International Journal of Multidisciplinary Research and Growth Evaluation.

BYOD Adoption and Information-Security Risk in University Administrative Offices: Evidence from Nigerian Federal Universities

Virginia Ochanya Onche [1*], Mayokun Philips Adegbite [2], Chuks Sunday Ogbonna [3]
[1] Department of Educational Management, Faculty of Education, University of Ibadan, Nigeria
[2] Oshawa Power and Utilities Corporation, Canada
[3] Wellworks Ohio University, Athens

* Corresponding Author: **Virginia Ochanya Onche**

Article Info

ISSN (online): 2582-7138
Impact Factor: 5.307 (SJIF)
Volume: 04
Issue: 06
November-December 2023
Received: 25-10-2023
Accepted: 22-11-2023
Published: 25-12-2023
Page No: 1549-1563

Abstract
The proliferation of personally owned smartphones, tablets and laptops within institutional workspaces has reshaped the perimeter of organisational information assets, dissolving the historical distinction between sanctioned enterprise endpoints and consumer-grade devices. In Nigerian federal universities, administrative offices increasingly tolerate or implicitly encourage staff to perform sensitive tasks, including student record processing, financial reconciliation, examination workflows and human-resources transactions, on devices that are not centrally provisioned. This study interrogates the convergence of consumer device adoption and the cybersecurity exposure of administrative units within the federal university subsystem, examining how device heterogeneity, weak enforcement of mobile-device-management protocols, intermittent power, ageing campus network architectures and limited security awareness culminate in a markedly elevated risk profile. Drawing on protection-motivation theory, the deterrence framework and the unified theory of acceptance and use of technology, the review synthesises evidence from peer-reviewed literature, regulatory documentation and Africa-focused empirical work to argue that the consumerisation of computing within Nigerian public higher education has outpaced the institutional capacity to govern it. The analysis identifies five interlocking risk domains: device-layer vulnerabilities, network-layer exposure, application-layer leakage, governance-policy fragmentation and user-behaviour deficits. It further contends that the absence of binding ICT-security frameworks tailored to the operational realities of federal universities has created a permissive environment for credential theft, unauthorised data exfiltration and ransomware contamination of institutional records. The paper closes by advancing a layered, context-sensitive risk-mitigation architecture that integrates technical controls, policy reform, awareness pedagogy and institutional governance, and outlines an agenda for empirical inquiry capable of generating actionable evidence for university administrators, regulators and policymakers operating within Nigeria's federal higher education subsystem.

DOI: https://doi.org/10.54660/.IJMRGE.2023.4.6.1549-1563

Keywords: consumerisation of IT, information-security risk, federal universities, mobile device management, policy compliance, Nigerian higher education

1. Introduction

The arrival of inexpensive smartphones, ultraportable laptops and ubiquitous cellular data in the second decade of the twenty-first century recast the relationship between the worker and the workspace, displacing the centrally provisioned desktop and dissolving the perimeter on which enterprise security architectures had long relied (Disterer & Kleiner, 2013; Miller, Voas & Hurlburt, 2012). Consumer devices, once peripheral to professional practice, became the principal interface through which information was created, transmitted and stored, prompting a sweeping reorganisation of how organisations conceive of endpoints, identity and trust (Niehaves, Köffer & Ortbach, 2012). In higher education, this transformation has been particularly conspicuous, as university staff, executives and middle-rank administrative officers have come to depend on personal devices

for tasks ranging from calendar management to the handling of student data, payroll instructions and procurement records (Patten & Harris, 2013; Steel, 2014). The accompanying shift towards what scholarship has termed the consumerisation of information technology has produced both efficiency gains and a profusion of governance dilemmas, since the security posture of an institution is now mediated by hardware, operating systems and applications selected by individual users rather than central procurement (French, Guo & Shim, 2014; Köffer, Ortbach & Niehaves, 2014). For organisations operating in jurisdictions characterised by uneven regulatory enforcement and resource-constrained information-technology departments, this displacement of authority carries especially acute consequences.

In Nigeria, the federal university subsystem occupies a strategic position within the national knowledge infrastructure, training the bulk of the country's professional workforce while custodianing voluminous personal data on students, staff and external partners (Yusuf, Maina & Dare, 2013; Mbarika *et al*., 2005). Federal universities operate under the National Universities Commission's regulatory umbrella, yet their internal administrative practices vary considerably across institutions, departments and even individual offices (Sangodoyin, Sani & Idowu, 2017). The post-pandemic acceleration of remote work, electronic correspondence and cloud-based record-keeping, observed across sectors globally, has reverberated through Nigerian higher education with notable intensity, with administrative officers increasingly conducting institutional business on private devices, often across networks of variable security maturity (Ezeh *et al*., 2022; Omotayo & Kuponiyi, 2020). The pattern is reinforced by chronic underfunding of campus information-technology services, persistent power instability and the inability of central units to provision and maintain enterprise hardware at scale (Olatokun & Ayanbode, 2008).

The risk implications of this trajectory are significant. Personally owned devices typically lack hardened configurations, are seldom enrolled in mobile-device-management platforms, may run unsupported operating systems and frequently traverse networks beyond the institution's control (Garba *et al*., 2015; Olalere *et al*., 2015). When sensitive administrative data, examination scripts, financial spreadsheets, biometric records, personnel files, is processed on such devices, the institution effectively externalises core security functions to individual users whose technical competence, motivation to comply and awareness of threat vectors are heterogeneous (Bulgurcu, Cavusoglu & Benbasat, 2010; Ifinedo, 2012). The resulting exposure includes credential theft through phishing, malware contamination via untrusted software, data loss through device theft, and breaches of confidentiality through informal data-sharing practices (Eslahi *et al*., 2014; Wang, Wei & Vangury, 2014). Recent practitioner-oriented work has further underscored how cyberadversaries increasingly target lower-resourced public institutions because they offer rich data troves alongside weaker defences (Bukhari *et al*., 2022; Adebayo, 2022).

This review situates the discussion of consumer-device-driven administrative computing within the institutional, regulatory and infrastructural realities of Nigerian federal universities. It synthesises evidence drawn from international scholarship on the consumerisation of computing, peer-reviewed work on information-security governance, regulatory pronouncements applicable to Nigerian public institutions and the modest but growing body of Africa-focused empirical research. The objective is to develop a coherent account of why personal-device practices among administrative officers should be understood not as a marginal IT-management issue but as a strategic determinant of institutional integrity. By doing so, the paper contributes to the literature on cybersecurity in resource-constrained higher-education systems and provides a foundation for subsequent empirical interrogation.

The conceptual purchase of such an inquiry is sharpened by the distinctive intersection of two trends that have, until recently, been studied in relative isolation. The first is the global trajectory of consumerisation, which has fundamentally altered the technological substrate of professional work and, in so doing, demanded a wholesale reconsideration of how organisations conceptualise the perimeter of their information assets (Disterer & Kleiner, 2013; Singh, 2012). The second is the protracted struggle of African higher-education systems to develop information-technology infrastructures of sufficient maturity to support modern administrative operations under conditions of resource scarcity (Mbarika *et al*., 2005; Ogbomo & Ogbomo, 2008). Where these trends intersect, as they do within the administrative offices of Nigerian federal universities, the conventional scholarly templates derived from well-resourced contexts cease to function as adequate guides to practice. The result is a research and policy lacuna of considerable consequence: the very institutions whose continued integrity is most strategically important to the Nigerian state are also those whose security postures are least well documented, least systematically governed and least adequately supported by sector-specific guidance. The review that follows treats this lacuna not as a peripheral inconvenience but as the central organising challenge of its argument, and the structure of its sections has been deliberately constructed to traverse the analytical terrain in a manner that produces actionable insight for practitioners while remaining methodologically rigorous and theoretically engaged (Yusuf, Maina & Dare, 2013; Yakubu & Dasuki, 2018).

The argumentative trajectory of the review reflects a deliberate sequencing in which conceptual foundations precede empirical mapping, empirical mapping precedes institutional diagnosis, and institutional diagnosis precedes prescriptive architecture. This sequencing is intended to discipline the analysis against the temptation to leap from observation to recommendation without the intervening work of synthesising mechanisms, conditions and constraints. It also serves to make the argument accessible to readers operating from different vantage points: information-security practitioners seeking guidance on operational priorities, university administrators evaluating governance choices, regulators considering sector-wide policy instruments and scholars pursuing further empirical investigation. The contribution offered is therefore not a single thesis but an integrated framework whose constituent claims are individually defended and collectively oriented toward the protection of institutional information assets in conditions where the easy assumptions of well-resourced contexts cannot be relied upon (Ifinedo, 2014; Crossler *et al*., 2014).

1.1. Background and Contextual Framing

The trajectory of personal computing in Nigerian public administration cannot be appreciated without reference to a

broader continental pattern in which the diffusion of mobile devices has substantially outpaced the maturation of organisational information-technology governance (Mbarika *et al*., 2005). Mobile phones moved from luxury to indispensable within a decade, and laptops followed a similar arc, with academic staff and administrative officers acquiring portable computing power chiefly through personal expenditure rather than institutional provisioning (Ogbomo & Ogbomo, 2008). Within federal universities, the cumulative effect has been the layering of consumer-procured devices over institutional information systems whose architectures were never designed to authenticate, monitor or sandbox heterogeneous endpoints. Administrative officers in registry, bursary, examinations, student affairs and human-resources offices routinely move data between desktop terminals, personal laptops and smartphones to navigate intermittent electricity, network unreliability and software compatibility constraints (Fasae & Adegbilero-Iwari, 2015). What began as an informal accommodation has solidified into a settled operational practice that lies almost entirely outside formal security policy. The contextual frame is further complicated by the post-pandemic normalisation of partial remote working, which has transformed what was once an episodic concession into a structural feature of administrative routine. Understanding this background is essential because the contemporary risk profile of Nigerian federal universities is not a discrete technical phenomenon but a residue of long-standing infrastructural and managerial choices whose security consequences are now becoming consequential. The path from infrastructural improvisation to systematic exposure has been gradual, but its destination is sufficiently dangerous to demand explicit, evidence-grounded scholarly attention rather than the diffuse, reactive treatment it has hitherto received within sectoral and policy discourse.

