International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Cybersecurity Awareness and Risk Management in the Public Sector

Gbemisola Kayode-Bolarinwa [1]

Submitted: 07/01/2025 **Revised:** 01/03/2025 **Accepted:** 08/03/2025

Abstract*:* Cybersecurity has emerged as a significant concern for public sectors in this period of speedy digital transformation and increasing dependence on technology. As these entities are custodians of enormous warehouses of sensitive information, such as classified data, financial, and personal, they are key targets for malicious cyber activities. The adoption of emerging technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), and cloud computing is intensified by the growing threat landscape, which compels a vigorous and multidimensional approach to cybersecurity. The behaviour of the employees, mostly affected by low awareness and weak digital hygiene, remains a crucial vulnerability. This research studies the interdependency of awareness of cybersecurity and risk management approaches in public sector organizations. Making use of a qualitative method that features literature review, case study, and policy analysis, the research examines common threat vectors, analyzes practical incidents, assesses regulatory frameworks, and offers actionable recommendations to improve cyber resilience. The findings highlight the significance of a socio-technical method that merges people, processes, and technology to efficiently manage the risks of cybersecurity in government establishments.

Keywords: *Public Sector, Cybersecurity Awareness, Risk Management, Insider Threat, Phishing, National Policy, Governance*.

1. Introduction

The threats of cybersecurity have intensified in scale, intricacy, and occurrence, exhibiting major challenges for the public sector worldwide. Kshetri (2022) mentioned that government organisations are increasingly dependent on technological infrastructure for their service delivery, making them exposed to attacks that can compromise national security, interrupt operations, and destroy public trust. According to NCPS (2021), which stated that with the increase in the use of advanced technologies such as 5G, AI, cloud computing, and IoT devices, the attack landscape has broadened substantially.

The advent of the COVID-19 pandemic significantly enhanced digital transformation, leading to the extensive acceptance of remote work and digital platforms. This change has also presented further exposures as indicated by ENISA (2023). According to OECD (2023), which mentioned that government establishments must steer these challenges while functioning under limited resources, governing administration, and the treble responsibility to safeguard both security and transparency. According to IBM (2023), it opined that despite improved investing in cybersecurity infrastructure, threats like ransomware, insider threats, and phishing remain persevere regularly because of insufficient awareness and human error. Hence, effective cybersecurity should broaden further than technical controls to integrate the culture of the organization, training of employees, and strategic risk management.

2. Cybersecurity Threats in the Public Sector

The government agencies are distinctively exposed to cyber threats because of their responsibility as the guardians of huge volumes of sensitive, mission-critical, and usually classified data. Public sectors collect, process, and store information, for example, tax and health records, defense-related intelligence, national identification data, and financial transactions. The compromise of such data not only puts personal confidentiality at risk but could also undercut public trust, economic stability, and national security in government agencies (Kshetri, 2022; OECD, 2023). Contrasting the private sector, government establishments usually function in extremely regulated ecosystems with legacy IT infrastructures, restricted budgets for cybersecurity, and bureaucratic restrictions that impede swift reactions to arising threats. In several nations, specifically developing countries, government establishments confront additional challenges, for example, weak governance frameworks, inadequate access to cybersecurity tools, and shortages of skills (NCPS, 2021; GAO, 2023).

2.1. Phishing and Social Engineering:

Phishing continues to be one of the greatest persistent and effective methods of cyberattacks aimed at government employees. These attacks are intended to trick people into disclosing confidential information like credentials for login or downloading malicious attachments. Public sectors are major recipients due to invaders could use their access to vital infrastructure, employees' data, and financial platforms (Verizon, 2023). Phishing emails usually imitate reliable sources, for example, internal divisions, affiliate organisations, or international corporations, to circumvent conventional email filters and social defenses. According to CISA (2022) stated that it was reported by the U.S. Department of Homeland Security that more than 60% of successful breaches in federal establishments started with phishing attacks. The hierarchical communication culture of the public sector can intensify this issue because employees may be reluctant to query requests that seem to come from supervisors.

