Journal of Global Order, Security, and Policy Cultures
ISSN: 2806-3600
Vol: 3, Issue No.1, 2026

The Influence of Employee Technological Factors on the Management of Cybersecurity Breaches at the Independent Policing Oversight Authority, Kenya

Abdirahman, Omar Jibril
Researcher, Department of Security, Diplomacy and Peace Studies, Kenyatta University, Kenya
Omboto John Onyango, PhD
Lecturer, *Department of Security, Diplomacy and Peace Studies, Kenyatta University, Kenya*

***Published on**: 30/04/2026*

***DOI:** https://doi.org/10.5281/zenodo.19916275*

Abstract:

Purpose: This study examined how employee technological factors influence the management of cybersecurity breaches at the Independent Policing Oversight Authority (IPOA), Kenya. The research addressed concerns over increasing cyber incidents linked to employee technological weaknesses, including poor system use, limited digital literacy, and weak compliance with cybersecurity protocols.

Methodology: The study adopted a descriptive cross-sectional research design guided by General Deterrence Theory. From a target population of 290 IPOA employees, 160 respondents were selected using quota, convenience, and purposive sampling. Data were collected through structured questionnaires and semi-structured interviews, then analyzed quantitatively and qualitatively.

Findings: The findings established that employee technological factors significantly influence the management of cybersecurity breaches at IPOA. Employees with stronger digital literacy, higher technological competence, and better understanding of cybersecurity systems demonstrated improved ability to prevent, detect, and respond to cyber threats. Regression analysis showed a statistically significant relationship between technological competence and reduced occurrence of breaches. Qualitative findings further revealed that inadequate system familiarity, poor password practices, and low adherence to cybersecurity procedures contributed to phishing attacks, malware infections, and unauthorized access to sensitive case records. Improved system usability also enhanced employee compliance with cybersecurity measures.

Conclusion: The study concludes that employee technological capability is central to effective cybersecurity breach management in public institutions. IPOA should prioritize continuous ICT training, improve system usability, and strengthen technological support frameworks to enhance cybersecurity resilience and minimize vulnerabilities associated with employee technological weaknesses.

Keywords: *Employee technological factors, cybersecurity breaches, digital literacy, ICT competence, public sector cybersecurity, Kenya.*

1.0 Introduction

The rapid advancement of digital technologies has fundamentally transformed how organizations operate, store data, and deliver services. However, this digital transformation has simultaneously increased exposure to cybersecurity threats, particularly those linked to employee technological limitations. Despite heavy investments in advanced security systems, research consistently shows that human-related technological weaknesses — including poor digital literacy, inadequate password practices, and the inability to detect phishing attacks — remain a leading cause of cybersecurity breaches worldwide (Colabianchi et al., 2025; Alsharif et al., 2022). Organizations with low levels of employee technological readiness tend to report higher rates of system misconfigurations, delayed software updates, and improper use of security tools, all of which significantly increase vulnerability to cyberattacks.

In the United States, technological shortcomings among employees have been widely identified as a major contributor to cybersecurity breaches, especially in organizations that handle large volumes of sensitive data. High-profile incidents have demonstrated how misconfigured systems — often resulting from employee error or insufficient technical expertise — can lead to massive data exposures. Studies indicate that inadequate employee training and over-reliance on automated systems frequently result in poor monitoring practices, thereby allowing unauthorized access and prolonged system infiltration before detection (Garg, 2025).

In China, the rapid expansion of digital infrastructure and e-governance systems has made employee technological competence increasingly important for safeguarding organizational data. While the country has made significant investments in cybersecurity technologies, challenges persist due to disparities in employee digital skills and system usage capabilities. Research shows that employees who cannot effectively navigate complex systems, coupled with inadequate cybersecurity training, face increased risks of data breaches and system vulnerabilities (Alsharif et al., 2022).

In Nigeria, cybersecurity challenges are increasingly linked to employee technological inefficiencies, particularly within financial institutions and public organizations. Cases of unauthorized system access, data manipulation, and digital fraud have been attributed to poor technological skills, weak system controls, and inadequate cybersecurity awareness among employees. Studies reveal that gaps in ICT training and limited understanding of system functions expose organizations to internal vulnerabilities, with employees often unintentionally bypassing security protocols due to usability challenges or lack of technical knowledge (Ajufo & Qutieshat, 2023).