1.2. Statement of the Problem

Despite the widespread reliance of administrative units in Nigerian federal universities on personally owned devices, there exists no coherent body of evidence describing the precise scope, severity or pattern of the information-security exposures that this dependency generates. Institutional risk registers, where they exist at all, seldom capture endpoint heterogeneity, application-layer leakage or the porousness of administrative workflows that traverse personal hardware and unmanaged networks. Anecdotal reports of compromised email accounts, unauthorised disclosure of examination materials, financial fraud occasioned by credential theft and ransomware contamination of student-record databases persist, yet remain methodologically disconnected from systematic inquiry. The problem is compounded by the absence of binding, sector-wide information-security policy frameworks tailored to the realities of public higher education in Nigeria. Existing national and international standards either presume operational and budgetary capabilities that federal universities do not possess or are framed at levels of abstraction that fail to translate into actionable controls within the administrative environments where the bulk of sensitive data are processed. The challenge is not merely an absence of documentation but the asymmetry between adversaries who increasingly target the public sector and institutions whose defensive postures lag well behind the threats they face. Without an empirically grounded account of how device adoption interacts with policy gaps, infrastructural fragility and human factors, university administrators, regulators and security practitioners are compelled to formulate interventions on the basis of conjecture rather than evidence. The persistence of this evidentiary deficit is itself a contributor to institutional vulnerability. It permits the slow normalisation of practices whose security implications are imperfectly understood, attenuates the urgency with which leadership engages with cybersecurity questions and forecloses the possibility of a defensible allocation of scarce resources to controls that would deliver the greatest marginal reduction in risk.

1.3. Significance of the Study

The case for sustained scholarly attention to the security implications of consumer-device adoption in Nigerian federal university administration rests on a confluence of institutional, regulatory and societal considerations. Federal universities collectively process the personal and academic records of millions of Nigerians, manage financial flows of national consequence and maintain the documentary infrastructure on which professional qualifications are predicated. A compromise of these records, whether by external adversaries or insiders exploiting weak controls, would not merely inconvenience individual institutions but reverberate through labour markets, regulatory bodies and the credentialing ecosystems on which graduates depend. The significance of disciplined inquiry into administrative-office security practices therefore extends well beyond the campus perimeter. The findings of such inquiry are also of significance to policy. The National Universities Commission, the Nigerian Communications Commission and the Office of the National Security Adviser have each issued instruments touching upon cybersecurity in critical sectors, yet none have produced a binding, operationalisable framework for university administrative offices. A rigorous review of the conditions under which personal devices become security liabilities is thus a precondition for informed regulatory action, providing the analytical foundation on which sector-specific guidelines, audit protocols and capacity-building investments can be designed. The study is further significant to international comparative scholarship on cybersecurity in higher education. Much of the existing literature on personal-device adoption is grounded in the experiences of well-resourced institutions in Europe, North America and parts of Asia, where mobile-device-management platforms, robust network infrastructure and mature compliance cultures provide a baseline against which exceptions can be analysed. The Nigerian federal university context inverts these baselines and therefore offers a critical site for theory-testing, contributing evidence on how widely cited frameworks perform in environments of acute resource constraint.

1.4. Aim, Objectives, and Scope of the Review

The overarching aim of this review is to develop a coherent, evidence-informed account of the convergence between the use of personally owned digital devices and the information-security posture of administrative offices within Nigerian federal universities. The review proceeds from the premise that this convergence is not adequately addressed by either the international literature on consumerisation of computing or the regional literature on information-technology adoption in African higher education, and seeks to bridge these strands by sustained synthetic engagement with both. To realise this

aim, the review pursues four interlocking objectives. The first is to characterise the conceptual terrain by which personal-device use within institutional settings has been theorised, with particular attention to the analytic frameworks most consequential for security inquiry. The second is to map the empirical evidence concerning the threat landscape that personal devices generate when integrated into administrative workflows, drawing on both global and African-context studies. The third is to interrogate the institutional, regulatory and infrastructural conditions specific to Nigerian federal universities that mediate the relationship between device adoption and risk exposure. The fourth is to articulate the elements of a layered, context-sensitive mitigation architecture that responds to the realities of federal universities rather than presuming operational capacities they do not possess. The scope of the review is bounded in three respects. It focuses on administrative offices, including registry, bursary, examinations, student affairs, human resources and procurement, rather than on academic teaching and research environments, whose risk profiles differ qualitatively. It is geographically delimited to federal universities operating within Nigeria, although evidence from comparable jurisdictions is engaged for analytical leverage. It adopts a synthesis methodology that privileges peer-reviewed literature and authoritative regulatory documentation while incorporating practitioner-oriented work where this clarifies operational realities.

2. Conceptual Foundations of Personal-Device Practice in Institutional Settings

The intellectual scaffolding for the contemporary analysis of personal-device use in organisational contexts emerged from a confluence of scholarly traditions, including the consumerisation-of-information-technology literature, the diffusion-of-innovations paradigm and the broader sociotechnical critique of organisational computing (Niehaves, Köffer & Ortbach, 2012; Köffer, Ortbach & Niehaves, 2014). The term consumerisation, in its present usage, denotes the trajectory by which technologies developed and refined for individual consumer markets, smartphones, cloud storage services, instant-messaging applications, eventually permeate organisational settings, displacing or supplementing artefacts originally selected through formal enterprise procurement (Disterer & Kleiner, 2013). When consumerisation crosses the threshold at which employees use their own devices for organisational tasks, scholars have variously labelled the practice bring-your-own-device, choose-your-own-device or use-your-own-device, with significant analytic differences across these designations (French, Guo & Shim, 2014; Singh, 2012).

Theoretical engagement with personal-device practice has drawn substantially on the unified theory of acceptance and use of technology, the protection-motivation theory and the general deterrence theory, each illuminating a distinct facet of the phenomenon. The unified theory of acceptance and use of technology and its extensions explain why employees adopt personal devices for work in the first place, foregrounding performance expectancy, effort expectancy, social influence and facilitating conditions (Weeger *et al*., 2020). The protection-motivation theory, in turn, illuminates why users engage in, or fail to engage in, protective behaviours, conceptualising compliance as a function of perceived threat severity, threat vulnerability, response efficacy and self-efficacy (Crossler *et al*., 2014; Ifinedo, 2012; Vance, Siponen & Pahnila, 2012). The general deterrence theory contributes a complementary account in which compliance is shaped by the perceived certainty and severity of sanction (D'Arcy, Hovav & Galletta, 2009; Herath & Rao, 2009).

The sociotechnical critique of organisational computing further insists that personal-device practice is not reducible to individual preferences but reflects negotiated arrangements between users, managers and infrastructure (Dhillon & Backhouse, 2001; Furnell & Clarke, 2012). The implications for higher-education administrative offices are direct. Administrative practice in resource-constrained universities is shaped by chronic infrastructural deficiencies, intermittent electricity, slow institutional procurement cycles and limited information-technology support, all of which incentivise the appropriation of personal devices as a coping strategy (Sangodoyin, Sani & Idowu, 2017; Olatokun & Ayanbode, 2008). The conceptual frameworks above therefore require local recalibration to capture how facilitating conditions interact with infrastructural fragility, how threat perceptions are formed in environments with limited cybersecurity public discourse, and how deterrence operates when policy enforcement mechanisms are weak or inconsistent. This recalibration is the analytic task taken up in subsequent sections of the review.

It is also instructive to recognise that personal-device practice operates within an emerging analytic conversation that situates endpoint heterogeneity alongside broader questions of cloud-service adoption, data-pipeline management and analytics governance (Akindemowo *et al*., 2021; Akindemowo *et al*., 2022). Where institutional data increasingly flow between local devices, hybrid cloud workloads and external platforms, the boundaries of the organisational endpoint blur in ways that complicate traditional perimeter defences. This convergence has direct implications for the security posture of administrative offices in Nigerian federal universities, where ad hoc cloud-storage practices, the use of consumer messaging applications for sharing official documentation and the reliance on personal email accounts for institutional correspondence are routine. Theorising personal-device practice within this expanded analytic frame is thus essential to producing security guidance that responds to actual operational realities rather than idealised models of bounded enterprise endpoints (Eboseremen *et al*., 2022).

A further conceptual dimension deserves explicit attention: the asymmetric distribution of agency between users and institutions in personal-device contexts. When the device is institutionally provisioned, the institution retains a presumptive authority over its configuration, its acceptable use and its disposal. When the device is privately owned, that authority must be negotiated, often through policy instruments whose legitimacy is contested by users who regard the device as fundamentally theirs (Putri & Hovav, 2014; Mohamed & Ahmad, 2012). This asymmetry shapes the empirical realities of policy compliance, the ethical dimensions of monitoring and the contractual frameworks that govern employer–employee relationships in the contemporary workplace. It also unsettles the inherited theoretical vocabulary, which presumes that organisational property and organisational data are coextensive — an assumption that personal-device practice systematically violates. A satisfactory conceptual treatment must therefore engage with the renegotiation of authority, the contestation of

legitimate monitoring and the construction of trust that personal-device deployment makes unavoidable. For administrative offices in Nigerian federal universities, these conceptual concerns translate into concrete questions about whose consent is required for the monitoring of personal devices, what categories of data may legitimately be processed on them and how disputes between officers and institutions over device-related practices should be adjudicated. Without explicit attention to these matters, the policy frameworks that institutions adopt risk being either unenforceable or perceived as illegitimate, undermining the very compliance they are designed to secure (Bulgurcu, Cavusoglu & Benbasat, 2010; Lebek, Degirmenci & Breitner, 2013).

3. The Information-Security Threat Landscape Associated with Personal-Device Use

The information-security threat landscape associated with personal-device use is empirically rich and analytically multidimensional. At the device layer, vulnerabilities arise from outdated operating systems, unpatched applications, weak authentication credentials and the absence of disk encryption (Garba *et al*., 2015; Olalere *et al*., 2015). Personally owned smartphones and laptops are frequently configured with permissions and applications that would not pass an enterprise security review, including side-loaded software, jailbroken or rooted firmware and synchronisation tools that propagate documents to consumer cloud accounts without organisational oversight (Eslahi *et al*., 2014; Imgraben, Engelbrecht & Choo, 2014). The device layer is also the locus of physical security failures: theft, loss and surreptitious access have repeatedly been documented as principal vectors of data exposure in personal-device deployments (Wang, Wei and Vangury, 2014; Souppaya & Scarfone, 2013).

At the network layer, personal devices traverse a wide variety of connectivity environments, many of which fall outside the institution's observational and defensive purview. Hotel Wi-Fi networks, public hotspots, residential broadband and tethered cellular connections each present distinct adversarial conditions, ranging from man-in-the-middle interception to malicious access-point impersonation (Alotaibi & Almagwashi, 2018). The proliferation of unencrypted protocols, weak certificate validation in mobile applications and the limited adoption of virtual private networks aggravates the exposure (Abomhara & Køien, 2015). When administrative officers in Nigerian federal universities transmit student records, examination materials or financial spreadsheets across such networks, the data become accessible to a far broader threat surface than would obtain on enterprise-managed connections (Ali, Qureshi & Abbasi, 2015).

At the application layer, threats arise from the diverse ecosystems of mobile applications that personal devices host. Many applications request, and obtain, broad permissions to access contacts, files and network resources, providing a covert channel through which institutional data can leak into third-party hands (Miller, Voas & Hurlburt, 2012). Cloud storage, messaging and document-sharing services compound the issue, with informal practices, sharing institutional records via consumer instant-messaging apps, storing examination files on personal cloud drives, opening up administrative workflows to opaque and weakly governed external infrastructures (Wani, Mendoza & Gray, 2020). The risk is amplified by the increasing sophistication of mobile malware, which now targets credentials, banking applications and identity tokens through techniques such as overlay attacks, accessibility-service abuse and supply-chain compromise (Yang *et al*., 2013).

At the governance layer, the threat landscape is shaped by the absence or inadequacy of policy instruments that would prescribe how personal devices may be used for institutional work, what data may be processed on them, and how access is provisioned, monitored and revoked (Romer, 2014; Zahadat *et al*., 2015). Where governance is weak, technical controls operate in isolation from organisational expectations, and human factors, motivation, awareness, perceived legitimacy, become the principal determinants of security outcomes (Bulgurcu, Cavusoglu & Benbasat, 2010; Soomro, Shah & Ahmed, 2016). At the user-behaviour layer, the threat landscape is shaped by the practices, beliefs and habits of administrative officers themselves, including the willingness to share devices with family members, the use of weak or reused passwords, the disregard of security warnings and the tendency to disable inconvenient protections (Schultz, 2005; Beautement, Sasse & Wonham, 2008; D'Arcy, Hovav & Galletta, 2009). Recent work has demonstrated that artificial intelligence-driven detection mechanisms, while promising, presuppose levels of telemetry and instrumentation that resource-constrained institutions seldom achieve, leaving the bulk of administrative endpoints in an effectively unmonitored state (Bukhari *et al*., 2022; Ajayi *et al*., 2022).

An additional dimension of the threat landscape that warrants explicit treatment is the temporal one. Threats associated with personal-device use are not static; they evolve in tempo with the broader evolution of the threat ecosystem, the deployment of new operating systems and applications and the diffusion of attack tooling that adversaries can deploy at progressively lower cost (Chigada & Daniels, 2021). The contemporary period has witnessed the maturation of ransomware-as-a-service offerings, the commoditisation of phishing kits and the proliferation of credential-stealing malware capable of harvesting passwords, browser cookies and authentication tokens within seconds of execution. Administrative officers in Nigerian federal universities therefore face a threat surface whose characteristics change faster than the institutional capacity to monitor, document and respond. A purely static map of threats is consequently of limited operational value; what is required is an analytic posture that recognises threats as moving targets and that builds institutional adaptability into the very architecture of defence. The temporal dimension also intersects with the resource-allocation question, since the controls that suffice today may prove inadequate within a short horizon, demanding investments in capabilities that can be scaled as threats evolve rather than purchases of fixed, one-off solutions whose obsolescence is preordained. The aggregate implication is sobering: federal universities cannot defer the conversation about personal-device exposure, because the longer the deferral, the greater the accumulated risk and the more entrenched the practices that adversaries will inevitably exploit. This recognition shapes much of the architectural reasoning advanced in later sections of the present review (Filani *et al*., 2022; Adebayo, 2022).

4. Higher Education in Nigeria and the Federal University Subsystem

Nigerian higher education is organised through a tripartite structure of federal, state and private institutions, with federal universities occupying a distinctive position by virtue of their direct funding through the federation account, their regulatory subordination to the National Universities Commission and their historical role as flagship institutions of the country's tertiary system (Yusuf, Maina & Dare, 2013). Federal universities are charged with delivering undergraduate, postgraduate and professional programmes; conducting research of national and global relevance; and providing community service across an array of disciplinary domains (Mbarika *et al*., 2005). They operate alongside a smaller but rapidly growing number of state and private universities, with which they share regulatory oversight but from which they differ in funding model, infrastructural endowment and institutional culture.

Administrative offices within federal universities perform an indispensable but often under-theorised function. The registry oversees student admissions, records and certification; the bursary manages financial flows including tuition collections, salary disbursements and project accounts; the examinations office coordinates assessment cycles and the secure handling of question papers and scripts; the human-resources office maintains personnel records and processes promotions and disciplinary actions; and the procurement unit conducts tendering, contract management and supplier engagement (Olatokun & Ayanbode, 2008). Each of these offices processes information whose confidentiality, integrity or availability is consequential, and each interacts daily with a heterogeneous mix of internal stakeholders, external partners and regulatory authorities.

The information-technology environment of federal universities is shaped by a combination of central provisioning, faculty-level autonomy and the informal innovation of individual offices. Most federal universities maintain a central information and communications technology unit responsible for institutional networks, electronic mail services, learning-management platforms and selected administrative systems (Sangodoyin, Sani & Idowu, 2017). However, the resourcing of these units has historically lagged behind operational demand, with the result that core administrative functions are frequently supplemented by personal hardware, free or freemium software services and ad hoc workflows developed by officers in response to local exigencies (Adejo *et al*., 2018). The proliferation of these workarounds reflects ingenuity in the face of constraint but simultaneously expands the information-security threat surface in ways that the central information-technology unit cannot readily monitor or remediate (Yakubu & Dasuki, 2018).

The post-pandemic acceleration of digital working has further reshaped this environment, with administrative officers increasingly conducting institutional business from home, processing student communications via personal email accounts, attending meetings on personal devices and storing official files on consumer cloud services (Ezeh *et al*., 2022; Omotayo & Kuponiyi, 2020). This shift, while pragmatic, has institutionalised practices whose security implications were never explicitly evaluated, and has compressed the temporal window within which universities might have negotiated a transition with adequate procedural safeguards (Frempong, Ifenatuora & Ofori, 2020). Practitioner literature on data-pipeline modernisation and risk-monitoring dashboards underscores the magnitude of the governance gap that has thereby opened, particularly for public institutions whose enterprise data architectures remain partial and uneven (Filani *et al*., 2022; Moyo *et al*., 2021). The federal university subsystem accordingly enters the contemporary moment with elevated digital dependence and a security infrastructure that has not kept pace, making it a particularly important site of inquiry.

A further analytic point about the federal university subsystem concerns its strategic position within the national knowledge economy. The data assets curated by federal universities are not merely operational records; they constitute a foundational substrate of the country's human-capital infrastructure, supplying the verifiable credentials, performance histories and demographic information on which employers, professional bodies, scholarship administrators and regulatory authorities depend. A compromise of these assets, whether by external adversaries, internal opportunists or accidental disclosure, propagates through downstream systems whose dependencies on university-issued records are seldom appreciated until a breach occurs. The federal university subsystem therefore occupies a position analogous to that of critical-infrastructure operators in other sectors, and the security expectations placed upon it should reflect this analogy rather than the more relaxed posture commonly associated with educational institutions. Recognising this strategic position is essential for any analysis of personal-device exposure within the subsystem, because the consequences of compromise are not bounded by the institutional perimeter but reverberate through the wider ecosystem of Nigerian economic, professional and civic life. This recognition also illuminates the asymmetry between the value of the assets at stake and the modest resources currently directed at protecting them, an asymmetry whose persistence is increasingly difficult to justify on policy or operational grounds (Yusuf, Maina & Dare, 2013; Sangodoyin, Sani & Idowu, 2017).

The structural distinctiveness of the federal university subsystem also conditions the receptivity of these institutions to externally derived governance models. Federal universities operate within a unique web of constitutional autonomy, public-service regulation and union representation that constrains the speed and form of administrative reform (Yusuf, Maina & Dare, 2013; Adejo *et al*., 2018). Reform programmes imported wholesale from corporate or technology-sector contexts have historically encountered resistance grounded in legitimate concerns about academic freedom, employment security and institutional self-determination, and they have rarely sustained themselves beyond the tenure of the senior officers who introduced them. A durable approach to personal-device governance must therefore engage with these institutional realities rather than treat them as obstacles to be circumvented, recognising that the federal university operates simultaneously as a workplace, a regulated public entity and a community of inquiry whose internal compact must be honoured even as security requirements are met (Mbarika *et al*., 2005; Yakubu & Dasuki, 2018).

5. Drivers of Personal-Device Adoption in Administrative Workflows

The adoption of personally owned devices in university administrative workflows is driven by a constellation of

factors that operate at the individual, institutional and infrastructural levels. At the individual level, perceived performance gains feature prominently. Administrative officers report that personal devices, especially smartphones, enable continuous responsiveness to institutional demands, accommodate work at irregular hours and reduce the friction of moving between physical workstations (Weeger *et al*., 2020; Doargajudhur & Dell, 2019). Familiarity with personal devices, accumulated over years of consumer use, reduces the cognitive effort of task execution relative to institutional terminals whose interfaces, performance profiles and software stacks vary unpredictably (Lee *et al*., 2017). The hedonic dimension is also relevant: officers derive satisfaction from working on devices they have selected, customised and invested in, and this affective relationship influences their willingness to integrate the device into their professional practice (Hovav & Putri, 2016).

At the institutional level, the absence of consistent, well-provisioned enterprise endpoints creates conditions under which the adoption of personal devices is functionally inevitable. Administrative offices in many Nigerian federal universities operate with desktop terminals that are ageing, irregularly maintained and intermittently unavailable due to power interruptions (Olatokun & Ayanbode, 2008; Sangodoyin, Sani & Idowu, 2017). The procurement and replacement of institutional hardware proceeds on cycles that lag well behind the depreciation of consumer technology, and the budgetary pressure on universities has tightened over time. Faced with the choice between deferring tasks indefinitely and completing them on a personal device, administrative officers, judged by performance metrics that presuppose timely execution, predictably choose the latter (Fasae & Adegbilero-Iwari, 2015). The institutional response has often been an informal accommodation of personal-device use, with neither explicit prohibition nor positive policy framing.

At the infrastructural level, the broader Nigerian environment shapes adoption in distinctive ways. The expansion of cellular data coverage and the relative affordability of entry-level smartphones have made personal mobile computing accessible to a wide swath of the administrative workforce (Mbarika *et al*., 2005). Cloud-based productivity suites, freemium messaging applications and consumer file-sharing services are easily integrated into personal workflows without negotiation with the institutional information-technology unit. The result is a parallel infrastructure, partly visible to central administration but largely operated through private accounts and personal subscriptions, that has become indispensable to the conduct of routine administrative work (Adejo *et al*., 2018; Yakubu & Dasuki, 2018).

The drivers are reinforced by post-pandemic operational changes that normalised remote and hybrid working. The expansion of virtual meetings, the routinisation of digital correspondence and the migration of selected administrative processes to web-based platforms each create demands that personal devices are better positioned to satisfy than ageing institutional terminals (Omotayo & Kuponiyi, 2020; Frempong, Ifenatuora & Ofori, 2020). Recent practitioner accounts of healthcare digitisation document a comparable dynamic, in which legacy systems and pandemic-era flexibility produced enduring shifts in endpoint composition that subsequent governance has struggled to consolidate (Ezeh *et al*., 2022). A realistic account of why personal devices have come to occupy a central place in Nigerian federal university administration must therefore weigh individual preferences, institutional shortfalls and macro-infrastructural conditions in concert, recognising that any intervention which targets only one of these levels is unlikely to alter the trajectory in any durable way.

A further set of drivers operates through social and organisational dynamics that are less frequently foregrounded in the literature but exert appreciable influence on adoption trajectories. Peer practice within administrative units functions as a powerful normative signal: where senior officers conspicuously rely on personal smartphones to process correspondence, junior colleagues infer that such practice is sanctioned and adopt it without seeking explicit authorisation (Ifinedo, 2014; Tu & Yuan, 2014). The absence of countervailing institutional messaging reinforces the inference, and the resulting equilibrium is one in which personal-device use is woven into the routine fabric of administrative work without any episode of formal decision. The dynamic is intensified by the migration of communication into messaging platforms whose default expectation is continuous availability, and which administrative officers cannot plausibly meet through institutional terminals alone (Doargajudhur & Dell, 2019; Adesemowo, Von Solms & Botha, 2016). A complementary driver lies in the perceived inadequacy of institutional support channels. When administrative officers encounter performance problems with enterprise endpoints, the latency between fault report and resolution often extends across days or weeks, during which the immediate workload continues to accumulate (Olatokun & Ayanbode, 2008; Fasae & Adegbilero-Iwari, 2015). Personal devices, by contrast, offer immediate recourse, with users assuming responsibility for their own configuration, troubleshooting and replacement. The economic calculus, from the user's perspective, favours personal-device reliance even where the institutional expectation might be different. Recent practitioner literature on financial forecasting and operational dashboards in Nigerian and African contexts has documented analogous patterns of informal tool adoption in response to constrained institutional capacity, reinforcing the view that the drivers of personal-device practice are structural rather than incidental (Ajayi *et al*., 2022; Bukhari *et al*., 2022; Filani *et al*., 2022; Sakyi *et al*., 2022).

6. Vulnerabilities and Attack Surfaces in Administrative Office Environments

Administrative office environments in Nigerian federal universities present a distinctive constellation of vulnerabilities that follows from the intersection of the broader threat landscape with the specific operational realities of the sector. The first cluster of vulnerabilities arises from the heterogeneity of devices in active use. A single registry or bursary office may host desktop computers running outdated operating systems alongside personal laptops, tablets and smartphones spanning multiple vendors, firmware generations and software environments (Olalere *et al*., 2015; Wani, Mendoza & Gray, 2020). The diversity precludes uniform patching, complicates the deployment of endpoint-protection agents and renders incident response a bespoke exercise for each device, with corresponding costs in time and expertise. Where the institutional information-technology unit lacks an inventory of devices in use, even the most rudimentary risk assessment becomes infeasible.

The second cluster of vulnerabilities is rooted in identity and

access management. Administrative offices rely heavily on shared credentials, sticky-note password practices and the use of generic accounts for activities that should be individually attributable (Bulgurcu, Cavusoglu & Benbasat, 2010; Whitman & Mattord, 2018). Where multi-factor authentication has been deployed at all, it is often inconsistently applied across systems and may be circumvented through informal workarounds. The reuse of passwords across institutional and personal services, coupled with the susceptibility of personal email accounts to phishing, creates a credential-theft surface that adversaries can exploit through low-cost campaigns (Imgraben, Engelbrecht & Choo, 2014). Adversaries seeking access to institutional records routinely target the personal accounts of administrative officers as a stepping stone to institutional systems.

The third cluster relates to data flows. Administrative workflows in federal universities often involve the transfer of files between personal devices, departmental email accounts, removable storage media and central administrative systems, each transition introducing potential points of leakage (Souppaya & Scarfone, 2013). The use of consumer messaging applications and personal cloud accounts for the sharing of official documentation, including spreadsheets containing student personal data, intensifies this exposure (Garba *et al*., 2015). Data, once externalised through such channels, are effectively beyond the institution's ability to recover, audit or delete. The fourth cluster of vulnerabilities concerns physical and environmental security. Administrative offices in many federal universities operate in shared physical spaces with intermittent access controls. Personal devices used for institutional work travel daily between such offices and homes, hotels, transit and public places, where they are exposed to theft, observation and tampering (Anderson, 2008; Wang, Wei & Vangury, 2014).

A fifth cluster of vulnerabilities involves the supply chain and software ecosystem. The applications that administrative officers install on personal devices, including productivity suites, document-conversion utilities and communication tools, are sourced from a global supply chain whose security characteristics vary considerably (Abomhara & Køien, 2015). Counterfeit or modified versions of legitimate software, particularly those obtained through informal distribution channels, can contain backdoors, credential-harvesting routines and surveillance capabilities (Bukhari *et al*., 2022; Adebayo, 2022). Practitioner studies of secure data-exchange architectures highlight that institutions with weak provenance verification face elevated risks of contaminated software entering their endpoint estate (Shittu, Adeniji & Shittu, 2022; Adeniji, 2019). Considered cumulatively, these clusters define an attack surface that is large, heterogeneous and unevenly visible to the institution, with implications addressed in the sections that follow.

Beyond the discrete clusters of vulnerability already discussed, an integrative perspective draws attention to the systemic conditions under which these vulnerabilities compound. The shadow-information-technology phenomenon, in which administrative units procure, configure and operate technology outside the oversight of the central information-technology unit, has been documented across organisational settings and acquires particular prominence in the personal-device context (Crossler *et al*., 2014; Lee *et al*., 2017). In Nigerian federal universities, the shadow-information-technology footprint is sustained by the proliferation of consumer applications used for institutional purposes, the routine sharing of credentials between officers and the unmonitored installation of browser extensions, communication clients and file-synchronisation tools (Olalere *et al*., 2015; Sangodoyin, Sani & Idowu, 2017). The cumulative consequence is an institutional information environment whose true topology is opaque to those nominally responsible for its protection. The insider dimension of the attack surface deserves explicit attention. Disgruntled or coerced officers, malicious recruiters of credentials and inadvertent collaborators in social-engineering campaigns each contribute to a category of risk that purely external defences cannot address (D'Arcy, Hovav & Galletta, 2009; Herath & Rao, 2009). Where authentication is weak, audit logging is incomplete and segregation of duties is poorly enforced, the institutional capacity to detect, attribute and respond to insider-mediated incidents is correspondingly diminished (Anderson, 2008; Whitman & Mattord, 2018). The intersection of personal devices with these institutional weaknesses produces a compound exposure that exceeds the sum of its parts. Practitioner studies in adjacent sectors have similarly emphasised that institutional opacity is itself a form of vulnerability, in that it precludes the targeted application of mitigations and undermines the assurance posture on which external stakeholders ultimately depend (Bukhari *et al*., 2022; Filani *et al*., 2022; Adebayo, 2022).

7. Policy Frameworks, Governance, and Compliance Mechanisms

The governance of information security in organisations is grounded in a body of international standards and national instruments, each providing a vocabulary for risk identification, control selection and assurance. ISO/IEC 27001 articulates requirements for the establishment, operation and continuous improvement of information-security management systems, including specific guidance on the management of mobile and personal devices (ISO/IEC, 2013). The NIST Cybersecurity Framework offers a complementary model organised around the functions of identify, protect, detect, respond and recover, which translate into operational expectations for organisations seeking to manage cyber risk in a structured manner (NIST, 2014). These frameworks have been widely adopted in well-resourced jurisdictions and have shaped a sizeable practitioner literature on personal-device governance, including specific guidance from authoritative sources on mitigating the risks of consumer endpoints in enterprise settings (Souppaya & Scarfone, 2013; Zahadat *et al*., 2015).

Within Nigeria, the regulatory environment for information security has matured considerably over the past decade but remains fragmented in its application to higher education. The Nigeria Data Protection Regulation and successor data-protection instruments place duties on data controllers to protect personal information, while sectoral regulators have issued guidance on cybersecurity in banking, telecommunications and critical infrastructure (Adesina & Ayo, 2010; Adesemowo, Von Solms & Botha, 2016). Higher education, however, has not been the subject of a dedicated information-security policy instrument with operational specificity. The National Universities Commission's guidance on information and communications technology in universities addresses governance, infrastructure and academic uses but does not extend in detail to administrative-

office security practices, mobile-device management or personal-device-related risk (Yusuf, Maina & Dare, 2013; Sangodoyin, Sani & Idowu, 2017).

At the institutional level, the picture is uneven. Some federal universities have adopted information and communications technology policies that include statements on acceptable use, password discipline and data protection, but few have developed comprehensive personal-device frameworks comparable to those described in the international literature on the subject (Disterer & Kleiner, 2013; Romer, 2014). Where policies exist, enforcement is frequently undermined by limited monitoring capacity, the absence of formal sanctioning processes and the political complexities of disciplining senior officers (Ifinedo, 2014; Tu & Yuan, 2014). Compliance is further constrained by the absence of regular awareness training, the limited reach of internal audit and the discretion that administrative units enjoy in shaping their own operational practices (Olusegun & Ithnin, 2013; Yaokumah, 2014).

The governance challenge is therefore not merely the formulation of policy but the integration of policy with technical controls, awareness pedagogy and managerial accountability. Effective personal-device governance requires that institutions distinguish between high-risk and lower-risk administrative functions, prescribe device-eligibility criteria, mandate baseline technical configurations and define the conditions under which personal devices may access institutional resources (Crossler *et al*., 2014; Lee *et al*., 2017). It also requires explicit attention to the legal and ethical dimensions of monitoring personal devices used for work, including issues of privacy, consent and proportionality (Mohamed & Ahmad, 2012; Lebek, Degirmenci & Breitner, 2013). For Nigerian federal universities operating under constrained budgets, the design of governance instruments must be sensitive to the realities of implementation, prioritising the controls most likely to deliver meaningful risk reduction while remaining operationally tractable (Pahnila, Siponen & Mahmood, 2007).

The operationalisation of policy in resource-constrained institutional environments calls for explicit attention to the mechanics of compliance assurance. The literature on information-security management distinguishes between policy formulation, policy communication and policy enforcement, and notes that weakness at any of these stages erodes the practical efficacy of governance instruments (Dhillon & Backhouse, 2001; Whitman & Mattord, 2018). In the Nigerian federal university context, policy communication has historically been treated as an administrative formality, with documents circulated through electronic mail and posted on institutional portals without supporting briefings, scenario-based illustration or regular refresher cycles (Boniface & Onifade, 2014; Yakubu & Dasuki, 2018). Enforcement, similarly, has tended to rely on retrospective sanction following discrete incidents rather than the ongoing monitoring, peer review and managerial conversation that sustain compliance in mature governance regimes (Tu & Yuan, 2014; Yaokumah, 2014). A further governance gap concerns the integration of personal-device risk with broader institutional risk management. Where personal-device practices are treated as an information-technology matter rather than a strategic risk, executive attention is intermittent and resource allocation is correspondingly modest (Soomro, Shah & Ahmed, 2016). Best practice points toward the elevation of information-security risk to the level of the governing council, with periodic reporting, integration into the institutional risk register and explicit linkage to the institution's strategic objectives (Disterer & Kleiner, 2013; Garba *et al*., 2015). Within Nigeria, recent practitioner work on key-performance-indicator frameworks for large organisations has emphasised analogous principles, suggesting that the governance maturity required for effective personal-device policy is consistent with broader institutional improvements pursued elsewhere in the public sector (Sakyi *et al*., 2022; Filani *et al*., 2022).

8. Human Factors, Awareness, and Behavioural Compliance

The persistent observation across information-security scholarship is that human factors constitute the most consequential determinant of organisational security outcomes (Schultz, 2005; Furnell & Clarke, 2012). Technical controls, however sophisticated, are routinely circumvented by users whose motivations, beliefs and habits diverge from the security expectations encoded in policy (Beautement, Sasse & Wonham, 2008). Within the personal-device context, this observation acquires particular salience, since the user simultaneously owns the endpoint, controls its configuration and serves as the principal source of accountability for its security state (Hovav & Putri, 2016; Crossler *et al*., 2014). The reliance on user behaviour for the realisation of security objectives means that any analysis of personal-device risk must engage directly with the cognitive, social and motivational structures that shape user practice.

Several theoretical frameworks have been advanced to account for the variability of user security behaviour. The protection-motivation theory posits that protective behaviour is a function of perceived threat severity, perceived vulnerability, response efficacy and self-efficacy, with the balance of these factors determining whether users engage in security-supportive actions (Ifinedo, 2012; Vance, Siponen & Pahnila, 2012). The general deterrence theory holds that compliance is shaped by the certainty, severity and celerity of sanction, with implications for how policy enforcement is structured (D'Arcy, Hovav & Galletta, 2009; Herath & Rao, 2009). The health-belief model and theory of planned behaviour have also been adapted to security contexts, illuminating the role of perceived benefits, social norms and behavioural intention (Ng, Kankanhalli & Xu, 2009). Fear appeals have been studied as mechanisms for motivating protective behaviour, with mixed evidence as to their durability and proportionality (Boss *et al*., 2015).

The empirical literature on user behaviour in personal-device contexts paints a mixed picture. Users frequently exhibit a gap between security intention and security action, articulating commitments to protective behaviour that are not consistently realised in practice (Crossler *et al*., 2014). The phenomenon of security neutralisation, in which users develop rationalisations that excuse non-compliance, has been documented across organisational settings (Siponen & Vance, 2010). The compliance budget concept describes how users allocate finite cognitive and affective resources to security tasks, with the result that controls perceived as burdensome are selectively ignored (Beautement, Sasse & Wonham, 2008). These dynamics are intensified in personal-device contexts, where the user's sense of ownership over the device shapes their reception of organisational security

demands (Hovav & Putri, 2016).

In Nigerian federal universities, the human-factors dimension is shaped by additional contextual considerations. Cybersecurity awareness training has historically been irregular, with administrative officers rarely receiving structured instruction on the security implications of their workflow choices (Boniface & Onifade, 2014). The broader public discourse on cybersecurity in Nigeria has been dominated by high-profile financial fraud, with less attention to the routine security risks of organisational data handling (Adesina & Ayo, 2010). Officers may underestimate the threat to their institutions or rationalise their behaviour by appealing to operational necessity. Effective intervention, therefore, requires sustained awareness pedagogy, the alignment of policy with realistic operational constraints, and the cultivation of organisational cultures in which security-supportive behaviour is recognised, valued, and rewarded (Kruger & Kearney, 2006; Olusegun & Ithnin, 2013).

The design of awareness pedagogy that produces measurable behavioural change is itself a substantive undertaking, and the gap between perfunctory training and pedagogically defensible instruction is widely acknowledged in the empirical literature (Bulgurcu, Cavusoglu & Benbasat, 2010; Ifinedo, 2012). Effective programmes are characterised by frequency, contextualisation, and an explicit link between the learning content and the operational realities of the trainee's role. Generic instruction divorced from the workflows of registry, bursary, and examination functions is unlikely to alter the security behaviour of administrative officers, whose risk perceptions are shaped by their concrete daily experience (Boss *et al*., 2015; Vance, Siponen & Pahnila, 2012). Scenario-driven exercises, including simulated phishing campaigns and tabletop incident-response walkthroughs, have demonstrated greater efficacy than lecture-style instruction, both in terms of immediate comprehension and longer-term behavioural retention (Furnell & Clarke, 2012; Herath & Rao, 2009). The social dimension of compliance also merits explicit cultivation. The construction of organisational norms that valorise careful information handling, the visible commitment of senior leadership to security-supportive practice, and the integration of security expectations into performance appraisal each contribute to a climate in which compliant behaviour is socially reinforced rather than treated as an imposition (Schultz, 2005; Beautement, Sasse & Wonham, 2008). Within Nigerian federal universities, where hierarchical norms exert appreciable influence on staff behaviour, executive modelling of secure practice carries particular weight. Recent literature on knowledge management, business intelligence, and decision support in African public-sector contexts has emphasised that culture-level interventions, rather than isolated training events, are the principal lever through which sustainable change in administrative behaviour is achieved (Moyo *et al*., 2021; Bukhari *et al*., 2022; Eboseremen *et al*., 2021).

9. Technical Controls: Mobile Device Management, Containerisation, and Network Segmentation

The technical mitigation of personal-device risk rests on a set of capabilities collectively referred to as mobile-device management, mobile-application management, and enterprise-mobility management, complemented by network-layer controls and identity-management infrastructure. Mobile-device management platforms enable institutions to enforce baseline configurations on enrolled devices, including password complexity, screen-lock timeouts, disk encryption, the use of approved applications, and the capacity for remote wiping in the event of loss or compromise (Souppaya & Scarfone, 2013). Mobile-application management, a more granular approach, focuses on the secure provisioning, configuration, and monitoring of specific applications rather than the device as a whole, accommodating user preferences while protecting institutional data (Romer, 2014; Zahadat *et al*., 2015).

Containerisation offers an architectural strategy that addresses one of the central tensions in personal-device deployment: the coexistence of institutional and personal data on a single device. By creating a logically isolated environment, the container, in which institutional data and applications reside, this approach permits the application of strong security controls to the institutional portion of the device while preserving the user's autonomy over their personal applications and content (Disterer & Kleiner, 2013; Wani, Mendoza & Gray, 2020). Containerisation also simplifies the legal and ethical dimensions of monitoring, since the institution's purview is bounded to the institutional container rather than the device as a whole (Lebek, Degirmenci & Breitner, 2013). Implementation, however, requires either modern operating-system support or third-party platforms, with associated licensing costs that may be prohibitive for resource-constrained universities.

Network-layer controls complement device-level measures by reducing the consequences of endpoint compromise. Virtual private networks encrypt traffic between devices and institutional resources, frustrating man-in-the-middle attacks on hostile networks (Alotaibi & Almagwashi, 2018). Network segmentation isolates sensitive systems from general user traffic, limiting the blast radius of incidents that originate on compromised endpoints (Anderson, 2008; Whitman & Mattord, 2018). Web-filtering, intrusion-detection, and security-information-and-event-management platforms provide visibility into device-network interactions and support the detection of anomalous behaviour (Bukhari *et al*., 2022; Filani *et al*., 2022). Identity controls, including multi-factor authentication, conditional access policies, and risk-based authentication, raise the cost of credential-based attacks and provide a foundation for differentiated access decisions (Adesemowo, Von Solms & Botha, 2016).

For Nigerian federal universities, the deployment of these technical controls is feasible but requires deliberate prioritisation. Comprehensive mobile-device management on every personal endpoint is unlikely to be affordable, but selective application to higher-risk roles, including bursars, examination officers, and senior administrative staff, may be tractable. Multi-factor authentication, network segmentation, and the encryption of sensitive workflows are achievable at modest cost and deliver substantial risk reduction (Pahnila, Siponen & Mahmood, 2007). Cloud-based identity and security services, increasingly available at price points compatible with public-sector budgets, offer a route to enhanced control without the capital expenditure historically associated with enterprise security infrastructure (Akindemowo *et al*., 2021; Adejo *et al*., 2018). The technical architecture must, however, be integrated with the policy and human-factors interventions discussed in earlier sections, since standalone controls will be neither sustainable nor effective in isolation (Jeong & Zo, 2017; Eboseremen *et al*., 2021).

Detection, monitoring, and incident-response capabilities constitute an additional dimension of technical control that warrants explicit treatment in the personal-device context. Endpoint-detection-and-response platforms extend traditional antivirus functionality with behavioural analytics, telemetry collection, and orchestration capabilities that materially improve the institution's capacity to detect and contain compromise (Whitman & Mattord, 2018; Wani, Mendoza & Gray, 2020). Their deployment on personal devices, however, raises legal and ethical considerations associated with the visibility of personal data, requiring careful policy framing, transparent user communication, and the use of architectures that confine institutional telemetry to the institutional container (Lebek, Degirmenci & Breitner, 2013; Mohamed & Ahmad, 2012). Security information and event management platforms aggregate logs from devices, network controls, identity systems, and applications, enabling correlation across the attack chain and supporting investigative workflows when incidents occur (Bukhari *et al*., 2022; Filani *et al*., 2022). For federal universities, the deployment of such platforms may be approached incrementally, beginning with the highest-risk functions and expanding as institutional maturity grows. Residual risk management also calls for explicit attention. Even the most rigorous technical architecture cannot eliminate exposure, and prudent governance acknowledges the residual through cyber-insurance arrangements, incident-response retainers, business-continuity planning, and the periodic exercise of recovery procedures (Anderson, 2008; Soomro, Shah & Ahmed, 2016). The maturity of these arrangements within Nigerian universities is uneven and constitutes an area for sustained institutional investment. Recent practitioner literature on threat-intelligence dashboards, secure DevOps practice, and analytics engineering has emphasised that the integration of detection, response, and recovery capabilities forms the operational backbone of contemporary information-security programmes, and the analytical principles articulated in that literature translate directly to the personal-device context examined here (Adebayo, 2022; Akindemowo *et al*., 2022).

The selection of technical controls in any given institution should also reflect a clear-eyed assessment of the operational dependencies that those controls entail. Mobile-device management platforms require ongoing administration, expertise that may not be resident within the institution, and licensing arrangements whose costs scale with the size of the protected estate (Souppaya& Scarfone, 2013; Romer, 2014). Containerisation depends on operating-system features whose availability varies across the heterogeneous device populations typical of administrative offices, and which may force difficult trade-offs between security coverage and inclusivity (Wani, Mendoza & Gray, 2020; Disterer &Kleiner, 2013). Identity and detection platforms can deliver substantial uplift but require integration with directory services, log-storage infrastructure, and incident-response workflows whose maturity is itself a variable. A pragmatic technical strategy will therefore begin with a frank inventory of existing capabilities, prioritise controls whose dependencies are already satisfied, and grow the technical estate incrementally as institutional capacity matures, rather than attempting the simultaneous deployment of a comprehensive control set that the organisation cannot sustainably operate (Akindemowo *et al*., 2021; Bukhari *et al*., 2022).

10. Toward a Context-Sensitive Risk-Mitigation Architecture for Nigerian Federal Universities

The synthesis presented in the preceding sections supports the articulation of a layered, context-sensitive risk-mitigation architecture suited to the operational realities of Nigerian federal universities. The architecture is layered in the sense that it integrates governance, technical, behavioural, and infrastructural elements, recognising that any single layer of intervention is insufficient. It is context-sensitive in that it acknowledges the resource constraints, infrastructural fragilities, and institutional cultures that distinguish federal universities from the well-resourced organisations on whose experiences much of the global literature is based (Disterer & Kleiner, 2013; Garba *et al*., 2015). The architecture is organised around five mutually reinforcing components.

The first component is the formulation and ratification of a sector-wide personal-device policy framework, developed under the auspices of the National Universities Commission in consultation with federal universities, sectoral regulators, and the academic community. This framework should articulate baseline requirements for the use of personal devices in administrative work, prescribe device-eligibility criteria, define acceptable data categories, mandate authentication and encryption standards, and establish accountability mechanisms (ISO/IEC, 2013; NIST, 2014). The framework should accommodate institutional variation while providing a defensible floor of practice that no federal university would fall beneath (Yusuf, Maina & Dare, 2013). It should also incorporate explicit protections for the privacy of individual officers, balancing institutional security needs against legitimate expectations of personal autonomy (Mohamed & Ahmad, 2012).

The second component is institutional governance reform. Each federal university should designate an executive-level officer with responsibility for information security, supported by an operationally capable team integrated with the central information-technology unit (Soomro, Shah & Ahmed, 2016; Yaokumah, 2014). Information-security risk should be a standing item on the agenda of governing councils, with quarterly reporting on the state of personal-device exposure, incident trends, and the efficacy of remedial measures. Internal audit should incorporate cybersecurity within its scope, and the institutional risk register should explicitly capture endpoint heterogeneity and personal-device practices.

The third component is the prioritised deployment of technical controls calibrated to the risk profile of each administrative function. High-risk units, such as the bursary, examinations office, and human resources, warrant the strongest controls, including mobile-device management, container-based separation of institutional data, multi-factor authentication, and network segmentation (Souppaya & Scarfone, 2013; Alotaibi & Almagwashi, 2018). Lower-risk functions can be accommodated through lighter-weight controls, such as conditional-access policies, virtual-private-network requirements, and baseline endpoint protection. The deployment plan should be informed by an inventory of devices, applications, and data flows, conducted as a foundational step rather than a deferred aspiration (Bukhari *et al*., 2022; Filani *et al*., 2022).

The fourth component is sustained awareness pedagogy. Annual mandatory training for administrative officers should cover phishing recognition, password discipline, secure data-sharing practices, and incident reporting (Kruger & Kearney,

2006; Olusegun & Ithnin, 2013). Training should be evidence-based, scenario-driven, and regularly refreshed, with empirical evaluation of behavioural change rather than reliance on attendance records alone (Boss *et al*., 2015; Ifinedo, 2014). Tailored content for senior leadership is essential, since their security behaviours model expectations for the wider workforce. The fifth component is infrastructural investment, including reliable electricity, adequate enterprise endpoint provisioning, robust campus networks, and resilient backup systems (Olatokun & Ayanbode, 2008; Adejo *et al*., 2018). Without these foundational investments, the reliance on personal devices as a coping strategy will persist regardless of policy aspirations, and the residual risk will continue to grow. The five components must be pursued in concert, sequenced according to feasibility, and resourced through a combination of institutional budgets, donor partnerships, and federal allocations earmarked for cybersecurity in critical sectors (Akindemowo *et al*., 2022; Adebayo, 2022; Ajayi *et al*., 2022).

The implementation of the proposed architecture is best conceived as a phased programme whose sequencing reflects the relative tractability and risk-reduction yield of its constituent elements. In an initial phase, federal universities would prioritise foundational measures whose marginal cost is modest and whose impact is well established: mandatory multi-factor authentication for administrative officers accessing institutional services, comprehensive password-discipline policies supported by reputable password managers, an institution-wide inventory of personal devices used for sensitive functions, and a structured awareness curriculum delivered to all administrative officers (Kruger & Kearney, 2006; Bulgurcu, Cavusoglu & Benbasat, 2010; Souppaya & Scarfone, 2013). A subsequent phase would extend the architecture into more capital-intensive territory, including selective mobile-device management for high-risk roles, containerisation of institutional data on personal endpoints, and the deployment of network-segmentation and detection capabilities (Wani, Mendoza & Gray, 2020; Disterer & Kleiner, 2013). A third phase would consolidate the gains through institutionalisation of governance routines, the maturation of incident-response capability, and the integration of personal-device risk into broader strategic and audit processes (Soomro, Shah & Ahmed, 2016; Yaokumah, 2014). Critical success factors across the phases include sustained executive sponsorship, transparent communication with administrative staff, the cultivation of internal security expertise rather than dependence on episodic consultancy, and the deliberate measurement of programme outcomes against pre-specified indicators (Sakyi *et al*., 2022; Filani *et al*., 2022). Where institutions approach the architecture in this disciplined manner, the prospects for material reduction in personal-device-related risk are substantial, and the wider institutional benefits, in the form of improved data stewardship, sharper accountability, and enhanced stakeholder confidence, are likely to extend well beyond the immediate security domain (Eboseremen *et al*., 2022; Moyo *et al*., 2021).

11. Conclusion

The integration of personally owned digital devices into the administrative workflows of Nigerian federal universities is not a transient operational adjustment but a structural feature of contemporary institutional life. It has emerged from the intersection of consumer technology proliferation, infrastructural constraint, post-pandemic operational realignment, and the informal innovation of administrative officers who have responded creatively to the demands of their roles. While this integration has delivered tangible productivity benefits and enabled the continued functioning of institutions whose enterprise endpoint estates remain incomplete, it has simultaneously produced an information-security exposure whose dimensions are imperfectly understood and whose consequences are unevenly distributed across institutions, units, and individual officers. The review has argued that this exposure must be analysed at five interlocking levels: device, network, application, governance, and user behaviour, and that interventions which address only a subset of these levels will fail to deliver durable risk reduction. It has further been argued that the global literature on consumer-device security, while analytically valuable, presupposes operational capabilities that federal universities do not yet possess and must therefore be recalibrated for the Nigerian context. The proposed risk-mitigation architecture integrates sector-wide policy formulation, institutional governance reform, prioritised technical controls, sustained awareness pedagogy, and foundational infrastructural investment and must be pursued as a coordinated programme rather than a series of discrete initiatives. The path forward requires sustained engagement among regulators, university leaders, information-security practitioners, academic researchers, and the administrative officers whose daily choices shape institutional risk. Empirical work is urgently needed to refine the architecture, evaluate the relative efficacy of its components, and adapt it to the heterogeneous conditions of the federal university subsystem. Only through such disciplined inquiry and coordinated action can the institutional integrity on which Nigerian higher education depends be defended against the threats that contemporary computing practice has unmistakably introduced.

References

1. Abomhara M, Køien GM. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J Cyber Secur Mobil. 2015;4(1):65–88. https://doi.org/10.13052/jcsm2245-1439.414
2. Adebayo AO. Leveraging threat intelligence in DevSecOps for banking security. Int J Sci Res Mod Technol. 2022;1(2):14–27.
3. Adejo OW, Ewuzie I, Usoro A, Connolly T. E-learning to m-learning: framework for data protection and security in cloud infrastructure. Int J Inf Technol Comput Sci. 2018;10(4):1–9. https://doi.org/10.5815/ijitcs.2018.04.01
4. Adeniji OI. Design and Construction of a Temperature Monitoring Device with Security Features [Doctoral dissertation]. Akure: Federal University of Technology; 2019.
5. Adesemowo AK, Von Solms R, Botha RA. Safeguarding information as an asset: do we need a redefinition in the knowledge economy and beyond? SA J Inf Manag. 2016;18(1):1–12. https://doi.org/10.4102/sajim.v18i1.706
6. Adesina AA, Ayo CK. An empirical investigation of the level of users' acceptance of e-banking in Nigeria. J Internet Bank Commer. 2010;15(1):1–13.
7. Ajayi AE, Moyo TM, Tafirenyika S, Taiwo AE,

Tuboalabo A, Bukhari TT. Predictive analytics systems for enhancing financial forecast accuracy and real-time monitoring in hospital networks. Int J Multidiscip Educ Res. 2022;3(2):24–40. https://doi.org/10.54660/IJMER.2022.3.2.24
8. Akindemowo AO, Erigha ED, Obuse E, Ajayi JO, Adebayo A. A conceptual framework for automating data pipelines using ELT tools in cloud-native environments. J Front Multidiscip Res. 2021;2(1):440–452.
9. Akindemowo AO, Erigha ED, Obuse E, Ajayi JO, Soneye OM, Adebayo A. A conceptual model for agile portfolio management in multi-cloud deployment projects. Int J Comput Sci Math Theory. 2022;8(2):64–93.
10. Ali S, Qureshi MN, Abbasi AG. Analysis of BYOD security frameworks. In: Proceedings of the 2015 Conference on Information Assurance and Cyber Security (CIACS); 2015. p. 56–61.
11. Alotaibi B, Almagwashi H. A review of BYOD security challenges, solutions, and policy best practices. In: 2018 1st International Conference on Computer Applications and Information Security (ICCAIS); 2018. p. 1–6.
12. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 2nd ed. Indianapolis: Wiley; 2008.
13. Beautement A, Sasse MA, Wonham M. The compliance budget: managing security behaviour in organisations. In: Proceedings of the 2008 New Security Paradigms Workshop; 2008. p. 47–58. https://doi.org/10.1145/1595676.1595684
14. Boniface A, Onifade O. Cybersecurity awareness among undergraduate students in tertiary institutions in Nigeria. Int J Comput Sci Inf Secur. 2014;12(2):45–54.
15. Boss SR, Galletta DF, Lowry PB, Moody GD, Polak P. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Q. 2015;39(4):837–864. https://doi.org/10.25300/MISQ/2015/39.4.5
16. Bukhari TT, Moyo TM, Tafirenyika S, Taiwo AE, Tuboalabo A, Ajayi AE. AI-driven cybersecurity intelligence dashboards for threat prevention and forensics in regulated business sectors. Int J Multidiscip Educ Res. 2022;3(2):1–15.
17. Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. 2010;34(3):523–548.
18. Chigada J, Daniels N. Exploring information systems security implications posed by BYOD for a financial services firm. Bus Manag Rev. 2021;12(1):116–129.
19. Crossler RE, Long JH, Loraas TM, Trinkle BS. Understanding compliance with bring your own device policies utilizing protection motivation theory: bridging the intention-behavior gap. J Inf Syst. 2014;28(1):209–226. https://doi.org/10.2308/isys-50704
20. D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inf Syst Res. 2009;20(1):79–98. https://doi.org/10.1287/isre.1070.0160
21. Dhillon G, Backhouse J. Current directions in IS security research: towards socio-organisational perspectives. Inf Syst J. 2001;11(2):127–153. https://doi.org/10.1046/j.1365-2575.2001.00099.x
22. Disterer G, Kleiner C. BYOD: Bring Your Own Device. Procedia Technol. 2013;9:43–53. https://doi.org/10.1016/j.protcy.2013.12.005
23. Doargajudhur MS, Dell P. Impact of BYOD on organizational commitment: an empirical investigation. Inf Technol People. 2019;32(2):246–268. https://doi.org/10.1108/ITP-11-2017-0378
24. Eboseremen BO, Adebayo AO, Essien IA, Ofori SD, Soneye OM. The impact of interactive data visualizations on public policy decision-making. Int J Multidiscip Res Growth Eval. 2022;3(1):1189–1203. https://doi.org/10.54660/.IJMRGE.2022.3.1.1189-1203
25. Eslahi M, Naseri MV, Hashim H, Tahir NM, Saad EHM. BYOD: current state and security challenges. In: 2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE); 2014. p. 189–192. https://doi.org/10.1109/ISCAIE.2014.7010235
26. Ezeh FE, Anthony P, Adeleke AS, Gbaraba SV, Gado P, Moyo TM, *et al*. Digitizing healthcare enrollment workflows: overcoming legacy system barriers in specialty care. Int J Multidiscip Futur Dev. 2022;3(2):19–37.
27. Fasae JK, Adegbilero-Iwari I. Mobile devices for academic practices by students of the College of Sciences in selected Nigerian private universities. Electron Libr. 2015;33(4):749–759.
28. Filani OM, Nnabueze SB, Ike PN, Wedraogo L. Real-time risk assessment dashboards using machine learning in hospital supply chain management systems. Int J Multidiscip Educ Res. 2022;3(1):65–76. https://doi.org/10.54660/IJMER.2022.3.1.65-76
29. Frempong D, Ifenatuora GP, Ofori SD. AI-powered chatbots for education delivery in remote and underserved regions. Int J Front Multidiscip Res. 2020;1(1):156–172. https://doi.org/10.54660/.IJFMR.2020.1.1.156-172
30. French AM, Guo C, Shim JP. Current status, issues, and future of bring your own device (BYOD). Commun Assoc Inf Syst. 2014;35:191–197. https://doi.org/10.17705/1CAIS.03510
31. Furnell S, Clarke N. Power to the people? The evolving recognition of human aspects of security. Comput Secur. 2012;31(8):983–988. https://doi.org/10.1016/j.cose.2012.08.004
32. Garba AB, Armarego J, Murray D, Kenworthy W. Review of the information security and privacy challenges in bring your own device (BYOD) environments. J Inf Priv Secur. 2015;11(1):38–54.
33. Garba AB, Armarego J, Murray D. Bring your own device organizational information security and privacy. ARPN J Eng Appl Sci. 2015;10(3):1279–1287.
34. Herath T, Rao HR. Protection, motivation, and deterrence: a framework for security policy compliance in organisations. Eur J Inf Syst. 2009;18(2):106–125. https://doi.org/10.1057/ejis.2009.6
35. Hovav A, Putri FF. This is my device! Why should I follow your rules? Employees' compliance with BYOD policies. Pervasive Mob Comput. 2016;32:35–49. https://doi.org/10.1016/j.pmcj.2016.06.007
36. Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput Secur. 2012;31(1):83–95.

37. Ifinedo P. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inf Manag. 2014;51(1):69–79. https://doi.org/10.1016/j.im.2013.10.001
38. Imgraben J, Engelbrecht A, Choo KKR. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. Behav Inf Technol. 2014;33(12):1347–1360. https://doi.org/10.1080/0144929X.2014.934286
39. International Organization for Standardization. ISO/IEC 27001:2013 Information Technology — Security Techniques — Information Security Management Systems — Requirements. Geneva: ISO; 2013.
40. Jeong M, Zo H. Bring your own device: mediating effects of self-efficacy, employee productivity, and security risk on BYOD intention. In: Proceedings of the 38th International Conference on Information Systems (ICIS); 2017. p. 1–11.
41. Köffer S, Ortbach K, Niehaves B. Exploring the relationship between IT consumerization and job performance: a theoretical framework for future research. Commun Assoc Inf Syst. 2014;35:14. https://doi.org/10.17705/1CAIS.03514
42. Kruger HA, Kearney WD. A prototype for assessing information security awareness. Comput Secur. 2006;25(4):289–296. https://doi.org/10.1016/j.cose.2006.02.008
43. Lebek B, Degirmenci K, Breitner MH. Investigating the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices. In: Proceedings of the 19th Americas Conference on Information Systems (AMCIS); 2013. p. 1–8.
44. Lee J, Warkentin M, Crossler RE, Otondo RF. Implications of monitoring mechanisms on bring your own device adoption. J Comput Inf Syst. 2017;57(4):309–318.
45. Mbarika VWA, Okoli C, Byrd TA, Datta P. The neglected continent of IS research: a research agenda for sub-Saharan Africa. J Assoc Inf Syst. 2005;6(5):130–170.
46. Miller KW, Voas J, Hurlburt GF. BYOD: security and privacy considerations. IT Prof. 2012;14(5):53–55. https://doi.org/10.1109/MITP.2012.93
47. Mohamed N, Ahmad IH. Information privacy concerns, antecedents, and privacy measure use in social networking sites: evidence from Malaysia. Comput Hum Behav. 2012;28(6):2366–2375. https://doi.org/10.1016/j.chb.2012.07.008
48. Moyo TM, Taiwo AE, Ajayi AE, Tafirenyika S, Tuboalabo A, Bukhari TT. Designing smart BI platforms for government healthcare funding transparency and operational performance improvement. Int J Multidiscip Educ Res. 2021;2(2):41–51. https://doi.org/10.54660/IJMER.2021.2.2.41-51
49. Ng BY, Kankanhalli A, Xu YC. Studying users' computer security behavior: a health belief perspective. Decis Support Syst. 2009;46(4):815–825. https://doi.org/10.1016/j.dss.2008.11.010
50. Niehaves B, Köffer S, Ortbach K. IT consumerization — a theory and practice review. In: Proceedings of the 18th Americas Conference on Information Systems (AMCIS); 2012. p. 1–10.
51. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. Gaithersburg: NIST; 2014.
52. Ogbomo MO, Ogbomo EF. Importance of information and communication technologies (ICTs) in making a healthy information society: a case study of Ethiope East local government area of Delta State, Nigeria. Libr Philos Pract. 2008:1–7.
53. Olalere M, Abdullah MT, Mahmod R, Abdullah A. A review of bring your own device on security issues. SAGE Open. 2015;5(2):1–11.
54. Olatokun WM, Ayanbode OF. Use of educational technologies by Nigerian university lecturers: a case study of University of Ibadan. Inf Dev. 2008;24(3):213–220.
55. Olusegun OJ, Ithnin NB. People are the answer to security: establishing a sustainable information security awareness training (ISAT) program in an organization. Int J Comput Sci Inf Secur. 2013;11(8):57–64.
56. Omotayo OO, Kuponiyi AB. Telehealth expansion in post-COVID healthcare systems: challenges and opportunities. ICONIC Res Eng J. 2020;3(10):496–513.
57. Pahnila S, Siponen M, Mahmood A. Employees' behavior towards IS security policy compliance. In: Proceedings of the 40th Annual Hawaii International Conference on System Sciences; 2007. p. 156b. https://doi.org/10.1109/HICSS.2007.206
58. Patten KP, Harris MA. The need to address mobile device security in the higher education IT curriculum. J Inf Syst Educ. 2013;24(1):41–52.
59. Putri FF, Hovav A. Employees' compliance with BYOD security policy: insights from reactance, organizational justice and protection motivation theory. In: Proceedings of the 22nd European Conference on Information Systems (ECIS); 2014. p. 1–17.
60. Romer H. Best practices for BYOD security. Comput Fraud Secur. 2014;2014(1):13–15. https://doi.org/10.1016/S1361-3723(14)70007-7
61. Sangodoyin AA, Sani A, Idowu O. The challenges of implementing ICT policies in Nigerian universities. Afr J Inf Commun. 2017;19:43–62. https://doi.org/10.23962/10539/23574
62. Schultz EE. The human factor in security. Comput Secur. 2005;24(6):425–426. https://doi.org/10.1016/j.cose.2005.07.002
63. Shittu ISOMA, Adeniji IO, Shittu H. Blockchain-assisted secure data exchange architectures for SCADA-controlled power systems. IRE J. 2022;6(3):21–35.
64. Singh N. BYOD genie is out of the bottle — devil or angel. J Bus Manag Soc Sci Res. 2012;1(3):1–12.
65. Siponen M, Vance A. Neutralization: new insights into the problem of employee information systems security policy violations. MIS Q. 2010;34(3):487–502. https://doi.org/10.2307/25750688
66. Soomro ZA, Shah MH, Ahmed J. Information security management needs a more holistic approach: a literature review. Int J Inf Manag. 2016;36(2):215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009
67. Souppaya M, Scarfone K. Guidelines for Managing the Security of Mobile Devices in the Enterprise. NIST Special Publication 800-124 Revision 1. Gaithersburg: National Institute of Standards and Technology; 2013. https://doi.org/10.6028/NIST.SP.800-124r1
68. Steel S. BYOD: a look at past, present, and future trends. Educause Rev. 2014;49(2):20–32.

69. Tu Z, Yuan Y. Critical success factors analysis on effective information security management: a literature review. In: Proceedings of the 20th Americas Conference on Information Systems (AMCIS); 2014. p. 1–13.
70. Vance A, Siponen M, Pahnila S. Motivating IS security compliance: insights from habit and protection motivation theory. Inf Manag. 2012;49(3–4):190–198. https://doi.org/10.1016/j.im.2012.04.002
71. Von Solms R, Van Niekerk J. From information security to cyber security. Comput Secur. 2013;38:97–102. https://doi.org/10.1016/j.cose.2013.04.004
72. Wang Y, Wei J, Vangury K. Bring your own device security issues and challenges. In: 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC); 2014. p. 80–85. https://doi.org/10.1109/CCNC.2014.6866552
73. Wani TA, Mendoza A, Gray K. Hospital bring-your-own-device security challenges and solutions: systematic review of gray literature. JMIR mHealth uHealth. 2020;8(6):e18175. https://doi.org/10.2196/18175
74. Weeger A, Wang X, Gewald H, Raisinghani M, Sanchez O, Grant G, *et al*. Determinants of intention to participate in corporate BYOD-programs: the case of digital natives. Inf Syst Front. 2020;22:203–219. https://doi.org/10.1007/s10796-018-9857-4
75. Whitman ME, Mattord HJ. Principles of Information Security. 6th ed. Boston: Cengage Learning; 2018.
76. Yakubu MN, Dasuki SI. Assessing eLearning systems success in Nigeria: an application of the DeLone and McLean information systems success model. J Inf Technol Educ Res. 2018;17:183–203.
77. Yang TA, Vlas R, Yang A, Vlas C. Risk management in the era of BYOD: the quintet of technology adoption, controls, liabilities, user perspectives, and policies. In: 2013 International Conference on Social Computing; 2013. p. 411–416.
78. Yaokumah W. Information security governance implementation within Ghanaian industry sectors: an empirical study. Inf Manag Comput Secur. 2014;22(3):235–250.
79. Yusuf MO, Maina B, Dare MO. Information and communication technology and education: analysing the Nigerian national policy for information technology. Int Educ Stud. 2013;6(8):123–132.
80. Zahadat N, Blessner P, Blackburn T, Olson BA. BYOD security engineering: a framework and its analysis. Comput Secur. 2015;55:81–99. https://doi.org/10.1016/j.cose.2015.06.011