2.2. Ransomware:

This is another cybersecurity major threat that public organisations globally are vulnerable to. Cybercriminals encrypt vital data and request ransom payments to reinstate access in ransomware attacks. As mentioned by Deemantha (2024) that city councils,

education sectors, and public hospitals have progressively been targeted, causing disruptions in service, financial deficits, and possible threats to public safety. GAO (2023) reported that in 2021, Colonial Pipeline was attacked by ransomware that affected the distribution of fuel in the United States, emphasizing that the level of the public infrastructure is exposed to cyber perpetrators. Likewise, in 2020, IT infrastructures in Baltimore City were incapacitated for weeks due to a ransomware attack, as the recovery expenses cost taxpayers more than $18 million. Government establishments are usually delayed in patching vulnerabilities and spend on vigorous backups, which make them easy targets. IBM (2023) mentioned that ransomware-as-a-service (RaaS) models have reduced the opening for cybercriminals to attack, allowing even inexperienced players to launch devastating attacks.

2.3. Insider Threats:

Insider threats are known as cybersecurity threats originating from inside the establishments, either from careless behaviour or malicious intent. Among the civil servants who have authorised access to systems and data, they could carelessly reveal information by being victim to a phishing attack or by making use of vulnerable passwords. Malicious insiders may act for ideological, financial, or individual reasons (Ponemon Institute, 2021).

2.4. Supply Chain Attacks:

Present government institutions' services rely on a web of third-party vendors, suppliers, and IT service providers. As outsourcing may decrease expenses and enhance productivity, it presents further cybersecurity threats. A supply chain attack happens when a reliable third party is compromised, allowing hackers to gain access to connected systems. SolarWinds breach in 2020 is a well-known instance, where attackers introduced malware into software updates spread by SolarWinds to contractors used by several U.S. government organisations. The infringe went unobserved for months and compromised classified networks within national defense, security, and intelligence sections (GAO, 2023). According to ENISA (2023) stated that several government establishments require enough vendor risk management protocols, for instance, constant monitoring, contracts inclusive of cybersecurity clauses, or continuous audits. This causes them to be specifically exposed to supply chain exploits.

2.5. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks:

DoS and DDoS threats flood services online with traffic, making them difficult to appropriate users to access. Portals accessible by the public, for example election portals, vaccine registration (COVID-19), or tax filing systems, usually aim during critical periods for such attacks. DDoS attacks are commonly utilised by groups of hacktivists or state-funded players to interrupt public services or broadcast political messages. In 2007, Estonia's multiple government and banking websites were incapacitated due to DDoS cyberattacks, which is known to be the first large-scale cyberattack against an entire nation (CISA, 2022). DoS attacks do not involve data breaches but damage the reputation and disrupt service, which leads to the public losing confidence in digital governance.

2.6. Weak Identity and Access Management (IAM):

Several government establishments still depend on obsolete methods of authentication, for instance, shared accounts, unsegmented access control, or single-factor passwords. This enhances the threat of data interference, unauthorized access, and unrestrained movement by hackers in the networks. Appropriate IAM policies comprising multi-factor authentication (MFA), role-based access control (RBAC), and regular reviews of access are vital in limiting exposure and compensating for liability. Unfortunately, there are still low adoption rates, especially at local government levels in several developing nations (NIST, 2021).

The landscape of cybersecurity threats facing government establishments is varied, unrelenting, and progressing. As technical defences are critical, the actual strength of a public sector's posture of cybersecurity remains in its capability to promote awareness culture, spend on innovative infrastructure, and create institutional resistance. A practical, layered defense method accompanied by rigorous risk management and policy frameworks is needed to secure the digital fundamentals of public governance.

3. The Role of Cybersecurity Awareness

In the advancing landscape of cybersecurity threats, individual error continues to be the most utilised vulnerability. IBM (2023) research reveals that human factors contributed to more than 80% of cybersecurity breaches, which include carelessness, weak password hygiene, and falling victim to phishing or social engineering attacks. This emphasises the significance of awareness in cybersecurity as a frontier security procedure in any establishment, especially in government establishments where data sensitivity and the effect of infringements are usually much higher. Cybersecurity awareness goes further than a singular training session, rather, it involves a logical method to educate, engage, and empower employees at different levels to understand and alleviate possible risks. As public institutions increasingly digitalize services, a well-informed workforce becomes a crucial line of defense against cyber risks.

3.1. Training and Education

Regular training and education are preliminary to a successful strategy for cybersecurity awareness. The program aims to provide staff with the necessary knowledge and abilities to recognise, relate, and react to cyber threats on digital platforms, for instance, suspicious behaviour, phishing emails, and malicious attachments. According to the NIST (2022), businesses that conduct continuous and well-defined training courses see a marked development in staff security behaviour and incident response rates. The training program must be vibrant and contextualized to the risk profile of the establishment. For example, in the public sector dealing with personnel data, training should highlight principles of data privacy, secure practices of communication, and reporting procedures for impending threats. Moreover, customised training for diverse functions, for instance, executives, IT staff, and administrative employees, guarantees that everybody identifies their exact tasks in supporting cybersecurity (SANS Institute, 2023).

3.1 Attack Simulations and Behavioural Reinforcement

Phishing simulation drills are a verified technique to support the training of cybersecurity. Real-world attack scenarios are simulated by these controlled tests, for instance, misleading emails or false login pages, to determine the way staff will react under pressure. The purpose is not to reprimand failures, but to detect skill disparities and strengthen awareness via response and re-training (SANS Institute, 2023). Research reveals that companies

that consistently conduct such simulations see a substantial drop in the rates of clicking on phishing emails and quicker exposure of malicious emails (Hadnagy & Fincher, 2021). Furthermore, simulations offer helpful metrics for assessing the usefulness of awareness training and modifying approaches accordingly. For government establishments that function as key infrastructure providers, these procedures are important to supporting operational resilience and continuity.

3.2. Cultivating a Strong Security Culture

Further than the technical training and simulations, awareness of cybersecurity must be entrenched in the culture of the organization. A resilient security culture fosters collective responsibility, ethical behaviour, and active engagement with cybersecurity guidelines and processes. According to ISO/IEC 27001:2022, promoting security-minded values is crucial for making sure that technical regulations are adopted by human conformity and awareness (ISO/IEC, 2022). Leadership acts as a key part in forming this culture. When cybersecurity is prioritized by the executives, sufficient resources are allocated, and model secure behaviours, for instance, utilising multi-factor authentication and reporting malicious activity, this conveys a strong message to employees about the significance of cybersecurity (OECD, 2023).

4. Risk Management Frameworks for the Public Sector

In the era of escalating cyber threats, government establishments need an organised and proactive method of identifying, assessing, mitigating, and recovering from cybersecurity risks. Risk management frameworks provide a logical approach to the protection of vital data infrastructure, ensure conformity with laws, and create resilience against advancing digital risks. For public organisations that usually keep confidential citizen data and sources of vital services, the implementation of harmonised frameworks is key for public trust, clarity, and operational continuity, clarity (OECD, 2023). Respective internationally and nationwide accepted frameworks are contributory in guiding government establishments to comprehensively control cybersecurity threats. These frameworks offer actionable standards, control procedures, and governance structures that will facilitate organisations to align their security position with both the aims and governing responsibilities of the organization.

4.1. NIST Cybersecurity Framework (CSF)

The U.S. National Institute of Standards and Technology developed the NIST Cybersecurity Framework (CSF) as a widely accepted cybersecurity risk management tool. The framework comprises five core functions: Identify, Protect, Detect, Respond, and Recover, that mutually offer an advanced, tactical view of the risk management lifecycle (NIST, 2021).

- Identify: To be aware of the organizational environment, resources, and risk environment.
- Protect: To implement safety measures to guarantee service delivery.
- Detect: To create procedures to detect cybersecurity incidents.
- Respond: To initiate suitable measures to respond to identified incidents.
- Recover: To sustain strategies for resilience and restoration of abilities post-incident (NIST, 2021).

The NIST CSF strength remains in its flexibility, which can be adapted to several organizational sizes and levels of maturity. This makes it mainly valuable for government establishments with differing digital infrastructure levels. According to Ross et al. (2022), its use improves preparation and regulatory conformity and facilitates collaboration across sectors via a general language.

4.2. ISO/IEC 27001

The ISO/IEC 27001 standard is the international standard for implementing an Information Security Management System (ISMS). This offers a risk-based method for governing information security, ensuring data confidentiality, integrity, and availability (ISO, 2022). The standard outlines procedures for risk assessment, risk treatment, monitoring, and continual improvement. What differentiates ISO/IEC 27001 is its highlighting on:

- Involvement of leadership and roles/responsibilities definition.
- Systematic security controls documentation.
- Continuous improvement cycle (Plan-Do-Check-Act).

For government establishments, ISO/IEC 27001 promotes accountability and assurance, specifically when managing significant volumes of citizen data or active data exchanges within intergovernmental organizations. Akhgar & Brewster (2021) reported that ISO/IEC 27001 certification also improves public assurance and establishes an obligation to global information security best practices.

4.3. CIS Critical Security Controls

The Center for Internet Security (CIS) Critical Security Controls (v8) offers a highlighted and actionable set of 18 security procedures aimed to protect against the most common cyberthreats (CIS, 2023). These controls originate from actual attack data and are specifically significant for resource-constrained government establishments getting maximum security results with inadequate budgets. Some key CIS controls involve:

- Asset inventory of hardware/software.
- Network devices and operating systems secure configurations.
- Continuous vulnerability management.
- Security awareness and skills training.
- Incident response management.

The CIS Controls provide practical, scalable management that assists government establishments in shifting from reactive to proactive security management. Their prioritising and implementing stages permit businesses to customise implementation based on exposure of risk and level of maturity (SANS Institute, 2022).

4.4. Nigeria National Cybersecurity Policy and Strategy (NCPS)

Locally, Nigeria's National Cybersecurity Policy and Strategy (NCPS) 2021 offers an inclusive policy framework for securing the cyberspace of the country. It is fitted to the socio-economic, governance context and advances resilience in Nigeria via the following strategic pillars (Office of the National Security Adviser, 2021):

- Governance and coordination: Establishing cooperation among cybersecurity agencies and inter-ministerial bodies.
- Capacity building: Training programs for civil servants and

security professionals.

- Public-private partnership: Boosting collaboration between government and private sectors.
- Legal and regulatory reform: Facilitating regulations, for instance, the Cybercrimes Act 2015, to promote enforcement and compliance.

NCPS also highlights the protection of national critical infrastructure, cyber diplomacy, and local cybersecurity innovation. Its significance to the government establishment cannot be overemphasised, for its alignment with the institutional actions with national cybersecurity aims while focusing on related challenges, for instance, inadequate technical ability and enforcement restrictions (Adeleke et al., 2023).

5. Methodology

This paper employs a qualitative research design to explore the interrelated human behaviour dynamics, organizational policies, and technical protections in the cybersecurity architecture of government establishments. Qualitative methods are specifically appropriate for this type of study as they expedite a detailed perspective of complicated socio-technical events that are not quantifiable (Creswell & Poth, 2018). The study incorporates a multi-method approach involving a literature review, case study analysis, and policy analysis, triangulated to boost the reliability, validity, and transferability of results (Denzin, 2012).

5.1. Literature Review

The literature review outlines the introductory source of this study. It integrates academic data, practical perceptions, and evolving trends in government establishments' cybersecurity. Major sources consist of peer-reviewed academic journals accessed through databases like IEEE Xplore, ScienceDirect, and SpringerLink, in conjunction with governmental publications like those by the U.S. Government Accountability Office (GAO) and the National Institute of Standards and Technology (NIST).

Furthermore, reports of industry-specific threat communication from cybersecurity leaders like IBM and Verizon offer background evidence on present vulnerabilities, threats, and mitigation trends. The choice of literature aimed at publications from 2018 to 2024, making sure that the investigation is both recent and appropriate in light of hastily advancing cybersecurity theories (IBM, 2023; Verizon, 2024). Keywords guiding the review included "cybersecurity awareness," "risk management frameworks," "public sector cyber incidents," and "policy implementation challenges."

5.2. Case Study Analysis

Case studies are utilised to opine on the theoretical and policy discussions in practical occurrences. This approach offers a context-rich evaluation of certain incidents of cyberattacks relating to government establishment bodies, emphasising not only the technical influence but also the human, procedural, and strategic lessons learned (Yin, 2018). The chosen case studies cover diverse geopolitical zones and kinds of threat actors, from criminal groups to state-sponsored actors:

Incident	Year	Impact	Key Lesson
SolarWinds Breach	2020	Attacks on U.S. federal networks and private organisations	The compromise exposed vulnerabilities in supply chain management and highlighted the requirement for Zero Trust Architecture (SolarWinds, 2021).
Colonial Pipeline Ransomware	2021	Major fuel disruption throughout the Eastern U.S.	This event highlighted the significance of incident readiness, response protocols, and communication approaches during crises (GAO, 2022).
Australian Government Cyber Attacks	2022	Several government establishments aimed	The incident highlighted the emerging threat of state-sponsored attacks and the need for harmonised national defense approaches (Australian Cyber Security Centre, 2022).

These instances were chosen based on their significance to government establishments' vulnerabilities, variety of attack vectors, and the availability of official reports of post-incident that enabled deeper analysis.

5.3. Policy Analysis

Policy analysis in this study entails a comparative review of major global cybersecurity frameworks and their implementation within government institutions' environments. Particularly, the study reviews:

- European Union General Data Protection Regulation (GDPR)
- United States NIST Cybersecurity Framework (CSF), and
- The ISO/IEC 27001 international standard for Information Security Management Systems (ISMS).

The study emphasises commonalities, like highlighting risk-based methodologies and continuous enhancement, and also implementation issues encountered by government establishments. These issues comprise:

- Budget restrictions that limit investment in evolved security infrastructure,
- Obsolete IT infrastructures that are difficult to protect and integrate with the latest solutions,
- Inadequately experienced employees, specifically in developing countries.

Such policy study facilitates identifying differences between policy design and practical implementation that usually diminish government institutions' cyber resilience (Adeleke et al., 2023; Bada & Nurse, 2019).

5.4. Triangulation

To improve methodological rigor, the research uses triangulation, the method of validating evidence from several sources and approaches. Denzin (2012) pointed out that triangulation improves the reliability and validity of study results by cross-verifying data from the literature review, case studies, and policy documents.

This method reduces bias and ensures that perceptions are not originated from a specific data stream but are constantly reinforced within diverse forms of evidence.

6. Challenges in Public Sector Cybersecurity

Compared to private sector organisations, government establishments often lag in cybersecurity resilience, despite being a custodian of huge and confidential citizen data. According to Bada & Nurse (2019) pointed that the lag is because of a convergence of budget limitations, technical, structural, and regulatory challenges. These exposures not only grow the threats of effective cyberattacks but also jeopardise national security, public trust, and the continuity of crucial services. Below are the very important impediments hindering cybersecurity advancement in public organisations:

6.1. Budget Limitations

One of the most significant hindrances to effective cybersecurity in government establishments is scarce finances. Contrasting private organisations that can apportion significant funds to digital infrastructure and cyber defense, several public organisations operate under strict financial limitations. Cybersecurity is usually underprioritized in financial allocations, contending with more perceptible or politically exigent programs like education, infrastructure, and healthcare (GAO, 2023). Insufficient budget effects in:

- IT and security teams are short-staffed.
- Limited assets in security tools such as endpoint protection, firewalls, and SIEM (Security Information and Event Management) systems,
- Inability to conduct constant security audits or penetration testing.

This persistent underbudgeting initiates variances, which are utilised by threat actors. According to a 2023 U.S. Government Accountability Office (GAO) report stated that almost 70% of investigated federal establishments reported that budget limitations substantially limited their ability to deploy strong cybersecurity procedures.

6.2. Legacy Infrastructure

Government establishments often depend on obsolete infrastructure, legacy systems, and applications that are end of support by vendors and are therefore extremely exposed to cyber threats. CISA (2022) mentioned that these IT infrastructures usually lack the latest security features like automated patch management, encryption by default, and multi-factor authentication. For instance:

- Outdated operating systems could not support the latest security protocols.
- Obsolete applications may not integrate well with the latest security procedures.
- Patching and upgrading these systems can be unsafe, expensive, or even unfeasible because of operational dependencies.

CISA (2022) continually cautioned that obsolete systems present systemic imperils to state and local government processes. In sectors like finances, transportation, and public health, these vulnerabilities may have surging effects on vital infrastructure and the delivery of services.

