A Framework to Secure Business Assets Against Social Engineering Attacks in State Corporations in Kenya

Структура захисту бізнес-активів від атак соціальної інженерії в державних корпораціях Кенії

John Maiyo [A]

Corresponding author: Postgraduate Student, Department of Information Technology, School of Computing and Informatics, e-mail: lomezjay@gmail.com, ORCID: 0009-0007-9847-4034

Satwinder Singh Rupra [A]

Dr., Senior Lecturer, Department of Information Technology, School of Computing and Informatics, e-mail:dotanga@mmust.ac.ke, ORCID: 0000-0003-3695-196X

Daniel Otanga [A]

Dr., Senior Lecturer and Dean, Department of Information Technology, School of Computing and Informatics, e-mail: ssingh@mmust.ac.ke, ORCID: 0000-0001-7212-1088

Джон Маййоа [A]

Corresponding author: аспірант, кафедра інформаційних технологій, Школа обчислювальної техніки та інформатики, e-mail: lomezjay@gmail.com, ORCID: 0009-0007-9847-4034

Сатвіндер Сінгх Рупраб [A]

Доктор, старший викладач, кафедра інформаційних технологій, Школа обчислювальної техніки та інформатики, e-mail: dotanga@mmust.ac.ke, ORCID: 0000-0003-3695-196X

Даніель Отангак [A]

Доктор, старший викладач і декан, кафедра інформаційних технологій, Школа обчислювальної техніки та інформатики, e-mail: ssingh@mmust.ac.ke, ORCID: 0000-0001-7212-1088

[A] Masinde Muliro University of Science and Technology, Kakamega, Kenya

[A] Університет науки і технологій Масінде Муліро, Какемега, Кенія

Received: June 21, 2025 | Revised: August 01, 2025 | Accepted: August 31, 2025

DOI: https://doi.org/10.33445/sds.2025.15.4.14

Purpose. To develop a framework for securing business assets against social engineering attacks in state corporations in Kenya.

Method: Mixed methods.

Findings. The study found a rise in social engineering (SE) attacks, with phishing being the most common. Employee awareness and training were identified as the most critical factors in managing SE threats, supported by awareness programs, reporting practices, and integration with other training initiatives.

Theoretical Implications. A lack of tailored frameworks and methods for addressing SE attacks in Kenyan state corporations was identified, underscoring the need for an effective cybersecurity framework.

Practical implications. The study provides insights for cybersecurity professionals to better prevent, detect, and respond to SE attacks, while helping state corporations strengthen security, promote cybersecurity culture, and improve policy and governance.

Value. It highlights the importance of employee compliance with security policies and skills in mitigating SE threats to business assets.

Future Research. Further work should focus on advanced detection techniques, such as machine learning, and the impact of emerging technologies like AI chatbots on SE methods.

Paper type. Empirical.

Key words: Social Engineering attacks, cybersecurity, State Corporations, phishing, business assets.

Мета дослідження. Розробити рамкову модель для захисту бізнес-активів від атак соціальної інженерії у державних корпораціях Кенії.

Метод дослідження. Застосовано змішаний підхід.

Результати дослідження. Встановлено зростання атак соціальної інженерії, серед яких найпоширенішим є фішинг. Ключову роль у протидії відіграє рівень обізнаності та навчання персоналу з питань інформаційної безпеки.

Теоретичне значення. Виявлено брак спеціалізованих фреймворків та методик для протидії атакам соціальної інженерії у держкорпораціях Кенії, що підкреслює потребу у створенні ефективної моделі кіберзахисту.

Практичне значення. Результати корисні для фахівців з кібербезпеки та державних корпорацій у посиленні захисту, формуванні культури кібербезпеки та вдосконаленні політики інформаційної безпеки.

Цінність дослідження. Дослідження допомагає краще зрозуміти рівень захищеності організацій та наголошує на важливості дотримання політик і процедур безпеки працівниками.

Подальші дослідження. Доцільно розвивати сучасні методи виявлення атак, зокрема на основі машинного навчання, а також аналізувати вплив нових технологій, таких як чат-боти зі штучним інтелектом.

Тип статт.: Емпірична.

Ключові слова: Атаки соціальної інженерії, кібербезпека, державні корпорації, фішинг, бізнес-активи.

Introduction

State corporations in Kenya increasingly rely on information technology to operate and manage their assets. However, this reliance has made them vulnerable to a range of cyber threats, among which social engineering attacks have emerged as a significant concern. Social engineering is defined by [1] as tactics that exploit human weaknesses and persuade individuals to violate established security processes and protocols. According to [2], the effectiveness of social engineering attacks stems from the fact that they target people, who are the most vulnerable component of any security framework. Unlike technological flaws, which can be identified and corrected, human behavior is unpredictable and easily manipulated. In today's digital age, social engineering poses a substantial

threat to both informational and economic security. This is largely due to the growing complexity of information and technological systems. Additionally, [3] found that social engineers attempt to exploit the weakest element in a security architecture by convincing individuals and organizations to disclose essential, sensitive, and confidential information belonging to the organization. Similarly, the principle of persuasion, as highlighted by [4], suggests that humans are more likely to accept and act upon a message if it is presented in a way that appears authentic. According to [5], the focus of social engineering has shifted from targeting individual users to exploiting the entire social network within an organization. Moreover, [6] observed that phishing and other social engineering tactics have evolved significantly. This evolution has been fueled by the development of collaborative systems and practices such as BYOD (bring your own device), which provide avenues for threats like phishing, email fraud, and other malicious communication tools, thereby increasing the risks of network intrusions, especially through counterfeit websites or phishing emails. Recent cybersecurity incidents have revealed such vulnerabilities, for example, the attack on the eCitizen platform in 2023 by the Anonymous Sudan group, which caused major disruptions to critical government services. In this attack, private-sector entities were also affected, including mobile payment providers and ticketing services operated by SGR, as discussed by [7] and [8]. The aim of this research was to develop a framework to secure business assets against social engineering attacks. This framework is intended to provide valuable insights for policymakers in state corporations and researchers seeking to advance knowledge in the field of social engineering. To achieve this, state corporations from four different cities were surveyed through questionnaires and strategic interviews that focused on various aspects of social engineering and cybersecurity threats. The quantitative data were analyzed using descriptive statistics, which were applied to organize and present the findings in the form of tables, graphs, percentages, and frequencies. Thematic analysis was employed to interpret the qualitative data. Data analysis was conducted using the latest version of the Statistical Package for the Social Sciences (SPSS, version 30.0).

Data and methods

This study reviewed frameworks within the cybersecurity domain, with a particular emphasis on social engineering (SE) threats, drawing insights from extensive literature on securing business assets against such attacks in state corporations in Kenya. The literature search encompassed peer-reviewed journal articles, case studies in government agencies, conference proceedings related to social engineering and cybersecurity attacks, and documented best practices in cybersecurity. The review was limited to articles published within the last 10 to 15 years to capture recent findings and advancements. The databases consulted included ACM Digital Library, JSTOR, Google Scholar, Scopus, IEEE Xplore, Web of Science, the Directory of Open Access Journals (DOAJ), and ScienceDirect. Additionally, databases specializing in social engineering and cybersecurity attacks were used for specific case studies.

1. Research Design

According to [9], research design is a structured approach employed to gather reliable responses to questions concerning a research topic. It provides a detailed guide on how to define parameters, collect data, conduct measurements, and analyze the information obtained. The study adopted a mixed-methods design, combining both quantitative and qualitative approaches. Research tools, including questionnaires, interviews, and observations, were also used to provide a comprehensive understanding of the study. The quantitative design enabled the researchers to measure the population required for statistical investigation, offering valuable indicators regarding which variables were most suitable for quantitative testing. [10] emphasized that qualitative research helps evaluate data systematically by using common expressions to draw appropriate conclusions and recommendations in a social context, reflecting the perspectives of the individuals studied.

2. Location of the Study

The primary focus of this study was the cities of Nairobi, Kisumu, Mombasa, and Nakuru. These four cities were selected because they are major centers of state corporations that rely heavily on IT for day-to-day operations. Additionally, their excellent internet connectivity promotes higher adoption rates of IT technologies compared to other towns in Kenya, making them ideal locations for examining the protection of business assets against social engineering attacks. Respondents in these state corporations were chosen using purposive sampling to ensure that the study focused on the most relevant participants.

3. Population of the Study

[11] defines a target population as the entire set of individuals or entities toward which research aims to generalize its findings. [12] supports this view by describing population as a collective of entities, objects, or individuals that share specific homogeneous characteristics. This homogeneity allows results obtained from sampled subsets to accurately reflect the features of the entire group. The study selected 30 state corporations, involving CEOs, Directors, Deputy Directors, CFOs, System Administrators, Network Administrators, Database Administrators, Computer Technologists, system end users, and employees from HR and Procurement departments, yielding a target population of 153 respondents. Purposive sampling was employed to determine the sample sizes for each city, as summarized in Table 1 below.

Table 1 – Sampling setting

City	No. of respondents
Nairobi	105
Mombasa	26
Kisumu	13
Nakuru	9
Total	**153**

Source: <Author (2025)>

4. The Sample Size and Sampling Procedure

Purposive and stratified random sampling methods were employed to select participants from four cities in Kenya. According to [13], purposive sampling is an appropriate approach when certain groups of people have unique characteristics and can provide more insightful information compared to other groups within the same population. In this study, purposive sampling was used because individuals with essential knowledge were intentionally selected to provide information that could not be obtained from other sources. Stratified random sampling was also employed, as it ensures that every employee has an equal chance of being selected within their respective strata and allows participants to be chosen in proportion to their representation in the general population, as emphasized by [14].

Purposive sampling was applied to select 153 individuals with IT expertise and key system users—specifically those handling sensitive, confidential, and critical data requiring secure privacy measures and the use of IT resources for daily operations. The decision to use purposive sampling is supported by [15], who argues that individuals are intentionally chosen for the valuable information they can provide, which cannot be obtained elsewhere. In total, 153 individuals were purposively selected from 30 state corporations to participate in the study. Consequently, the overall sample size for this study was 153 respondents, as shown in the distribution detailed in Table 2 below.

Table 2 –Members of State Corporation Engaging in the Survey

Section/Users	No. of participants
CEO/Directors/Deputy Directors	10
CFOs	10
System admins/ Network Admins/ IT Technicians/ Database Admins/ Computer Technologists	40
Human Resource Department	20
Procurement Department	25
Other End Users/ Other System Users	48
Total	**153**

Source: <Author (2025)>

5. Reliability and Validity Analysis

According to [16], the validity of a tool is defined as its ability to accurately measure what it is intended to measure. Similarly, [14] noted that validity refers to how effectively the chosen instrument assesses the variables under study. Additionally, [17] defines reliability as the stability of outcomes across time or among different respondents. In this study, reliability refers to the internal consistency of the instrument, which evaluates the consistency of responses related to an underlying variable. Incorporating feedback from experts and participants ensured that both validity and reliability were thoroughly addressed, thereby strengthening the study's credibility. In this research, validity was assessed through content validity, which determines how effectively the survey instruments captured the variables outlined in the study. Furthermore, credibility was examined by conducting suitability tests on the research data, including the Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy and Bartlett's test of sphericity. Internal validity was evaluated for each subscale, as presented in Table 3 below.

Table 3 –Test of internal validity

KMO Index	Bartlett's Test		
	Approx. Chi-Square	df	Sig.
0.869	5290.936	150	0.000

Source: <Research Data (2025), SPSS Analysis>

Table 3 shows that all subscales of the questionnaire yielded a significant value of less than 0.0001 ($p \leq 0.001$) on Bartlett's test of sphericity. Moreover, the KMO index was 0.869, which is above the minimum threshold of 0.8 for internal validity. According to [18], a significant KMO index combined with a Bartlett's test value exceeding 0.6 indicates that the conditions for sufficient internal validity are met.

The data obtained were used to calculate the Cronbach's alpha coefficient (α) as a measure of the internal consistency of the respondents' data, derived from how closely related the data sets are. A high level of reliability is indicated by the Cronbach's alpha value of 0.93, leading to the conclusion that the instrument demonstrated "good" reliability. Additionally, [19] confirms that the instrument was considered reliable, since the reliability coefficient of the variables was 0.93, as shown in Table 4 below.

Table 4 –Test of reliability

Cronbach's Alpha Coefficient (α)	Cronbach's Alpha coefficient (α) standardized Items	N of Items
.928	.935	17

Source: <Research Data (2025), SPSS Analysis>

Results and Discussion

1. The types of SE attacks

The study evaluated the different forms of SE threats affecting state corporations in Kenya. Participants were asked to indicate the extent to which they had been affected by various types of SE attacks. They were instructed to specify their responses using the following categories: no level, little level, moderate level, great level, and very great level. The prevalence of SE attacks was assessed using a five-point Likert scale ranging from 1: No Level (NL), 2: Little Level (LL), 3: Moderate Level (ML), 4: Great Level (GL), to 5: Very Great Level (VGL), and the results were analyzed as percentages. The respondents' views are summarized in Table 5 below.

Table 5 –Respondents' views on the types of social engineering attacks

Item	NL	LL	ML	GL	VGL
	Frequency	Frequency	Frequency	Frequency	Frequency
Ransomware Attacks	46	25	34	31	14
Reverse Social Engineering Attacks	48	34	30	24	14
Pretexting Attacks	36	41	29	18	26
Phone/Email Scam Attacks	33	19	37	38	23
Phishing Attacks	16	26	26	42	40

Source: <Research Data (2025)>

Table 5 highlights that phishing attacks (68.5%) have emerged as the most prevalent and highly effective cybersecurity threat. In these schemes, attackers use deceptive e-mails, web pages, websites, or text messages designed to mislead individuals into revealing confidential information such as login credentials, credit card details, or other private data. Frequently, attackers impersonate legitimate entities through sophisticated social engineering techniques. Because phishing is one of the most common ways attackers gain initial access, it represents a significant threat, paving the way for additional malicious activities such as phone or email scams (59.9%), which pose serious risks to both individuals and government agencies.

The findings also indicated that 49.6% of respondents had not been affected by reverse social engineering attacks. Table 5 further suggests that 31.5% of state corporations in Kenya lack adequate protection for access to and use of their information systems. Consequently, these corporations do not sufficiently train or raise awareness among employees about the types of social engineering attacks that affect daily operations. As a result, business assets remain vulnerable, and the extent of this vulnerability is substantial enough to warrant attention. The findings of this study are consistent with [20] and [21], who emphasized that major concerns within government agencies are linked to threats such as phishing, which has emerged as the most prevalent type of SE attack in Kenyan state corporations.

2. Current Security Measures

The study aimed to identify the current security measures in use within state corporations. Respondents were asked to rate the extent of implementation as follows: no level, little level, moderate level, great level, or very great level, across different types of security measures applied in their organizations. The status of these security measures was assessed using a five-point Likert scale ranging from 1: No Level (NL), 2: Little Level (LL), 3: Moderate Level (ML), 4: Great Level (GL), to 5: Very Great Level (VGL), and was analyzed in percentages.

Findings from Table 6 reveal that 70.9% of state corporations have implemented corporate endpoint security, while 29.1% have not yet done so. Endpoint security, along with access controls for data and systems, is crucial for ensuring the security of information systems. Moreover, 72.7% of state corporations enforce strong password policies effectively, while 27.3% have not done so adequately. The respondents' views are summarized in Table 6 below.

Table 6 –Respondents' views on the current security measures

Item	NL	LL	ML	GL	VGL
	Frequency	Frequency	Frequency	Frequency	Frequency
What is the level of implementation of corporate endpoint security in the state corporation	4	28	38	42	38
What is the level of implementation of control access to data and systems assets in the state corporation	6	19	29	50	46
To what extent to have strong passwords been enforced in the state corporation	7	25	38	29	51
To what extent is scanning of malware on your PC performed	13	19	39	45	34

Source: <Research Data (2025)>

Table 6 also shows that 69.1% of respondents agreed that malware scanning on PCs is performed effectively, while 30.9% of state corporations reported that it is not performed efficiently. The results further indicate that 74.8% of state corporations in Kenya do not effectively control access to data and system assets, while only 25.2% manage access control effectively. These findings are consistent with [22], who noted that levels of access control in computing environments should be carefully considered by institutions. [22] also emphasizes that access to assets and systems is typically secured through mechanisms such as physical controls, firewalls, access lists, and privileged access, thereby strengthening access control practices. Supporting the study's findings, [23] evaluated information systems and concluded that controlled access to data, systems, assets, and other computing resources is a vital component of information security. Furthermore, the study's results corroborate those of [24], which pointed out that the availability of resources in information systems within Kenyan state corporations is influenced not only by data loss incidents but also by cybersecurity attacks.

3. Level of employee information security awareness and training

The study examined the level of employee information security awareness and training available and in use within state corporations. Awareness and training levels were assessed using a five-point Likert scale ranging from 1: No Level (NL), 2: Little Level (LL), 3: Moderate Level (ML), 4: Great Level (GL), to 5: Very Great Level (VGL), and were analyzed as percentages. Table 7 indicates that participants agreed that all employees, regardless of their position, are informed about cybersecurity and available training programs for online work, and that they undergo regular

training to report security incidents (61.1%). The views of respondents were recorded and are presented in Table 7 below.

Table 7 –Respondents' views on the level of employee information security awareness and training

Item	NL	LL	ML	GL	VGL
	Frequency	Frequency	Frequency	Frequency	Frequency
To what degree has the state corporation implemented initiatives focused on cybersecurity education and training for staff working online and remotely?	10	37	41	59	3
To what extent has the state corporation established continuous improvement programs	6	48	54	32	10
To what extent has the state corporation implemented effective security training programs	19	33	47	45	6
What is the extent of integration of other training programs with information security programs	15	33	59	33	10

Source: <Research Data (2025)>

Notwithstanding this progress, 41.3% of respondents indicated that the integration of information security with other training programs has not been implemented in state corporations, while 58.7% stated that such integration has been achieved. Moreover, 58.1% of participants reported that employees across different levels are provided with appropriate cybersecurity awareness and training on social engineering attacks. Similarly, 58.9% of respondents confirmed that their state corporation has established continuous improvement programs in cybersecurity.

These results align with the research conducted by [25], which highlights that such attacks exploit employees' lack of cybersecurity knowledge, leading them at times to unknowingly expose sensitive data or install malicious software. Additionally, [26] recommend that education and training programs should aim to raise awareness among all employees about the different types of SE attacks, the methods or tactics used by attackers, and the consequences of a successful attack within the organization. Moreover, [26] propose the use of effective simulations of social engineering attack scenarios, allowing employees to practice responding in a controlled and safe environment. According to [27], user engagement or gamification can be employed as a means of enhancing awareness among employees. To increase attention and commitment during training, [27] suggests using interactive and engaging training materials, which is supported by the findings of this study.

It is therefore clear that cultivating a cybersecurity culture within state corporations is essential, and that organizational leadership must actively support and promote this culture.

4. Organizational Culture and Policies

The study aimed to identify the different organizational cultures and policies in use within state corporations. The status of organizational culture and policies was evaluated using a five-point Likert scale ranging from 1: No Level (NL), 2: Little Level (LL), 3: Moderate Level (ML), 4: Great Level (GL), to 5: Very Great Level (VGL), and was analyzed based on percentages. The views of the respondents were recorded and are presented in Table 8 below.

Table 8 –Respondents' views on organizational culture and policies

Item	NL	LL	ML	GL	VGL
	Frequency	Frequency	Frequency	Frequency	Frequency
To what extent has the information security policy be implemented in the state corporation	3	35	35	60	17
What is the level of incident response in relation to the organizational culture	10	40	40	38	22
To what extent has the state corporation adopted risk management framework	10	28	45	54	13
To what extent has the state corporation defined collaboration between departments	3	40	49	40	18

Source: Research Data (2025)

Table 8 shows that 67.1 percent of state corporations in Kenya have implemented an information security (IS) policy. However, 32.9 percent of respondents reported that they either do not have such a policy or have not engaged with it in their organizations. This indicates that nearly one-third of state corporations lack sufficient safeguards for controlling access to and use of their information systems. Such a high proportion of corporations without an IS policy represents a significant issue that must be addressed. This finding contradicts [28], which describes an IS policy as a comprehensive document typically linked to executive leadership that defines goals and constraints for the use of information systems and should therefore be an integral part of every state corporation, accessible to all users of information systems.

The findings of this study diverge from previous research that characterized the IS policy as a management document prohibiting risky computing behaviors and practices, thereby enhancing the security of organizational systems. Additionally, Table 8 reveals that 64.3 percent of respondents stated that a risk management framework has been adopted and implemented in their corporations and effectively guides the actions of individuals using information systems. By contrast, 35.7 percent indicated that the framework has not been implemented and therefore does not adequately guide user behavior. This aligns with [29], who stated that the foundation of a robust information security framework lies in the IS policy. Similarly, [30] emphasized that a risk management framework includes effective risk assessment strategies that help identify weaknesses in information security and guide the implementation of stronger protective measures.

Furthermore, 62.9 percent of respondents reported that they were not aware of incident response practices related to organizational culture, while only 37.1 percent were sensitized to such practices and safe computing behavior. According to [31], IT security can be enhanced by establishing IS policies and incident response mechanisms that include staff training and awareness. It was also observed that 64 percent of respondents agreed that no formal collaboration between departments had been established in their corporations, while 36 percent confirmed that such collaboration had been implemented. Therefore, the insufficient execution of IS policies can be linked to the growing number of system breaches occurring within Kenyan state corporations.

Conclusion

The frequency and severity of SE attacks have been increasing, causing significant emotional distress among employees and severe financial damage to organizations. These attacks have become a serious concern, particularly when carried out without direct technical methods. