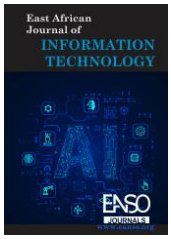
Article DOI: https://doi.org/10.37284/eajit.8.1.3283



East African Journal of Information Technology
eajit.eanso.org
Volume 8, Issue 1, 2025
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Has Increased Digitisation of Services Led to More Cyber Exposure? A Desk Review

Morrisson Mutuku, PhD[1]

[1] Kenyatta University, P. O. Box 43844 00100, Nairobi, Kenya.
[*] Author for Correspondence ORCID ID; https://orcid.org/0000-0003-0662-7157; Email: mutuku.morrisson@ku.ac.ke

Article DOI: https://doi.org/10.37284/eajit.8.1.3283

Date Published:

08 July 2025

Keywords:

Digitisation, Cybersecurity, Exposure, Africa, Kenya.

ABSTRACT

The rapid process of digitisation of services has changed economies, altered social relationships and changed the governance processes across geographies. It has, however, exposed people, organisations, and governments to numerous cyber threats. This paper discusses the relationship between digitalisation of services and cyber exposure by the use of the desk review method. Using international reports and focusing on global, African and Kenyan research, the paper has been able to identify a similar pattern nationally and internationally: although digitisation contributes to efficiency, it also increases the number of chances to get hacked, particularly when the cybersecurity capacity is lower than expected. Cybercrime has been on the increase in Kenya, especially in the areas of finance and e-commerce, as well as government services. In conclusion, the paper will argue that to make digital transformation as sustainable, there is a need to mainstream cybersecurity in digital transformation policies.

APA CITATION

Mutuku, M. (2025). Has Increased Digitisation of Services Led to More Cyber Exposure? A Desk Review. *East African Journal of Information Technology*, *8*(1), 320-326. https://doi.org/10.37284/eajit.8.1.3283.

CHICAGO CITATION

Mutuku, Morrisson. "Has Increased Digitisation of Services Led to More Cyber Exposure? A Desk Review". *East African Journal of Information Technology* 8 (1), 320-326. https://doi.org/10.37284/eajit.8.1.3283.

HARVARD CITATION

Mutuku, M. (2025) "Has Increased Digitisation of Services Led to More Cyber Exposure? A Desk Review", *East African Journal of Information Technology*, 8(1), pp. 320-326. doi: 10.37284/eajit.8.1.3283.

IEEE CITATION

M. Mutuku "Has Increased Digitisation of Services Led to More Cyber Exposure? A Desk Review", *EAJIT*, vol. 8, no. 1, pp. 320-326, Jul. 2025.

MLA CITATION

Mutuku, Morrisson. "Has Increased Digitisation of Services Led to More Cyber Exposure? A Desk Review". *East African Journal of Information Technology*, Vol. 8, no. 1, Jul. 2025, pp. 320-326, doi:10.37284/eajit.8.1.3283.

Article DOI: https://doi.org/10.37284/eajit.8.1.3283

INTRODUCTION

Digital transformation has revolutionised the provision of services across both public and private sectors. Innovations in mobile applications, artificial intelligence (AI), cloud computing, and the Internet of Things (IoT) have enabled faster, broader, and more data-driven service delivery (Mutuku & Muathe, 2020; World Economic Forum, 2023). However, the expanded reliance on digital ecosystems has simultaneously intensified cyber vulnerabilities. Studies show that while digitisation enhances efficiency and accessibility, it also introduces more complex cyber threats, particularly where security frameworks, public awareness, and regulatory mechanisms remain underdeveloped (Waliullah et al., 2025).

Globally, cybercrime is rising at a staggering pace. According to Cybersecurity Ventures (2020), cybercrime damages are projected to hit USD 10.5 trillion annually by 2025, up from USD 3 trillion in 2015. Aon and the World Economic Forum (2023) identify cyberattacks among the top five business risks globally. These threats are not limited to monetary loss; they include data breaches, ransomware, espionage, and service disruption, affecting institutions of all sizes. Cloud environments, in particular, have become prime targets, with 82% of reported breaches in 2023 involving cloud-based data (Forbes, 2024). Europe has been at the forefront of digital transformation, with the European Commission promoting a digital single market strategy and ambitious plans under the *Digital Europe Programme* and *Europe's Digital Decade* targets. Key sectors—including banking, healthcare, transportation, education, and public administration—have increasingly adopted digital technologies such as artificial intelligence, cloud services, big data, and the Internet of Things (IoT). While this digitisation has streamlined services, improved governance, and enhanced access, it has simultaneously expanded the region's cyber threat surface.

Over the past decade, cyberattacks in Europe have become more frequent, sophisticated, and damaging. According to the European Union Agency for Cybersecurity (ENISA, 2022), ransomware attacks in Europe increased by 150% between 2019 and 2021, and phishing attacks targeting public and private institutions rose by over 85% during the COVID-19 pandemic. In the healthcare sector, for example, hospitals in Germany, Ireland, and France experienced severe ransomware attacks that disrupted patient care and compromised sensitive data (Heinlein & Schäfer, 2021). Meanwhile, the financial sector has seen a sharp rise in credential theft, digital fraud, and denial-of-service attacks, prompting regulatory responses such as the EU's Network and Information Security Directive (NIS2) and the General Data Protection Regulation (GDPR).

Countries like Estonia, often cited as digital leaders, have also been targeted. In 2022, Estonia reported a record-breaking number of cyber incidents, despite its mature cybersecurity posture (Estonian Information System Authority, 2023). In the UK, the National Cyber Security Centre (NCSC) recorded over 2.7 million cases of cyber fraud in 2022 alone (NCSC, 2023). Smaller EU economies such as Bulgaria, Romania, and Croatia face even steeper challenges due to limited investment in cybersecurity infrastructure and expertise. Overall, while Europe benefits from its digital-first agenda, increased reliance on digital services has undoubtedly led to greater cyber exposure. The region's experience underscores the importance of not just expanding digital services but concurrently strengthening cybersecurity policies, cross-border cooperation, and cyber resilience mechanisms to mitigate the risks of digital dependence.

In North America, the United States experiences some of the highest volumes of cyberattacks globally. The FBI's Internet Crime Complaint Center (IC3) reported over 880,000 complaints in 2023 alone, with losses exceeding USD 12.5 billion—up from USD 1.4 billion in 2017 (FBI IC3,

Article DOI: https://doi.org/10.37284/eajit.8.1.3283

2024). Major sectors affected include healthcare, education, and financial services. Notably, the Colonial Pipeline ransomware attack in 2021 disrupted critical infrastructure, sparking legislative and regulatory reforms in cybersecurity. Asia has also seen a dramatic surge in cyber incidents, particularly in fast-growing digital economies like India, China, and Southeast Asia. India's CERT-IN (2023) reported over 1.4 million cybersecurity incidents in 2022, up from 208,000 in 2018. China's digitisation through platforms like WeChat, Alipay, and government e-services has been paralleled by sophisticated cyber espionage, phishing, and data breaches (Li et al., 2022). Southeast Asia, home to emerging fintech markets, has seen a 200% rise in ransomware and e-commerce fraud between 2019 and 2023 (Interpol, 2023).

In Australia, digitisation has grown significantly across public services, with initiatives such as MyGov and digital health records. However, high-profile breaches—including the 2022 Optus and Medibank hacks—exposed millions of personal records and prompted national cybersecurity overhauls (Australian Cyber Security Centre, 2023). The government has since pledged over AUD 2.3 billion toward enhancing national cyber defence through its 2023–2030 Cyber Security Strategy. Across Africa, the digital transformation is accelerating, especially in mobile banking and e-governance. However, cyber resilience lags behind. In Kenya, cyber threat events rose from under 20 million in 2013 to over 860 million in Q4 2023 alone (CAK, 2024). Financial fraud, SIM-swap scams, and ransomware are particularly rampant. Similarly, in Nigeria and South Africa, weak regulatory enforcement and limited cybersecurity investments make institutions vulnerable (Aguboshim & Udokwu, 2020; Mutune et al., 2023). The African Union's Convention on Cyber Security (Malabo Convention) remains under-implemented. In Kenya, the rise in digital adoption has not been matched by robust cybersecurity measures. As M-PESA and eCitizen continue to redefine service delivery, cyber threats to SMEs, government portals, and financial systems have increased significantly (Kabaya & Kageni, 2024).

These global, African and Kenyan trends confirm a global paradox: as digital transformation expands, so does cyber exposure. Without matching investments in cybersecurity infrastructure, training, and policy enforcement, the promise of digitisation may be overshadowed by growing threats to data, privacy, and national stability.

Research indicates that critical infrastructures such as financial systems, healthcare services, and supply chains are increasingly susceptible to evolving threat vectors. For instance, Waliullah et al. (2025) found that fintech platforms are regularly targeted by phishing, ransomware, and malware attacks. Likewise, Radanliev et al. (2018) and Turel et al. (2021) showed how IoT expansion widens the attack surface, complicating cyber defence mechanisms. Another review by Sowon et al. (2024) proposed privacy-preserving protocols to reduce cyber risk in agent-assisted mobile money transactions.

The gap between cyber risk awareness and readiness remains stark. A PwC (2024) global survey fewer than 15% had implemented comprehensive risk mitigation strategies such as zero-trust architecture or real-time threat intelligence systems. Despite these efforts, vulnerabilities persist, especially in regions experiencing rapid digitisation without proportional cybersecurity investment.

This background frames a fundamental revealed that while over 55% of business leaders ranked cybersecurity among their top concern: Has the accelerated digitisation of services led to greater exposure to cyber risks both globally and in Kenya? This desk review seeks to examine this critical question using empirical insights from recent literature.

Article DOI: https://doi.org/10.37284/eajit.8.1.3283

Statement of the Problem

Over the past decade, Kenya has witnessed exponential growth in digital service delivery across sectors such as finance, healthcare, commerce, and government. This digitisation has significantly enhanced efficiency, accessibility, and economic participation. However, it has also exposed the country to escalating cyber threats, which have consistently outpaced the development of corresponding cybersecurity safeguards. This mismatch between digital growth and cyber resilience presents a pressing national challenge.

Statistical trends reveal a concerning trajectory. In 2013, cyber threat incidents in Kenya were minimal, with fewer than 4 million reported annually (Serianu, 2014). By 2018, threats had surged to over 51 million (CAK, 2018), marking a 135% increase from the previous year. The trend continued, with the country recording nearly 200 million cyber threat events in 2020 (CAK, 2020). This number more than quadrupled by the end of 2023, with 860.9 million threats reported in the fourth quarter alone—a 61.8% jump from the previous quarter (CAK, 2024). The rise in incidents is particularly acute in the financial services sector, e-government platforms, and among small and medium-sized enterprises (SMEs), which remain ill-prepared to withstand sophisticated cyberattacks (Musau, 2024).

Despite efforts by the Kenyan government to improve cybersecurity through the National Cybersecurity Strategy (2022–2027) and the Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC), capacity constraints persist. A shortage of cybersecurity professionals, fragmented institutional coordination, and low public digital literacy exacerbate the problem (Obuhuma & Zivuku, 2020; Serianu, 2019). Without urgent interventions, Kenya risks not only financial loss but also erosion of public trust in digital platforms, disruption of critical infrastructure, and impediments to future digital innovation (Too & Mutuku, 2023).

LITERATURE REVIEW

Jamilov et al. (2021) describe cyber risk as a systemic threat influenced by digital infrastructure, user behaviour, and institutional resilience. Their macroeconomic study finds that countries with advanced digital ecosystems face more frequent and complex cyberattacks. Aldasoro et al. (2022) note that the financial sector's digitisation increases vulnerability due to interconnected systems and real-time transactions. Milani et al. (2022) find that increased online engagement, particularly on social platforms and digital services, raises the likelihood of victimisation. Radanliev et al. (2018) warn that the proliferation of IoT devices, often lacking security protocols, is expanding the global cyberattack surface. Turel et al. (2021) argue that cognitive and behavioural limitations among users contribute to security lapses in digital environments.

Mutune et al. (2023) report frequent data breaches and fraud in mobile money platforms, which are widely used across East Africa. Bada and Sasse (2015) reveal a critical deficit in cybersecurity education and awareness among African users. Rutenberg and Omariba (2022) highlight challenges in maintaining data privacy in Africa's digitising health sector. Aguboshim and Udokwu (2020) examine West African nations, pointing out the limited capacity of institutions to detect and respond to cyber threats. Mothobi and Chair (2019) stress that Africa's digital progress has outstripped its cybersecurity policies, creating a dangerous imbalance.

In Kenya, Ndeda and Odoyo (2019) warn that SMEs, which form the backbone of the economy, are highly vulnerable to cybercrime due to poor security frameworks. Waithaka (2016) identifies inadequate cybersecurity staffing and inconsistent strategies in government ministries. Kabaya and Kageni (2024) highlight how Kenya's ambition to embrace Industry 4.0 technologies is not matched

Article DOI: https://doi.org/10.37284/eajit.8.1.3283

by corresponding cyber risk preparedness. Karanja and Gatobu (2024) show that fintech firms using IoT tools experience frequent digital fraud attacks. Wekundah (2015) developed a cybersecurity model for SMEs but noted low adoption due to financial and technical barriers.