In Uganda, the adoption of digital systems in public administration and service delivery has introduced new cybersecurity risks associated with employee technological capacity. Evidence indicates that many institutions face challenges related to insufficient ICT training, poor system maintenance practices, and limited user competence in handling digital platforms. These factors

contribute to frequent system errors, weak access controls, and increased susceptibility to cyber threats.

In Kenya, the accelerated digitization of government services has increased exposure to cybersecurity risks, particularly those associated with employee technological factors. Reports indicate that system misconfigurations, poor password management, and inadequate cybersecurity training among employees have contributed to several high-profile breaches in public institutions (CAK, 2025). The Independent Policing Oversight Authority operates within this digital landscape, managing highly sensitive data including investigative reports and personal records. Despite the critical role of employee technological competence in safeguarding such information, empirical evidence on how these factors influence cybersecurity breaches within the Authority remains limited, thereby necessitating this study.

2.0 Problem Statement

Internal vulnerabilities arising from employee conduct have emerged as a leading cause of cybersecurity incidents in Kenya's public sector. According to the Communications Authority of Kenya (CAK, 2025), nearly one-third of all public-sector cyber incidents reported between 2020 and 2024 were attributed to staff errors or misuse, surpassing incidents caused by external malware and nation-state attacks. At IPOA, the 2024 annual security report documents 50 confirmed incidents during this period, including unauthorized access to case files, phishing-induced credential compromise, and malware infections affecting sensitive witness databases (IPOA, 2024). These incidents resulted in system downtime, costly forensic investigations, and exposure of confidential information, thereby undermining whistleblower protection and the credibility of the Authority's oversight functions.

While the CAK (2025) categorizes contributory factors into individual, technological, and organizational culture dimensions, this classification remains largely descriptive and does not empirically establish how specific employee-related technological factors translate into cybersecurity breaches within public institutions such as IPOA. Existing studies predominantly examine insider threats in generalized or private-sector contexts, often treating employee behaviour as a uniform risk factor. Although prior research emphasizes training deficits, risk perception, and weak policy enforcement as drivers of human error (Colabianchi et al., 2025; AL-Nuaimi, 2024), these studies offer limited institution-specific evidence and do not adequately explain why breaches persist despite enhanced technical controls and awareness programs — such as those implemented by IPOA in 2022. This gap necessitates an institution-focused empirical investigation.

3.0 Literature Review: The Influence of Technological Factors on Cybersecurity

Exploring how technological factors contribute to cybersecurity breaches requires examining the specific infrastructural and system-level weaknesses that expose organizations to internal and

external threats. Ewoh and Vartiainen (2024) conducted a systematic literature review of cybersecurity vulnerabilities in healthcare institutions and identified several recurring technical themes, including outdated IT infrastructure, inadequate monitoring systems, and weak security evaluation mechanisms. Their review showed that legacy systems running unsupported software accounted for a disproportionate share of breach incidents, as attackers routinely exploited known but unpatched vulnerabilities. The findings established a direct relationship between the age and quality of IT infrastructure and the frequency of successful cyberattacks — a pattern that extends beyond healthcare to public sector institutions generally.

Building on these infrastructural concerns, Pollini et al. (2022) examined how the usability of security technologies can itself become a source of vulnerability when human-machine interactions are poorly designed. Their mixed-methods study, anchored in a human factors framework and grounded in interviews with healthcare personnel in Italy, found that complex and poorly designed security interfaces drive employees to bypass or disable protective mechanisms. Users subjected to interfaces requiring multiple manual steps frequently opted for speed over security, inadvertently sharing data through unencrypted channels. Pollini et al. concluded that without integrating user-centred design principles into security tools, technological defences will remain underutilized and ineffective, converting rather than mitigating human-error vulnerabilities. This "usability-security trade-off" is especially relevant in resource-constrained public institutions.

Shifting from usability to organizational preparedness, Berlilana et al. (2021) applied a Technology-Organization-Environment (TOE) framework combined with Technology Readiness Index metrics to assess how technological readiness affects breach outcomes among 260 surveyed organizations. Using Structural Equation Modelling via SmartPLS, they found that robust IT infrastructure — comprising skilled personnel, modern hardware, and comprehensive software toolsets — positively correlated with cybersecurity readiness ($\beta = 0.62$, $p < 0.001$). Organizations with higher readiness scores reported significantly fewer successful intrusions, largely due to their capacity for rapid patch deployment and configuration management. Conversely, organizations relying on legacy systems and lacking dedicated IT experts exhibited longer detection and response times, creating extended windows for attackers. Berlilana et al. further noted that technology readiness supports not just technical defences but also the intangible benefit of a stronger security culture — reinforcing the critical role of systemic technology investment.

