Enhancing Cyber Resilience through Adaptive Security Policies

by
Thuranira Mark Linturi, and Chemosit Nick William

Abstract

Rapid advancements in technology have led to increased cyber incidents and data breaches. This has made cyber resilience a crucial aspect of a comprehensive cybersecurity framework. Kenya has also seen a surge in cyberattacks targeting critical infrastructure and important government services. This underscores the need for a cybersecurity resilience framework based on adaptive security principles. The Directorate of Immigration and Citizen Services is crucial in providing efficient services and setting cybersecurity standards for all government agencies. This study investigates how adaptive security policies bolster cyber resilience within the Directorate of Immigration Services in Kenya while scrutinising the impact of organisational culture on both technical and non-technical aspects of cybersecurity resilience. The research design used a mixed-methods approach, including a systematic literature review and interviews with 73 cybersecurity professionals, system administrators, network engineers, and non-technical staff from the Directorate. Data collection methods included questionnaires, interviews, and forensic examination of past cyber incidents. Quantitative data was analysed using SPSS, while qualitative data underwent thematic analysis. The study reveals that the Directorate of Immigration Services uses advanced technologies and methods to address cyber threats. However, challenges remain in identifying, addressing, and recovering from these incidents. Organisational culture is vital in promoting cybersecurity awareness and practices among employees. To enhance cyber resilience in the Directorate of Immigration Services and throughout Kenya, a comprehensive strategy is needed. This strategy should include promoting awareness, providing targeted training, reviewing policies, and implementing cutting-edge technologies. The research also suggests developing a national cyber resilience framework, adopting an adaptive security approach, fostering a security- first culture, prioritising cyber resilience training, implementing a comprehensive risk management framework, and establishing standardised incident reporting and response mechanisms to ensure cybersecurity resilience in Kenya.

Keywords: *security, policies, cyber-resilience, immigration, cyber threats,*

Introduction

The Directorate of Immigration Services in Kenya plays a vital role in border security, immigrationmanagement, and safeguarding citizen data. However, its significance extends beyond these functions, as any breach in its cybersecurity could lead to severe consequences, including unauthorised access to sensitive information, identity theft, and national security risks. Additionally, as the overseer of theeCitizen platform, it serves as a critical gateway for citizens to access government services online,making it a prime target for cyberattacks. Thus, securing the Directorate is essential for ensuring smooth service delivery, setting cybersecurity standards across government agencies, and fostering a culture ofawareness and preparedness.

The rising prevalence of cyber threats in Kenya's public institutions, accelerated by rapid digitaltechnology adoption post-COVID-19, highlights the urgent need for enhanced cybersecurity measures (World Economic Forum's Global Risks Report, 2024). In 2023, the cybersecurity sector surpassed global tech growth rates, signalling significant innovation alongside escalating risks (Kabui & Omondi, 2023). This trend was exemplified when cyber incidents in July 2023 disrupted over 5,000 government services for 48 hours, impacting Kenya's digital financial ecosystem, including key platforms likeeCitizen (Kabui & Omondi, 2023). The COVID-19 pandemic's digital acceleration heightened cybersecurity concerns, with a surge in remote work creating opportunities for cybercriminals (Jaber et al., 2021). Kenya faces significant cybersecurity challenges, with the Communications Authority of Kenya (CAK) reporting over 7.7 million attacks since 2017, targeting critical information infrastructure and essential government services (Africanews, 2023).

Critics point out gaps in cybersecurity policies and knowledge disparities between IT professionals and non-IT officials (Sliwinski, 2014; Caruson et al., 2012). Resilient frameworks for e-government projects and the potential of big data analytics in cybersecurity present avenues for improvement (Alrubaiq and Alharbi, 2021; Sharma and Barua, 2023). Cyber resilience, essential in the digital era, ensures continuity and functionality under adverse conditions (Safitra et al., 2023). Achieving this resilience demands a holistic approach integrating technological solutions, heightened employee awareness, and collaboration (World Economic Forum, 2024). The shortage of skilled cybersecurity professionals is challenging, emphasising the need to upskill current staff and diversify the talent pool (World Economic Forum, 2024). A robust cybersecurity culture, emphasising continuous learning, transparent communication, and ethical behaviour, is central to cyber resilience (Aksoy, 2024).

While technology advancements and cybersecurity strategies drive positive outcomes, they also contribute to increased cyber incidents and data breaches (Onwubiko, 2020). This has spotlighted theimportance of cyber resilience within a robust cybersecurity framework, with a notable research gap inthis area (Onwubiko, 2020). Security leaders express growing concerns about organisational readiness against cyber threats.

An adaptive security policy approach addresses the evolving threats, risks, and contextual factorsspecific to organisations. It encompasses a proactive approach that adapts and evolves to tackle emerging threats. Contrary to traditional security measures that mainly rely on static rules and signatures to detect and prevent cyber-attacks, adaptive security dynamically adjusts to the changing landscape of cyberthreats. A resilient organisation adopts a proactive approach to cyber security by implementing measures to avert cyber-attacks, detect them promptly, respond effectively, and recover swiftly. This necessitates a comprehensive cyber security strategy integrating cutting-edge technologies, established best practices, and pertinent policies. (Shahzad & Qiao, 2022).

Literature Review

Adaptive Security Policy and Cyber Security Resilience

“Cyber resilience” emerged in the early 2000s as a response to the need for systems that can resist andrecover from cyber incidents. It has gained considerable attention and is widely recognised as a concept and critical element of comprehensive cybersecurity strategies. (Tzavara et al., 2024). Currently,cybersecurity and cyber resilience are two distinct concepts, with cybersecurity focusing on protecting information and computer systems by limiting access to sensitive data and addressing potential threats,while cyber resilience encompasses a system’s ability to maintain functionality even in challenging situations, extending beyond technological measures and requiring employee awareness and cooperation. (Safitra et al., 2023),

The conversation surrounding cyber resilience has progressed. Montasari et al. (2018) emphasised the necessity of multi-layered, intelligence-driven strategies considering human psychology in attacks. Annarelli et al. (2020) advocated for robust tactics beyond traditional methods, highlighting the significance of cyber resilience in the digital age. Caron et al. (2019) proposed an adaptive security strategy leveraging automation, machine learning, and real-time threat intelligence for quicker anomaly detection and incident response. Brass and Sowell (2020) discussed the vulnerabilities associated with the Internet of Things (IoT) and proposed an adaptive regulatory governance model for continuousknowledge exchange. Robertson and Laddaga (2012) explored a DARPA-supported project for creating a self-aware network using self-adaptive techniques to sustain computational functions during attacks.

Munusamy and Khodadi (2023) emphasised achieving resilience through resilience itself amid technological advancements. Halabi et al. (2022) applied adaptive control theory to Cyber-Physical Systems (CPSs) in Industry 4.0 to ensure secure control approaches. Abdullayeva (2023) introduced an approach for enhancing cloud computing security focusing on virtualisation, service layers, and a new cybersecurity reference model. Tsigkanos et al. (2016) proposed Bigraphical Reactive Systems forspeculative threat analysis in cyber-physical systems. Al-Hawamleh (2024) developed a Cybersecurity Resilience Framework integrating governance, external collaboration, and continuous monitoring.Mbanaso et al. (2019) introduced a Cybersecurity Resilience Maturity Measurement framework for South African nations, focusing on organisational readiness. Malatji et al. (2020) examined cybersecurity responsibilities within South Africa’s water and wastewater sector, identifying gaps inimplementation and emphasising the need for a computer security incident response team.

Akech et al. (2020) highlighted cyber resilience vulnerabilities in Kakamega County, Kenya, emphasising collective responsibility in enhancing cyber resilience. Taruvinga (2020) comparedcybersecurity threats in Kenya and Zimbabwe, recommending prioritising human rights in cyber policies and implementing data protection laws.

Organisation Culture and Cyber Security Resilience

Organisational culture plays a crucial role in bolstering cyber security resilience. Leveraging organisational culture as an adaptive security policy is crucial for this endeavour; cyber resilience encompasses both technical and human aspects, including behaviours, values, and attitudes that shape an organisation’s cybersecurity approach (Aksoy, 2024). A robust cybersecurity culture permeatesemployees’ daily routines, practices, and mindsets, positioning the company’s values and practices in both professional and personal spheres.

Effective leadership is crucial in cultivating organisational organisational culture. Leaders play a vital role in shaping the attitudes, behaviours, and practices related to cybersecurity within an organisation. According to Watkins (2013), organisational culture is essential for fostering collaboration, understanding, and goal alignment, key drivers of unified action within an organisation. How leaders allocate resources, demonstrate knowledge and skills, promote awareness, and encourage continuous learning all contribute to developing a strong cybersecurity culture.

Zgouva (2020) stressed the importance of aligning governance and management models with an organisation's strategic direction, emphasising the necessity of a cyber strategy, skilled personnel, effective communication between boards and security leadership, and a clear reporting structure tobolster cyber resilience. Njoroge (2020) identified key factors influencing cybersecurity culture in SMEs in Nairobi City County, such as top management support, reward systems, policies, change management, training, awareness programs, and monitoring. These findings highlight the importance of continuous engagement in cybersecurity practices.

Herath and Rao (2009) suggested that a positive cybersecurity culture can significantly reduce thelikelihood of successful cyberattacks. However, Alawida et al. (2022) warned of the rising cyberattack risks, especially during events like the Covid-19 pandemic. Amankwah-Amoah et al. (2021) and Battisti, Alfiero, and Leonidou (2022) emphasised the need for robust cybersecurity practices in remote working environments, which COVID-19 has accelerated. Obuhuma et al. (2020) focused on social engineeringin cybersecurity, highlighting the importance of user education, awareness, and the implementation of information security policies and legislation. Chitechi et al. (2023) identified a significant lack ofpreparedness for cybersecurity vulnerabilities in Kakamega and Bungoma counties, Kenya, indicating a need for improvement in cybersecurity management within Kenya's County Governments.

De Silva (2023) and Gupta et al. (2023) advocated involving employees in policy development, rewarding responsible behaviour, and investing in comprehensive training programs to cultivate a strong cybersecurity culture. However, da Veiga et al. (2020), Cano (2021), and Hassandoust and Johnston (2023) pointed out gaps in comprehensive frameworks addressing the impact of organisational culture on cybersecurity. Were (2021) stressed the significance of cybersecurity in the fourth industrial revolution, identifying gaps in Kenya's implementation of UN Cyber Norms. Suggestions include

transitioning to international law, fostering collaboration between private and government sectors, and investing in cyber deterrence and transparency.

Theoretical framework

The Technology Acceptance Model (TAM) was used to understand ICT officers' and internal auditors' attitudes and perceptions towards ASP implementation. TAM is a theoretical framework developed to understand and predict how users adopt and use new information technologies. Fred Davis proposed it in the late 1980s, and has since become one of the most widely used models for studying user acceptance of technology. TAM provides a theoretical framework for examining ICT officers' and internal auditors' attitudes and perceptions regarding implementing adaptive security policy (ASP) and cybersecurityresilience within the Directorate of Immigration Services in Kenya. TAM uses the concepts of perceived usefulness and ease of use to predict the likelihood of adoption while identifying potential barriers and informing intervention strategies. By helping to understand stakeholders' acceptance of ASP, TAMfacilitates the assessment of obstacles to implementation and supports targeted interventions such astraining and support. Additionally, TAM enables the evaluation of success factors over time by monitoring changes in attitudes and adoption rates.

Research Methodology and Design

The research used a mixed-methods design, incorporating a systematic literature review and interviews with ICT officers and internal auditors from the Directorate of Immigration Services in Nairobi. The target population consisted of 89 individuals, including cybersecurity professionals, system administrators, network engineers, and non-technical staff. Data collection employed purposefulsampling to gather insights from experts in the field. A forensic examination of past cyber incidents was conducted to identify attack vectors and vulnerabilities. The sample size, calculated using Solvin's formula, comprised 73 respondents. Data collection tools included questionnaires and interviewschedules. Quantitative data was analyzed using SPSS software, while qualitative data underwentthematic analysis, ensuring a comprehensive examination of the research problem.

Findings and Discussion

Cyber Security Resilience in directorate of immigration and citizen services

The findings reveal that 50% of respondents believe their organisations would face challenges indetecting and responding to cyber threats. Ghelani (2022) conducted a qualitative study in Korea, highlighting a heavy reliance on preventive measures due to a focus on technology availability and limited awareness of broader security issues. The study suggests a need for a balanced approach thatintegrates preventive measures with other tactics at the operational level. Hasan et al. (2021) analysed 270 IT professionals in Bahrain and found that cyber-attacks are increasing and impacting organisational performance. Using the Technology-Organization-Environment framework, they identified seven factors that positively influence security performance, indicating that cybersecurity readiness enhances organisational security performance.

The findings on how often the organisation reviews and updates its cybersecurity policies and procedures indicate that 40% responded "others," suggesting no designated review timelines. Li et al. (2019) highlighted that employees with knowledge about company security policies demonstrate higher cybersecurity proficiency. A supportive organisational environment fosters compliance by enhancing threat and coping appraisals. Regarding disaster recovery, 90% of respondents confirmed having abackup disaster recovery plan. Chang (2015) emphasised the importance of disaster recovery in big data systems, proposing a multi-purpose approach that ensures close to 100% recovery rates.

The Directorate of Immigration experienced significant cyber incidents in 2023, mainly targeting itseCitizen platform. These attacks disrupted services, affecting Kenyan citizens and officials. Notableincidents involved Distributed Denial of Service (DDoS) attacks. Ali et al. (2022) warned of vulnerabilities in e-government due to technological advancements, while Shandler and Gomez (2022) highlighted the impact of cyber-attacks on public confidence. The Directorate employs a multifaceted approach to cyber risk management, with a dedicated cyber department overseeing security initiatives. Advanced technologies like load balancers, IDS, and IPS detect and prevent threats. Employee trainingprograms and regular updates mitigate vulnerabilities. Perimeter defences, system audits, and ethicalhacking tests further enhance resilience. DiMase et al. (2015) suggested a comprehensive risk management framework, emphasising the importance of identifying and prioritising cybersecurity risks.

The Directorate has robust measures in place for rapid recovery from cyber incidents, including disaster recovery plans, backup systems, secure authentication, firewalls, antivirus software, and regular audits. Whitham (2023) emphasised the importance of detailed plans in accelerating recovery. Incident response plans reduce downtime and maintain public trust (Nichols, 2023). Cybersecurity training and awareness programs vary within organisations, with strategies ranging from regular sessions to ad hoc training tailored to system importance. Ongoing awareness campaigns reinforce cybersecurity practices and educate employees on combating cyberattacks. Buchanan Technologies (2022) highlighted the significance of security awareness training in building a proactive defence mechanism.

Challenges in achieving cyber resilience include a lack of IT knowledge, cybersecurity expertise, innovation, talent shortages, and financial constraints. Human vulnerabilities, increasing interconnectivity, and regulatory complexity contribute to cybersecurity breaches. Addressing thesechallenges requires a multifaceted approach involving technological innovation, regulatory measures, education, and stakeholder collaboration (Wyman, 2020; Oh, 2024).

Adaptive Security Policy and Cyber Security Resilience

The finding on whether there is an established process for incorporating feedback from security incidents into policy updates revealed that 90% of respondents answered yes. Incorporating feedback from security incidents into policy updates is crucial for organisational learning and enhancing risk awareness (Patterson et al., 2023; Connolly and Wall, 2019). It ensures that lessons learned translate into actionable changes to prevent future incidents. Regarding how the organisation adapts its security policies to address emerging cyber threats, it employs technological upgrades, proactive testing, education,research, and compliance with best practices. Sexton (2017) emphasised the importance of safeguarding organisations before breaches occur by evaluating current preparedness levels and implementingimprovement programs. Cybersecurity automation enhances efficiency and response times (Raizada,2024).

The organisation prioritises cybersecurity through a multifaceted approach, employing various technologies and strategies such as Intrusion Detection and Prevention Systems (IDPS), Network Access Control, Least Privilege Principle, and system hardening. Advanced technologies like machine learning (ML) and Data Loss Prevention (DLP) bolster defences, while automated response mechanisms and

distributed security systems enhance real-time threat detection and mitigation. These cybersecurity automation technologies are a multiplier, improving security skills and impact (Wadhwa, 2023).

Machine learning and artificial intelligence (AI) are pivotal in enhancing cybersecurity, covering access management, threat detection, response, adaptability to emerging threats, automated auditing, access control, and government integration. While ML and AI hold significant potential in detecting andmitigating harmful activities within computer systems and networks (Holmes, 2023), a holistic approach combining these advanced technologies with traditional security measures is essential for bolsteringorganisational cybersecurity resilience (Atef, 2023).

The responses emphasise the importance of a comprehensive approach to cybersecurity, which includes reviewing and complying with policies, implementing education and awareness campaigns, updating infrastructure and technology, managing risks, and conducting evaluations. Continuous improvement, adaptation, and ongoing training and development efforts are also vital. Willie (2023) emphasisesfostering a security-focused culture to enhance resilience against cyber threats and protect vital digital assets. Temitayo et al. (2024) highlighted a trend towards leveraging advanced technologies like artificial intelligence (AI) and machine learning (ML) in cybersecurity. They also note the significant impact of human elements on cybersecurity outcomes and the influence of international policies onstandardising cybersecurity practices.

Organisational Culture and Cyber Security Resilience

50% of respondents rated the level of cybersecurity awareness among employees in the organisation as moderate, indicating existing vulnerabilities. Li et al. (2019) found that employees aware of their company’s information security policies are better equipped to manage cybersecurity responsibilities. Kemper (2019) highlights employees as the primary vulnerability in organisations, emphasising the importance of engaging and motivating them to actively participate in cybersecurity efforts through clear policies and compliance strategies.

Regarding cybersecurity training provision, 90% of respondents confirmed that the organisationconducts such training. Aaltola and Taitto (2019) stress the significance of recognising and leveraging learners’ existing skills, suggesting that the educational process should start by assessing participants’ competencies. Tolossa (2023) recommends tailoring training for remote work to enhance organisational

adaptability. Organisations can proactively safeguard assets and maintain a secure digital stance byinvesting significantly in cybersecurity awareness training. 60% of respondents confirmed that cybersecurity is included in the performance evaluation criteria for employees. Alqahtani and Erfani (2021) found a positive relationship between technical cybersecurity controls, accountability, monitoring, and employee stress levels. Koutsouris et al. (2021) stressed the importance of assessment methods in training initiatives and evaluation tools in enhancing organisational security measures.

Regarding reporting security incidents or suspicious activities, 90% indicated a clear process in place. Alharbi (2023) proposed the Holistic Evaluation Model for Information Security Awareness Programs, emphasising the need for a comprehensive approach combining passive and active data collection.Carpenter (2023) highlighted the importance of incident reporting in fostering a robust security culture, while Irei and Shea (2024) emphasised the risks associated with disorganised reactions to cyberattacks.

The organisational culture regarding cybersecurity reflects proactive vigilance mixed with occasionalindifference. Challenges persist in ensuring uniform adherence, especially among middle-level employees. Pavlova (2020) emphasised the role of management in maintaining organisational culture through education, reviews, rewards, and value hierarchies. Karlsson et al. (2021) suggested thatinternal-focused organisational cultures correlate with higher adherence to information security policies. Top management's proactive involvement in supporting cybersecurity initiatives is evident through their leadership, funding, and collaboration efforts. Loonam et al. (2020) highlighted the role of effective leadership in corporate-level attention to information security. Marotta and Pearlson (2019) discussed efforts by the leadership team at BPS to strengthen relationships and establish a robust cybersecurityculture.

Employee perceptions of cybersecurity vary; some show strong awareness and concern, while others exhibit neutral stances or lack awareness. Gratian (2018) stressed the importance of recognisingindividual differences in cybersecurity behaviours. Egelman and Peer (2015) and Sheng et al. (2010) found relationships between risk propensity and security behaviours. Barriers to fostering a more robust cybersecurity culture include limited resources, gaps in employee knowledge, dynamic cyber threats, communication difficulties, and inadequate training. Chaudhury (2020) highlighted challenges likefinancial constraints, organisational culture, and time constraints, particularly for smaller enterprises.

Hinchy (2023) emphasised the need for security teams to access the latest information and effectively communicate with stakeholders to address evolving threats.

Conclusion

Cyber resilience is gaining prominence as technology advances and cyber threats become more sophisticated. Organisations now understand the need to defend against attacks and maintain operations during disruptions. Cyber resilience is a burgeoning field within cybersecurity and presents an opportunity for the research community to contribute and develop a strong knowledge base.

The examination of cyber security resilience within the Directorate of Immigration and Citizen Services underscores both strengths and challenges in the organisation's ability to address cyber threats. The analysis reveals a complex landscape where management is crucial in promoting a cybersecurity- conscious environment. The results highlight that Organisational culture and cybersecurity resilience are closely intertwined, with awareness, training, reporting mechanisms, and leadership playing vital roles. Advanced technologies such as machine learning and artificial intelligence can enhance security capabilities. However, a comprehensive approach that combines them with conventional measures isvital for effective resilience. To enhance cyber resilience within the Directorate of Immigration and Citizen Services and across public institution in Kenya. There is a need for a holistic approach that prioritises raising awareness, providing targeted training, reviewing policies, and adopting advancedtechnologies.

Recommendations

- Develop a national framework for cyber resilience tailored to the specific needs of public institutionsin collaboration with cybersecurity experts, academia, and industry stakeholders.
- Adopt an adaptive security approach integrating governance principles, external collaboration,continuous monitoring, and organisational culture.
- Encourage the adoption of multi-layered, intelligence-driven security strategies incorporatingpeople, automation, machine learning, and real-time threat intelligence.
- Promote a security-first culture aligning governance and management models with cybersecurityobjectives.

- Prioritise cyber resilience training and capacity building for all employees, covering both technical and non-technical aspects of cybersecurity.
- Implement a comprehensive risk management framework integrating physical, information,cognitive, and social domains.
- Establish standardised incident reporting and response mechanisms across organisations.
- Foster a continuous improvement and adaptability culture in cybersecurity practices through regularupdates, risk management, and evaluations.

References

Abdullayeva, F. J. (2023, September 1). Cyber resilience and cyber security issues of intelligent cloud computingsystems. Results in Control and Optimisation. https://doi.org/10.1016/j.rico.2023.100268

AFRICA NEWS (2023), https://www.africanews.com/2023/10/03/kenya-hit-by-record-860m-cyber-attacks-in-a- year// retrieved march17 2024

Akech, P., Abeka, S., & Liyala, S. (2020). A Framework Based On Institutional Theory To Aid In Cyber Resiliency In County Governments Of Kenya. *International Journal of Innovative Research and Advanced Studies*(IJIRAS), 7(7), 142-147.

Aksoy, C. (2024). Building a cyber security culture for resilient organisations against cyber attacks. İşletme Ekonomi Ve Yönetim Araştırmaları Dergisi, 7(1), 96-110. https://doi.org/10.33416/baybem.1374001

Alharbi, T. (2023). A Holistic Evaluation Model for Information Security Awareness Programs in Work Environment. 2023 Eighth International Conference On Mobile And Secure Services (MobiSecServ),CFP23RAC-ART, 1-4.

Ali, S., Jamali, A. K., Shah, S. Z. H., Qureshi, S. N., & Tanveer, S. (2022, October 3). *IMPACT OF CYBER-TERRORISM ON NATIONAL SECURITY OF PAKISTAN*. https://archives.palarch.nl/index.php/jae/article/view/11396

Alqahtani, M., & Erfani, E. (2021). Impact of Technical Controls, Accountability, and Monitoring on the JobPerformance of Employees: Assessing the Mediating Role of Stress. ACIS.

Alrubaiq, A., & Alharbi, T. (2021, May 18). *Developing a Cybersecurity Framework for e-Government Project inthe Kingdom of Saudi Arabia. Journal of Cybersecurity and Privacy*. https://doi.org/10.3390/jcp1020017

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient

systems.
Computers & Industrial Engineering, 149, 106829.

Atef, M. (2023, April 16). The Role of Artificial Intelligence and Machine Learning in Cybersecurity. Medium. Retrieved 28 March 2024 from https://medium.com/@m.atef_72234/the-role-of-artificial-intelligence- and-machine-learning-in-cybersecurity-6ebaa28f9d72

Brass, I., & Sowell, J. H. (2020, July 13). Adaptive governance for the Internet of Things: Coping with emerging security risks. *Regulation & Governance*, 15(4), 1092–1110.

Buchanan Technologies (2022, July 15). Five Major Benefits of Security Awareness Training. Buchanan Technologies. https://www.buchanan.com/benefits-security-awareness-training/ Caron, F. (2019). Obtaining reasonable assurance on cyber resilience. *Managerial Auditing Journal.*

Carpenter, P. (2023, July 31). #HowTo: Create a Culture of Incident Reporting. Infosecurity Magazine. https://www.infosecurity-magazine.com/opinions/create-culture-incident-reporting/

Caruson, K., MacManus, S. A., & McPhee, B. D. (2012, December 4). *Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success. Journal of Homeland Security and Emergency Management.* https://doi.org/10.1515/jhsem-2012-0003

Chang, V. (2015). Towards a big data system disaster recovery in a private cloud. Ad hoc networks, 35, 65-82.Chaudhury, D. (2020, July 6). Barriers to Inculcating Good Cyber Security Habits Amongst Employees. ITSecurityWire. https://itsecuritywire.com/featured/barriers-to-inculcating-good-cyber-security-habits-amongst-employees/

Cheptoo, K. P., & Obare, R. M. (2023). A Framework for Electronic Document Management in theImplementation of E-Government in Kenya.

Chitechi, K. V., Benjamin Kiprono, & Frank Tireito. (2023). Cyber- Security Vulnerability and Initiatives inKenyan County Governments. African Journal of Computing and Information Systems (AJCIS), 7(X), 35–
51. https://doi.org/10.1234/ajcis.v7iX.38

Connolly, L., & Wall, D. S. (2019, November). The rise of crypto-ransomware in a changing cybercrimelandscape: Taxonomising countermeasures. *Computers & Security*, *87*, 101568. https://doi.org/10.1016/j.cose.2019.101568

Corradini, I., & Nardelli, E. (2018). Building Organisational Risk Culture in Cyber Security: The Role ofHumanFactors. Advances in Intelligent Systems and Computing.

De Silva, B. (2023). Exploring the Relationship Between Cybersecurity Culture and Cyber Crime Prevention: A Systematic Review. *International Journal of Information Security and Cybercrime.* demographic analysis of phishing susceptibility and effectiveness of interventions. In Proceedings of the

Egelman, S., & Peer, E. (2015, April). Scaling the security wall: Developing a security behavior intentions scale (sebis). In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems(pp. 2873-2882). ACM.

Fortinet. (2022). 2022 Cybersecurity Skills Gap Survey. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A Review. *AuthoreaPreprints*.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. computers & security, 73, 345-358.

Gupta, V., Singh, S.P., Singh, C., & Mangla, A. (2022). A Systematic review on Cybersecurity: Models, Threats and Solutions. 2022 10th International Conference on Emerging Trendsin Engineering andTechnology - Signal and Information Processing (ICETET-SIP-22), 1 6

Halabi, T., Haque, I., & Karimipour, H. (2022, December). Adaptive Control for Security and Resilience ofNetworked Cyber-Physical Systems: Where Are We?. In 2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA) (pp. 239-247). IEEE.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organisations and its influence on performance. Journal of Information Security and Applications, 58, 102726.

Hinchy, E. (2023, March 9). 6 Ways To Go Beyond Awareness And Foster A Real Culture Of Cybersecurity.Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/03/08/6-ways-to-go-beyond-awareness- and-foster-a-real-culture-of-cybersecurity/?sh=7b782aba2168

Holmes, J. (2023, October 17). The Role of AI and ML in Business Cyber Security. Stanfield IT. https://www.stanfieldit.com/the-role-of-ai-and-ml-in-business-cyber-security/

Irei, A., & Shea, S. (2024, January 30). What is incident response? A complete guide. Security. https://www.techtarget.com/searchsecurity/definition/incident-response

Jaber, A. N., & Fritsch, L. (2021). COVID-19 and Global Increases in Cybersecurity Attacks: Review of Possible Adverse Artificial Intelligence Attacks. In 2021 25th International Computer Science and

Engineering Conference (ICSEC) (pp. 434-442).

Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2021, December 21). The effect of perceived organisational culture on employees' information security compliance. Information & Computer Security. https://doi.org/10.1108/ics-06-2021-0073

Kasowaki, L., & Eden, S. (2023). *The Human Element in Cubersecurity: Understanding and Mitigating Risks* (No.11642). Easyschair

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, *2019*(8), 11- 14.

Koutsouris, N., Vassilakis, C., & Kolokotronis, N. (2021, July 26). Cyber-Security Training Evaluation Metrics. *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. https://doi.org/10.1109/csr51186.2021.9527946

Lebogang, V., Tabona, O., & Maupong, T. (2022). Evaluating Cybersecurity Strategies in Africa. Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security, 1–19. https://doi.org/10.4018/978- 1-7998-8693-8.ch001

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13-24.

Loonam, J., Zwiegelaar, J.B., Kumar, P., & Booth, C. (2020). Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective. IEEE Transactions on Engineering Management, PP, 1-14.

Majumdar, N., & Ramteke, V. (2022, October). Human elements impacting risky habits in cybersecurity. In *AIP Conference Proceedings* (Vol. 2519, No. 1). AIP Publishing.

Marotta, A., & Pearlson, K. E. (2019). A Culture of Cybersecurity at Banca Popolare di Sondrio. AmericasConference on Information Systems.

Marotta, A., & Pearlson, K.E. (2019). A Culture of Cybersecurity at Banca Popolare di Sondrio. AmericasConference on Information Systems.

Mbanaso, U. M., Abrahams, L., & Apene, O. Z. (2019, June 27). Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework. The African Journal of Information and Communication.https://doi.org/10.23962/10539/27535

Montasari, R., Hosseinian-Far, A., & Hill, R. (2018). Policies, innovative self-adaptive techniques and understanding psychology of cybersecurity to counter adversarial attacks in network and cyber environments. Cyber criminology, 71-93.

Munusamy, T., & Khodadi, T. (2023). Building Cyber Resilience: Key Factors for Enhancing

OrganizationalCyber Security. Journal of Informatics and Web Engineering, 2(2), 59-71.

Nichols, C. (2023, September 5). 3 Benefits of an Incident Response Plan. Cybriant. https://cybriant.com/incident- response-plan/

Njoroge, G. M. (2020). Human Factors Affecting Favourable Cybersecurity Culture- a Case of Small and Medium- sized Enterprises Smes Providing Enterprise-Wide Information Systems Solutions in Nairobi City Countyin Kenya. http://erepository.uonbi.ac.ke/handle/11295/153139

OBUHUMA, J., & ZIVUKU, S. (2020, May). Social engineering based cyber-attacks in kenya. In 2020 IST-Africa Conference (IST-Africa) (pp. 1-9). IEEE.

Ogonji, M. (2019). Promoting Security In Africa Through Effective Counter Cyber Terrorism Strategies (Doctoral dissertation, University of Nairobi).

Oh, H. (2024, January 29). 4 Challenges Organisations Face When Operationalizing Cybersecurity. SolCyber.https://solcyber.com/4-challenges-organizations-operationalizing-cybersecurity/

Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity strategy's role in raising Kenyan awareness ofmobile security threats. Information & Security, 32(2), 1.

Onwubiko, C. (2020). Focusing on the Recovery Aspects of Cyber Resilience. In International Conference onCyber Situational Awareness, Data Analytics and Assessment (CyberSA) (pp. 1-13). https://doi.org/10.1109/CyberSA49311.2020.9139685

Open Data Kenya, http://www.opendata.go.ke, accessed 15 March 2017.

Patterson, C. M., Nurse, J. R., & Franqueira, V. N. (2023, September). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, *132*, 103309. https://doi.org/10.1016/j.cose.2023.103309

Pavlova, E. (2020). Enhancing the Organisational Culture related to Cyber Security during the University Digital Transformation. Information & Security: An International Journal, 46(3), 239–249. https://doi.org/10.11610/isij.4617

Pérez-Morón, J. (2022) Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare, areview and future research agenda Open Access Journal of Asia Business Studies

Raizada, A. (2024, March 6). The Role of Automation in Making Cybersecurity Accessible to All. Copper Digital. Retrieved 28 March 2024 from https://copperdigital.com/blog/the-role-of-automation-in-cybersecurity-accessibility/

Resilience. (2023). 2023 Mid-Year Cyber Claims Report. https://unlock.cyberresilience.com/2023_midyear_claims_

Robertson, P., & Laddaga, R. (2012, September). Adaptive security and trust. In 2012 IEEE Sixth

InternationalConference on Self-Adaptive and Self-Organizing Systems Workshops (pp. 55-60). IEEE.

Rotich, E. K. (2020). Cyber Terrorism and National Security in Africa: a Case Study of Kenya (Doctoraldissertation, university of Nairobi).

Safitra, M. F., Lubis, M., & Kurniawan, M. (2023). Cyber Resilience: Research Opportunities. https://doi.org/10.1145/3592307.3592323

Schneier, B. (2008). "The New School of Information Security." Addison-Wesley Professional.

Security Scorecard. (2022). Cyentia Institute and SecurityScorecard Research Report: Close Encounters of the Third (and Fourth) Party Kind. https://securityscorecard.com/research/cyentia-close-encounters-of-the- third-and-fourth-party-kind/

Sexton, L. (2017, July 6). How companies can stay ahead of evolving cyber threats - Financial Services Thought Gallery. Financial Services Thought Gallery. https://eyfinancialservicesthoughtgallery.ie/steps-financial- services-companies-need-take-stay-ahead-evolving-cyberthreats/

Sharma, P., & Barua, S. (2023). From Data Breach to Data Shield: The Crucial Role of Big Data Analytics in Modern Cybersecurity Strategies. International Journal of Information and Cybersecurity, 7(9), 31–59.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish? A SIGCHI Conference on Human Factors in Computing Systems (pp. 373-382).

Sliwinski, K. F. (2014, September 2). Moving beyond the European Union's Weakness as a Cyber-Security Agent.

Contemporary Security Policy, *35*(3), 468–486.

Taruvinga, F. (2020). Emerging Cyber Security Threats: A Comparative Study Of Kenya And Zimbabwe.http://erepository.uonbi.ac.ke/handle/11295/153882

Wadhwa, P. (2023, September 18). 7 Best Cybersecurity Automation Tools. Sprinto. Retrieved 28 March 2024 from https://sprinto.com/blog/cybersecurity-automation-tools/

Watkins, M. (2013). What is organisational culture? And why should we care. *Harvard Business Review*, *15*, 1-5.

Were, T. O. (2021). Implementation of UN Cyber Norms in the Promotion of International Security: a Case Studyof Kenya (Doctoral dissertation, University of Nairobi).

Whitham, C. (2023, October 6). What Are the Benefits of Cyber Resilience? - North East Business Resilience Centre. North East Business Resilience Centre. https://www.nebrcentre.co.uk/what-are-the-benefits-of- cyber-resilience/

Willie, M. M. (2023). The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture.

SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4564291

World Economic Forum. (2022). Global Cybersecurity Outlook 2022.

https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

World Economic Forum. (2023, November 17). Facilitating Global Interoperability of Cyber Regulations in the Electricity Sector. https://www.weforum.org/publications/facilitating-global-interoperability-of-cyber- regulations-in-the-electricitysector/

Wout, V& Magdalena, C. (2019). Develop and maintain a cybersecurity organisational culture.

Wyman O (2020). The Seven Most Pressing Challenges Facing Cybersecurity. Retrieved march 29 2024 fromhttps://www.marshmclennan.com/insights/publications/2020/february/the-seven-most-pressing- challenges-facing-cybersecurity.html