investigations-report.pdf>
- [75] World Economic Forum. (2026, January 12). Global Cybersecurity Outlook 2026 (in collaboration with Accenture). <https://www.weforum.org/publications/global-cybersecurity-outlook-2026/>

Citation of this Article:

Dimie Nwankwe, & Boye Azibolelia Frederick. (2026). How Secure Are We? A Critical Assessment of the Global Cybersecurity Posture in an Era of Artificial Intelligence, Cloud Dependence and Interconnected Critical Infrastructure. *International Current Journal of Engineering and Science (ICJES)*, 5(10), 13-32. Article DOI: <https://doi.org/10.47001/ICJES/2026.510003>