Complementing survey-based findings with practitioner insights, Dikito et al. (2024) conducted focus groups with IT experts and senior managers from Zimbabwean commercial banks to map application, network, database, physical, and internet security factors that influence breach risk. Their results revealed deficiencies in application security, noting that unpatched software and default system configurations leave APIs and web portals exposed to injection attacks. Participants unanimously viewed artificial intelligence and machine-learning monitoring tools as promising solutions for real-time anomaly detection, given the high transaction volumes that human operators cannot feasibly oversee alone. The study also emphasized that flat network architectures without

proper segmentation enable lateral movement once an attacker gains a foothold, often resulting in full domain compromise within hours. Database security lapses — including insufficient encryption and coarse access controls — allowed internal users to execute unauthorized queries on customer records. These findings collectively illustrate how a weakness in any single technological layer can cascade across an organization's entire digital infrastructure.

Turning to the interplay between systemic vulnerabilities and their exploitation, Kadena and Gupi (2021) documented how hardware, software, and network protocol flaws translate directly into real-world breach vectors. Their analysis showed that hardware trojans — malicious implants embedded within chips — can subvert core security functions such as cryptographic modules and error-checking circuits, enabling attackers to bypass integrity checks. In the software domain, buffer-overflow exploits were highlighted as a primary mechanism for remote code execution, with simple input-validation failures capable of cascading into full system takeovers. These findings underscore that technical vulnerabilities are not passive risks; in the absence of active monitoring and patching, they become reliable pathways for attack.

Butavicius et al. (2020) explored a different dimension of technological risk: the tendency of employees to over-trust technical controls. Through the development and validation of a Trust in Technical Controls Scale (TTCS) with a survey of 607 Australian employees, they found that excessive confidence in firewalls and antivirus software correlated with poorer phishing detection rates. Participants who rated their trust in antivirus tools in the top quartile exhibited a 25% higher click-through rate on simulated phishing emails than those with moderate trust levels, suggesting that perceived technological infallibility leads to relaxed vigilance. Conversely, moderate scepticism about automated defences appeared to motivate greater user caution. Butavicius et al. (2020) concluded that technological safeguards, if perceived as all-powerful, can inadvertently undermine human security behaviour — a finding with direct relevance to organizations that invest heavily in technology without equally investing in security awareness.

Aslan et al. (2023) broadened the scope by examining how emerging technologies introduce novel vulnerabilities. They documented that the proliferation of Internet of Things (IoT) endpoints expands the attack surface exponentially, with the limited processing capacity of these devices precluding robust encryption or real-time anomaly detection. The multi-tenant nature of cloud infrastructures — where data from different organizations share physical hardware — creates side-channel and hypervisor escape vectors that can expose sensitive information. Their review of critical infrastructure systems further illustrated how industrial control protocols lacking encryption render these systems susceptible to replay and spoofing attacks. Aslan et al. concluded that emerging technologies must be accompanied by rigorous, technology-specific security controls if their operational benefits are not to be offset by their security costs.

4.0 Theoretical Framework: General Deterrence Theory

General Deterrence Theory (GDT) originates in classical criminology, most notably in the work of Cesare Beccaria and Jeremy Bentham in the late eighteenth century. Beccaria's treatise On

Crimes and Punishments (1764) argued that punishment should be prompt, certain, and proportionate to the offence in order to deter criminal behaviour. Bentham's utilitarian philosophy further developed this into a cost-benefit calculus: individuals will comply with rules when the anticipated pain of punishment outweighs the perceived gains of transgression. These ideas were later developed by twentieth-century criminologists who shifted focus toward how societal perceptions of detection likelihood and penalty severity shape behavioural norms. GDT has since been applied across diverse compliance domains, from traffic regulation and tax enforcement to, most recently, information security (Bhattacherjee & Shrivastava, 2018).

At its core, GDT posits three interrelated mechanisms — certainty, severity, and swiftness of sanctions — that collectively shape an individual's deterrence calculus. Certainty refers to the perceived probability that a policy violation will be detected and sanctioned. When employees believe that monitoring systems are robust and infractions are consistently uncovered, they are less inclined to risk non-compliance. Severity captures how harsh the consequences of a detected breach will be, ranging from formal warnings to termination or legal action. The greater the anticipated penalty, the stronger the disincentive for misconduct. Swiftness describes the temporal proximity between the infraction and its sanction; delays in enforcement weaken the cognitive link between action and consequence, reducing deterrent effects. Together, these three dimensions determine whether individuals perceive compliance as the rational choice.

These mechanisms map directly onto the problem of cybersecurity breaches by shaping employees' behavioural calculations. When certainty is low — because monitoring systems are limited or log reviews are infrequent — staff perceive that risky behaviours such as sharing credentials or disabling security settings will go unnoticed. Likewise, when policy violations result only in informal warnings rather than meaningful consequences, potential wrongdoers calculate that operational convenience outweighs the mild reprimand. When investigations unfold slowly, the cognitive link between a breach and its consequences weakens further (Alanezi & Brooks, 2014). Under such conditions, employees — whether acting deliberately or carelessly — are more likely to circumvent cybersecurity protocols.

GDT aligns directly with the purpose of this study, which investigates how employee-related factors influence cybersecurity breaches at IPOA. Under the theoretical lens of GDT, individual-level factors — such as work experience and technical knowledge — shape how employees perceive the likelihood and severity of being sanctioned for non-compliance. At the technological level, the presence of real-time monitoring systems and automated alerts increases the perceived certainty of detection, which in turn reinforces compliance behaviour. At the organizational level, visible enforcement by senior leadership and consistent application of disciplinary measures communicate both severity and swiftness, embedding cybersecurity as a core institutional value rather than a formality. Collectively, these dimensions allow GDT to explain variation in breach incidence across different institutional contexts.

While GDT is valuable for explaining deliberate non-compliance through a rational-choice model, it has limitations. It presumes that employees always act as fully rational actors and does not

adequately account for breaches rooted in unintentional errors, cognitive overload, or misunderstanding of protocols. It also underestimates the role of organizational culture and social norms in shaping security behaviour — factors that are better addressed through complementary frameworks. By situating GDT within a broader analytical lens that acknowledges both rational and non-rational drivers of behaviour, this study is better positioned to explain the complex relationship between employee technological factors and cybersecurity breaches at IPOA.

5.0 Study Area and Research Methodology

The research was conducted in Nairobi City County, selected because it serves as the administrative and operational hub of the Independent Policing Oversight Authority and concentrates the critical ICT infrastructure and personnel responsible for handling sensitive digital information. Nairobi's central role in public sector digitization made it an appropriate setting for examining how employee technological factors influence cybersecurity breaches. The target population comprised all employees who interact with digital systems, including technical staff, operational personnel, and senior management, since these groups play a direct role in system use, data handling, and cybersecurity practices.

The study employed a combination of purposive, quota, and convenience sampling techniques to select respondents. Purposive sampling targeted key informants — particularly ICT staff and senior managers — based on their expertise in cybersecurity management. Quota sampling ensured proportional representation across different staff categories, and convenience sampling was used to reach available respondents at the Nairobi headquarters and regional office. From a total population of 290 employees, a sample of 160 respondents was selected, alongside six to eight key informants who provided in-depth qualitative insights into technological challenges and cybersecurity practices.

Data collection was carried out using structured questionnaires and semi-structured interviews. The questionnaires gathered quantitative data on employee technological factors — including digital literacy, system usability, cybersecurity training, and adherence to security protocols — as well as on direct experience with cybersecurity incidents. Semi-structured interviews with key informants captured qualitative insights on system vulnerabilities, technological constraints, and organizational cybersecurity practices. Interviews were recorded to ensure accuracy, and secondary data were obtained from peer-reviewed journals, institutional reports, and credible official sources.

To ensure validity and reliability, the research instruments were pretested and reviewed by experts in cybersecurity and research methodology. Reliability of the questionnaire was assessed using Cronbach's alpha, with a threshold of 0.70 considered acceptable. Quantitative data were analyzed using SPSS through descriptive statistics and multiple linear regression to examine relationships between technological factors and cybersecurity breaches, while qualitative data were analyzed thematically. Ethical standards were upheld by ensuring voluntary participation, informed consent,

confidentiality, and secure handling of data — considerations of particular importance given the sensitive nature of the subject matter.

6.0 Research Findings

This section presents the descriptive analysis of technological factors and their influence on the management of cybersecurity breaches at IPOA. Descriptive statistics — including frequencies, means, and standard deviations — were used to summarize respondents' views on the statements used to measure this variable.

Table 1: Descriptive Analysis for Technological Factors

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	Std. Dev.
IPOA has the necessary technical skills and expertise to deploy and maintain cybersecurity tools effectively	0.0%	0.0%	27.3%	50.0%	22.7%	3.95	0.71
I feel confident in my ability to use the cybersecurity solutions provided by IPOA without extensive external support	4.5%	31.8%	22.7%	27.3%	13.6%	3.14	1.14
IPOA hardware and software systems are up to date and reliable	9.1%	13.6%	18.2%	36.4%	22.7%	3.50	1.24
The network and endpoint security configurations at IPOA adequately protect against common vulnerabilities	4.5%	13.6%	22.7%	40.9%	18.2%	3.55	1.08
IPOA monitoring systems (e.g., intrusion detection, log analysis) promptly alert me to suspicious activities	0.0%	13.6%	40.9%	31.8%	13.6%	3.45	0.89
I trust that IPOA cybersecurity tools can accurately detect and report potential threats before they cause damage	4.5%	13.6%	22.7%	50.0%	9.1%	3.45	0.99
Aggregate Mean Score						**3.51**	**1.01**

Source: Survey Data (2025)

The aggregate mean score for the technological factors variable was 3.51 (SD = 1.01), indicating a generally high level of agreement among respondents that technological factors influence cybersecurity breaches at IPOA. The relatively low standard deviation suggests that respondents held broadly similar views. These findings are consistent with those of Ewoh and Vartiainen (2024), who linked cybersecurity breaches to technical vulnerabilities — including poor ICT

infrastructure, weak monitoring systems, and inadequate security evaluation — and found that outdated systems accounted for a substantial proportion of cyber incidents.

Specifically, when asked whether IPOA has the necessary technical skills and expertise to deploy and maintain cybersecurity tools effectively, 72.7% of respondents agreed or strongly agreed (mean = 3.95). However, when asked whether they personally felt confident using these tools without extensive external support, only 41% agreed or strongly agreed (mean = 3.14), with 31.8% disagreeing. This gap between organizational capacity and individual confidence is significant, as it points to a layer of human-technology interaction risk that strong institutional infrastructure alone cannot address.

Regarding hardware and software currency, 59.1% of respondents agreed or strongly agreed that IPOA's systems were up to date and reliable (mean = 3.50), while 59.1% also agreed that network and endpoint security configurations adequately protected against common vulnerabilities (mean = 3.55). On the functionality of monitoring systems, 40.9% were neutral and 45.4% agreed or strongly agreed that intrusion detection and log analysis tools promptly alerted them to suspicious activity (mean = 3.45). Similarly, 59.1% agreed that IPOA's cybersecurity tools could accurately detect and report potential threats before causing damage (mean = 3.45).

Qualitative evidence reinforced these findings. One key informant noted: "IPOA's IT infrastructure is robust, with secure networks, firewalls, and intrusion detection systems that effectively counter common threats. The remote backup facility in Nakuru also serves as a fallback resource in the event of an attack." These views align with findings from Berlilana et al. (2021), Pollini et al. (2022), and Dikito et al. (2024), all of whom identified system complexity, availability of human expertise, and deficiencies in application security as key technological factors that expose institutions to cybersecurity breaches.

7.0 Summary and Conclusion

This study assessed the influence of technological factors on the management of cybersecurity breaches at IPOA. The findings revealed that IPOA possesses the necessary technical skills and infrastructure to deploy and maintain cybersecurity tools, indicating strong institutional capacity at the IT and systems administration level. However, the gap between organizational capability and individual staff confidence — as reflected in the lower mean score for personal self-efficacy with cybersecurity tools — points to a persistent vulnerability in the human-technology interface. The aggregate findings indicate a moderately strong technological foundation, but without parallel improvements in staff confidence, usability of systems, and trust in technology, IPOA remains susceptible to breaches that exploit these interaction gaps.

Inferential analysis confirmed that technological factors emerged as a significant predictor of cybersecurity breach management, indicating that the effective deployment of cybersecurity tools and the maintenance of updated systems significantly reduce the likelihood of breaches. This supports the theoretical framework of General Deterrence Theory, which suggests that visible and

credible technological monitoring increases employees' perceived certainty of detection and thus reduces risky behaviour.

The study concluded that robust technological mechanisms — including up-to-date hardware and software systems, reliable network and endpoint security configurations, and functional monitoring and alerting tools — are essential to reducing cybersecurity vulnerabilities. At the same time, organizational factors such as open communication about incidents and leadership-led reinforcement of security protocols complement these technical measures by sustaining vigilance among employees.

8.0 Recommendations

Based on the study's findings and conclusions, the following recommendations are made:

First, IPOA management should institutionalize hands-on cybersecurity training on at least an annual basis, ensuring that all employees — particularly those who expressed low confidence in using security tools — acquire both the knowledge and practical competence needed to navigate cybersecurity systems effectively. Training programs should be designed not just to transmit information but to build genuine confidence through simulation exercises and scenario-based learning.

Second, the Authority should invest in improving the usability of its cybersecurity tools. As Pollini et al. (2022) and Butavicius et al. (2020) demonstrate, complex or poorly designed interfaces encourage workarounds that undermine security. Streamlining security procedures and adopting user-centred design principles would reduce procedural friction and improve compliance.

Third, organizational leadership should ensure regular, timely, and transparent communication about new cybersecurity policies, emerging threats, and incident responses. Senior management should consistently model and communicate the importance of cybersecurity, embedding it as a core institutional value rather than a compliance requirement. This reinforces both the deterrent effect of sanction certainty and the normative pressure of organizational culture on employee behaviour.

Finally, IPOA should cultivate a culture of accountability by sensitizing employees to the specific consequences of non-compliance with cybersecurity guidelines, and by ensuring that disciplinary measures are applied consistently and promptly — in line with the swiftness principle of General Deterrence Theory.

9. References

Ajufo, G., & Qutieshat, A. (2023). An examination of the human factors in cybersecurity: Future directions for Nigerian banks. Indonesian Journal of Information Systems, 6(1), 1–16. https://doi.org/10.24002/ijis.v6i1.6639

Alanezi, F., & Brooks, L. (2014). Combatting online fraud in Saudi Arabia using General Deterrence Theory (GDT). In Proceedings of the UK Academy for Information Systems (UKAIS) Conference. https://core.ac.uk/download/pdf/301361896.pdf

AL-Nuaimi, M. N. (2024). Human and contextual factors influencing cybersecurity in organizations, and implications for higher education institutions: A systematic review. Global Knowledge, Memory and Communication, 73(1/2), 1–23. https://doi.org/10.1108/GKMC-07-2022-0168

Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of human vulnerabilities on cybersecurity. Computer Systems Science & Engineering, 40(3), 1153–1166. https://doi.org/10.32604/csse.2022.019938

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cybersecurity vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333

Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization benefit as an outcome of organizational security adoption: The role of cybersecurity readiness and technology readiness. Sustainability, 13(24), 13761. https://doi.org/10.3390/su132413761

Bhattacherjee, A., & Shrivastava, U. (2018). The effects of ICT use and ICT laws on corruption: A General Deterrence Theory perspective. Government Information Quarterly, 35(4), 703–712. https://doi.org/10.1016/j.giq.2018.07.006

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M., & Calic, D. (2020). When believing in technology leads to poor cybersecurity: Development of a trust in technical controls scale. Computers & Security, 98, 102020. https://doi.org/10.1016/j.cose.2020.102020

CAK. (2024). Cybersecurity Report: 36th Edition October–December 2024. Communications Authority of Kenya.

CAK. (2025). Cybersecurity Report: 37th Edition January–March 2025. Communications Authority of Kenya.

Colabianchi, S., Costantino, F., Nonino, F., & Palombi, G. (2025). Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. Journal of Innovation & Knowledge, 10(3), 100695. https://doi.org/10.1016/j.jik.2025.100695

Dikito, A. R., Kaiser, M. S., & Vincent, J. P. (2024). Factors influencing cybersecurity: A focus group approach. International Journal of Academic Research in Progressive Education and Development, 13(4), 1–18. https://doi.org/10.6007/IJARPED/v13-i4/23539

Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review. Journal of Medical Internet Research, 26, e46904. https://doi.org/10.2196/46904

Garg, S. (2025). Understanding employee vulnerability to cyberattacks using the lens of strategic human resource management. The International Journal of Human Resource Management, 36(19), 3401–3436. https://doi.org/10.1080/09585192.2025.2601788

IPOA. (2024). Annual Report 2023/2024. Independent Policing Oversight Authority, Nairobi, Kenya.

Kadena, E., & Gupi, M. (2021). Human factors in cybersecurity: Risks and impacts. Security Science Journal, 2(2), 51–64. https://www.securityscience.edu.rs/index.php/journal-security-science/article/view/54

Maphosa, V. (2024). An overview of cybersecurity in Zimbabwe's financial services sector. F1000Research, 12, 1251. https://doi.org/10.12688/f1000research.132823.2

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. Cognition, Technology & Work, 24(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y