6.3. Regulatory Complexity and Burden

Government establishments are usually subject to overlapping and fragmented cybersecurity laws that can lead to disorder and conformity exhaustion. These organisations must steer a complicated law landscape that comprises general data protection regulations, global standards, sector-specific obligations, and internal procedures, all of which may not be synchronised (OECD, 2023). Basic impediments comprise:

- Complexity in associating local guidelines with global standards such as ISO/IEC 27001 or GDPR.
- Contrary obligations across several jurisdictions.
- High cost of administrative costs related to establishing conformity.

This difficulty is usually due to compliance-driven security, where organisations emphasize marking checkboxes rather than employing adaptive, risk-based cybersecurity approaches (Pfleeger & Caputo, 2012). The OECD (2023) also notes that regulatory disintegration leads to inadequacies, reduces improvement, and burdens already overstressed public organisation IT personnel.

7. Recommendations

As cyber threats advance in complexity and occurrence, public organisations must embrace proactive and multi-layered cybersecurity approaches. A reactive or compliance-only position is no longer adequate. Instead, authorities must adopt a constant improvement, resilience, and foresight culture. The following recommendations offer a vigorous framework for strengthening cybersecurity positions across government establishments:

7.1. Implement Continuous Training

As indicated by Hadnagy & Fincher (2021), cybersecurity awareness should not be a one-time program but a constant, well-defined practice. Compulsory, role-based training courses and certifications must be introduced for all civil servants, designed for their level of data access and operational tasks. Simulated phishing attacks and gamified awareness modules are important to reinforce learning results and improve unsafe behaviours.

Deemantha (2024) stated that establishments that employed routine simulation-based training noticed up to a 50% decrease in staff-initiated security violations. Individual inaccuracy remains the major reason for cyber incidents; therefore, promoting a cyber-aware workforce is a strategic prerequisite.

7.2. Adopt Zero Trust Architecture (ZTA)

Zero Trust is a concept shift from the old model of perimeter-based security. It drives on the standard of "never trust, always verify," assuming vulnerability may occur both inside and outside the network. Forrester (2023) mentioned that all users and devices must be authenticated, authorized, and continuously validated before being given or retaining access to systems. Government establishments, specifically those with hybrid or remote employee-based structures, must implement least privilege access, micro-segmentation, and multi-factor authentication (MFA) as part of their ZTA deployment. According to Forrester's Zero Trust Maturity Model, institutions with established ZTA structures experience 30% fewer breach events (Forrester, 2023).

7.3. Enhance Incident Response Plans (IRPs)

IRPs are more than documentation, the public sector must perform

frequent red-team/blue-team practices, tabletop simulations, and reviews of after-action to authenticate and enhance their preparedness (NIST, 2022). These practices assist in identifying procedural gaps, enhancing team coordination, and fostering institutional muscle memory for reacting to real-world threats. The NIST SP 800-61 Revision 2 suggests structured incident lifecycle management, including preparation, detection and analysis, containment, eradication, recovery, and post-incident activity. Organisations that frequently test their IRPs report a 40% decrease in recovery time after an attack (NIST, 2022).

7.4. Invest in Artificial Intelligence and Automation

The extent and rapidity of advanced cyberattacks overtake manual discovery and reaction approaches. Public sectors must spend on AI-driven security tools that provide real-time threat intelligence, behavioural analytics, and automated incident response (Gartner, 2023). These technologies can discover anomalies across immense datasets, detect zero-day threats, and automatically detach compromised systems before damage worsens. Gartner (2023) notes that by 2026, AI-enabled security operations centers (SOCs) will decrease breach detection times by more than 50%. Tools like User and Entity Behavior Analytics (UEBA) and Security Orchestration, Automation, and Response (SOAR) are particularly effective in public sector environments with limited cybersecurity personnel.

7.5. Conduct Routine Penetration Testing

Public-facing applications and internal systems require routine penetration testing (pen testing) to expose unknown vulnerabilities before exploitation by malicious actors. This requires ethical hackers to simulate real-world attacks to evaluate the robustness of the organisation's defenses. According to the Open Web Application Security Project (OWASP), pen testing should be performed at least biannually and after infrastructure changes or major code updates. Authorities managing public data, like identity registrations or portals for digital services, must highlight that penetration testing must be inclusive in their risk assessment and compliance approaches (OWASP, 2022).

7.6. Strengthen Patch Management Protocols

The root cause of numerous high-profile breaches is being caused from delayed patching of known vulnerabilities. Public sectors should employ automated patch management systems and employ a real-time inventory of every IT asset to prioritize updates effectively (Keating, 2025). Keating (2025) highlighted that effective patch cycles of less than 30 days for vital vulnerabilities extensively lessen threat exposure. Failure to promptly patch exposes institutions to risks of ransomware, remote code execution, and data exfiltration.

7.7. Develop the Human Firewall

Cybersecurity is as much an individual problem as a technical one. Creating a "human firewall" involves entrenching cybersecurity awareness into the business culture. This comprises not just training but also leadership engagement, positive reinforcement, and the organisational of secure behaviour within every level (Deemantha, 2024). A cyber awareness culture is created through regular secure routines, reporting systems for irregular activity, and incorporating security into onboarding and performance evaluations. Hadnagy & Fincher (2021) stated that organisations that view employees as the first line of defense instead of the weakest link are well positioned to alleviate insider threats and social engineering attacks.

8. Conclusion

Cybersecurity in the government establishment is not only a technical issue, but it is a strategic imperative that needs a holistic and continuous dedication throughout every level of governance. As guardians of public databases, identity archives, tax records, public health systems, and other key digital assets, public organisations encounter unique vulnerabilities which require a multidimensional reaction (OECD, 2023). While endpoint protection, intrusion detection systems, and firewalls remain vital, these tools could not function in isolation. The latest threat landscape demands a sturdy cybersecurity posture that incorporates people, processes, and technologies into a unified defense structure (Pfleeger & Caputo, 2012).

8.1. Organizational Culture and Cyber Awareness

Cybersecurity awareness and behavioral change are fundamental components of this resilience. As individual error causes most of the cyber incidents (IBM, 2023), training civil servants to recognize threats such as malware, social engineering, and phishing is essential. Organizational culture plays an essential role; entrenching cybersecurity into workflows daily and reinforcing accountability at every level may significantly decrease insider threats and negligent behaviours (Hadnagy & Fincher, 2021).

8.2. Alignment with Global Standards and Frameworks

Public organisations must also affiliate their cybersecurity approaches with international best practices and frameworks like the NIST Cybersecurity Framework (2021), ISO/IEC 27001 (2022), and the CIS Controls (CIS, 2023). These frameworks offer a regulated method for identifying, mitigating, and recovering from cyber threats. Their importance of constant monitoring, governance, and adaptability makes them especially related for dynamic government ecosystems. Furthermore, domesticating an international standard through a national approach like Nigeria's National Cybersecurity Policy and Strategy (NCPS, 2021) makes sure that international standards are contextualized to address local infrastructural, legal, and cultural realities.

8.3. Learning from Case Studies and Threat Trends

Evidence-based policymaking, informed by real-world breaches and audit findings, is essential. Analysing notable cybersecurity events within public sectors, whether due to white papers, post-mortem reports, or simulation results assists in identifying systemic gaps and develop robust incident response abilities (NIST, 2022). The constant feedback loop from such case studies promotes better awareness and policy refinement.

8.4. Preparing for Emerging Threats

Looking ahead, authorities must proactively discover the cybersecurity effects of evolving technologies. Such as, quantum computing exhibits a dual-edged weapon: while it guarantees revolutionary advances in computing, it also pressures to render several present methods of encryption obsolete (Mosca, 2018). In preparation for the era of post-quantum cryptography, hence a need for early investments in research, frameworks regulation, and global collaboration. Likewise, the emergence of 5G, blockchain, Internet of Things, and artificial intelligence creates new prospects and threats. Cybersecurity governance must grow to control and

protect these technologies whilst balancing innovation with public interest (Gartner, 2023).

Final Thoughts

Cybersecurity in public institutions must be reframed from being a technical afterthought to an essential pillar of digital governance. Authorities must dedicate themselves to stakeholder engagement, policy harmonization, continuous capacity building, and forward-looking study to develop cyber-resilient institutions. The security of democratic processes, economic stability, and public trust gradually pivots on how effectively public establishments threaten and adapt to the cyber threat landscape.

References

[1] Adeleke, O., Onifade, A., and Ogunleye, A. (2023) 'Cybersecurity Policy Implementation in Nigeria: Challenges and Opportunities', *Journal of Cyber Policy and Governance*, 5(1), pp. 34–48.

[2] Akhgar, B. and Brewster, B. (2021) *Strategic Intelligence Management: National Security Imperatives and Information and Communications Technologies*. Elsevier.

[3] Australian Cyber Security Centre (2022) *Annual Cyber Threat Report 2021–2022*. Australian Government. Available at: https://www.cyber.gov.au (Accessed: 10 May 2025).

[4] Bada, M. and Nurse, J. R. C. (2019) 'The Social and Psychological Impact of Cybersecurity on Public Sector Organizations', *Journal of Cybersecurity*, 5(1), pp. 1–12.

[5] Center for Internet Security (CIS) (2023) *CIS Critical Security Controls Version 8*. Available at: https://www.cisecurity.org/ controls/cis-controls-list (Accessed: 10 May 2025).

[6] Creswell, J. W. and Poth, C. N. (2018) *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*, 4th edn. SAGE Publications.

[7] Cybersecurity and Infrastructure Security Agency (CISA) (2022) *Cybersecurity Advisory on Ransomware Threats*. U.S. Cybersecurity and Infrastructure Security Agency.

[8] Deemantha, N. S. (2024) 'Ransomware Threats Targeting the Healthcare Sector', *International Research Journal of Innovations in Engineering and Technology*, 8(1), pp. 158–167.

[9] Denzin, N. K. (2012) 'Triangulation 2.0', *Journal of Mixed Methods Research*, 6(2), pp. 80–88.

[10] European Union Agency for Cybersecurity (ENISA) (2023) *Threat Landscape for Public Sector Organizations*.

[11] Forrester (2023) *Zero Trust Extended Ecosystem Landscape, Q2 2023*.

[12] Gartner (2023) *Cybersecurity Trends and Forecasts*.

[13] Government Accountability Office (GAO) (2023) *Federal Agencies Need to Improve Supply Chain Risk Management*. U.S. Government Accountability Office.

[14] Hadnagy, C. and Fincher, M. (2021) *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails*. Wiley.

[15] IBM (2023) *Cost of a Data Breach Report 2023*. IBM Security. Available at: https://www.ibm.com/reports/data-breach (Accessed: 11 May 2025).

[16] International Organization for Standardization (ISO/IEC) (2022) *ISO/IEC 27001:2022 – Information Security Management Systems Requirements*.

[17] Keating, M. (2025) 'Ransomware is a Growing Threat, but Local Governments are Training Staffers to be More Aware', *The American City & County*.

[18] Kshetri, N. (2022) 'Cybersecurity in Government: Challenges and Solutions', *Government Information Quarterly*, 39(1).

[19] National Institute of Standards and Technology (NIST) (2021) *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*

[20] National Institute of Standards and Technology (NIST) (2022) *Cybersecurity Workforce Training Guide*.

[21] Organisation for Economic Co-operation and Development (OECD) (2023) *Building a Culture of Cybersecurity in the Public Sector*.

[22] Ponemon Institute (2021) *Cost of Insider Threats: Global Report*. Sponsored by ObserveIT and IBM.

[23] Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., and Guissanie, L. (2022) *Security and Privacy Controls for Information Systems and Organizations: NIST SP 800-53 Rev. 5*. National Institute of Standards and Technology.

[24] SANS Institute (2023) *Annual Phishing Simulation Benchmark Report*.

[25] Verizon (2023) *Data Breach Investigations Report (DBIR)*.

[26] Wang, Z., Zhu, H., and Liu, P. (2021) 'Social Engineering in Cybersecurity: A Domain Ontology and Knowledge Graph', *Cybersecurity*, 4(1).

[27] Yin, R. K. (2018) *Case Study Research and Applications: Design and Methods*, 6th edn. SAGE Publications.