METHODOLOGY

This study employed a desk review methodology, systematically examining existing secondary sources including journal articles, dissertations, industry reports, and institutional publications. Selection criteria included recency (post-2015), geographic scope (global, African, and Kenyan focus), and relevance to cyber risk and digitisation. Databases such as Google Scholar, IEEE, JSTOR, and the World Economic Forum database were utilised. A total of 25 publications were selected, offering a triangulated understanding of how digitisation correlates with cyber exposure. The choice of 25 articles strikes a methodological balance, offering sufficient breadth to capture major trends and insights, and enough focus to allow for detailed, meaningful interpretation.

FINDINGS AND DISCUSSION

The reviewed literature provides robust evidence that increased digitisation correlates with higher cyber exposure. Advanced economies with extensive digitisation face sophisticated and frequent cyberattacks. However, they also exhibit stronger cybersecurity infrastructure and enforcement mechanisms. The global cost of cybercrime continues to surge, with sectors like finance, health, and e-commerce most at risk. Africa shows a widening gap between digital adoption and cybersecurity infrastructure. Mobile money, e-health, and digital identity systems are growing rapidly, but institutional readiness remains low. Public education on cyber hygiene is underdeveloped, and legal frameworks are often outdated. Kenya's digitisation trajectory has been lauded, but the rise in cyber incidents is alarming. Threat vectors include social engineering, ransomware, and phishing, especially in sectors such as fintech, e-government, and e-commerce. SMEs are disproportionately affected due to limited budgets and skills. Governmental efforts, including the 2019 National Cybersecurity Strategy, are ongoing but require full implementation.

CONCLUSION AND RECOMMENDATIONS

Conclusion

The evidence indicates that increased digitisation leads to increased cyber exposure, particularly in contexts where cybersecurity frameworks, capacity, and user awareness are weak. Kenya, while digitally advanced, faces significant risks that could undermine its socio-economic gains if not urgently addressed.

Recommendations

- Mainstream Cybersecurity in Digital Policies: All digital transformation plans should include cybersecurity as a core pillar.
- SME Support Programs: The government should provide financial and technical support to SMEs for cybersecurity tools and training.
- National Awareness Campaigns: Improve cyber hygiene through mass media, school curriculums, and corporate training.
- Stronger Legislation and Enforcement: Update cyber laws and improve enforcement to deter and prosecute cybercrime effectively.
- Investment in Research and Innovation: Universities and think tanks should be supported to lead localised research into emerging threats and indigenous solutions.

REFERENCES

Aguboshim, A. C., & Udokwu, F. C. (2020). Cybersecurity Threats in West Africa. *African Journal of Security Studies*, 8(1), 45–60.

Article DOI: https://doi.org/10.37284/eajit.8.1.3283

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, 60, 100989.

Aon & World Economic Forum. (2023). *Global Risks Report*. Retrieved from https://www.weforum.org

Australian Cyber Security Centre. (2023). *Annual Cyber Threat Report: July 2022 to June 2023*.

Bada, A., & Sasse, M. A. (2015). Cybersecurity awareness campaigns: Why do they fail to change behaviour? *arXiv preprint* arXiv:1505.07676.

Bada, A., & Sasse, M. A. (2015). Cybersecurity awareness campaigns: Why do they fail to change behavior? *arXiv preprint arXiv:1505.03873*.

CAK. (2024). *Cybersecurity Report Q4 2023*. Communications Authority of Kenya.

CERT-IN. (2023). *Cybersecurity Incidents Report 2022*. Indian Computer Emergency Response Team.

Communications Authority of Kenya (CAK). (2018). *Quarterly Sector Statistics Report: Q4 2018*. Nairobi: CAK.

Communications Authority of Kenya (CAK). (2020). *Quarterly Sector Statistics Report: Q4 2020*. Nairobi: CAK.

Communications Authority of Kenya (CAK). (2024). *Cybersecurity Statistics Report Q4 2023*. Nairobi: CAK.

Communications Authority of Kenya. (2020–2024). Quarterly Sector Statistics Reports.

Cybersecurity Ventures. (2020). *Cybercrime to Cost the World $10.5 Trillion Annually by 2025*. Retrieved from https://cybersecurityventures.com

ENISA. (2022). *Threat Landscape 2022*. European Union Agency for Cybersecurity.

Estonian Information System Authority. (2023). *Cybersecurity in Estonia: Annual Report*.

FBI IC3. (2024). *Internet Crime Report 2023*. Federal Bureau of Investigation.

Forbes. (2024). *Why Cybersecurity Breaches Are Increasing*. Retrieved from https://www.forbes.com

Interpol. (2023). *ASEAN Cyber Threat Assessment Report*.

Jamilov, R., Rey, H., & Tahoun, A. (2021). The anatomy of cyber risk. *National Bureau of Economic Research* (No. w28906).

Kabaya, J., & Kageni, M. (2024). Cybersecurity preparedness in Kenya's digital economy. *African Journal of ICT Studies*, 6(2), 87–95.

Kabaya, M., & Kageni, M. (2024). Cybersecurity in the wake of the fourth industrial revolution in Kenya.

Karanja, M. W., & Gatobu, P. (2024). IoT and cyber attacks among fintech companies in Kenya. *IJSSME*, 8(1).

Li, T., Zhang, Y., & Wu, M. (2022). Digital Transformation and Cyber Risks in China. *Journal of Information Security*, 11(4), 251–268.

Milani, M., d'Addona, D., & Teti, R. (2022). Individual cyber-victimization and behavioral patterns. *Computers & Security, 112*, 102541.

Milani, R., Caneppele, S., & Burkhardt, C. (2022). Exposure to cyber victimization: Results from a Swiss survey. *Deviant Behavior*, 43(2), 228-240.

Musau, D. (2024). Alarm as Kenya Records 860 Million Cyber Threats in Q4. *Citizen Digital*. Retrieved from https://citizen.digital

Article DOI: https://doi.org/10.37284/eajit.8.1.3283

Mutuku, M. K., & Muathe, S. M. (2020). Nexus analysis: Internet of Things and business performance. *International Journal of Research in Business and Social Science*, *9*(4), 175-181.

Mutune, E., Odongo, J., & Wamalwa, M. (2023). Cybersecurity Vulnerabilities in Kenya's Mobile Money Ecosystem. *Kenya Journal of Information Systems*, 5(2), 33–49.

Mutune, J., Mwangi, M., & Maina, G. (2023). Vulnerability of Mobile Money Platforms in Kenya: A Cybersecurity Perspective. *Journal of Digital Finance, 5*(1), 22–35.

Mutune, M., Musumba, P., & Kiragu, S. (2023). Cyber fraud in mobile money in East Africa. *African Journal of Information Security*.

NCSC. (2023). *Annual Review*. UK National Cyber Security Centre.

Ndeda, L. A., & Odoyo, C. O. (2019). Cyber threats and cyber security in the Kenyan business context.

Obuhuma, J., & Zivuku, B. (2020). The State of Cybersecurity Preparedness in Kenyan Public Institutions. *African Journal of Information Security*, 5(2), 55–68.

PwC. (2024). *Global Digital Trust Insights Survey*. Retrieved from https://www.pwc.com

Radanliev, P. et al. (2018). Future developments in cyber risk assessment for the Internet of Things. *Computers in Industry*, 102, 14–22.

Radanliev, P., et al. (2018). Integration of cyber risk from the Internet of Things into cyber risk management. *Journal of Risk Research, 21*(6), 689–710.

Rutenberg, N., & Omariba, D. (2022). Data privacy and cybersecurity challenges in African healthcare systems. *Health Policy and Technology*, 11(1), 100594.

Serianu Ltd. (2014). *Africa Cyber Security Report: Kenya 2014*. Nairobi: Serianu.

Serianu Ltd. (2019). *Africa Cyber Security Report: Kenya 2019*. Nairobi: Serianu.

Sowon, K., et al. (2024). Privacy-Preserving Protocols for Mobile Money in Kenya. *African Journal of FinTech Innovation*, *4*(1), 14–26.

TOO, W. K., & MUTUKU, M. (2023). An examination of the effects of cyber security in enhancing performance of the public sector institutions. *Reviewed Journal International of Business Management [ISSN 2663-127X]*, *4*(1), 471-477.

Turel, O., Qahri-Saremi, H., & Vaghefi, I. (2021). Dark sides of digitalization. *International Journal of Electronic Commerce*, 25(2), 127-135.

Waithaka, G. (2016). An Assessment of Cybersecurity Readiness in Kenya's Public Sector. *Journal of ICT Policy and Regulation*, 3(1), 23–37.

Waithaka, S. W. (2016). Factors affecting cybersecurity in national government ministries in Kenya. (Doctoral dissertation, University of Nairobi).

Waliullah, M., Patel, K., & Singh, N. (2025). A Systematic Literature Review of Cybersecurity Threats in Digital Financial Services. *International Journal of Information Security, 24*(2), 113–138.

Wekundah, R. N. (2015). The effects of cybercrime on e-commerce; a model for SMEs in Kenya. (Doctoral dissertation, University of Nairobi).

World Economic Forum. (2023). *The Global Risks Report 2023*. Retrieved from https://www.weforum.org

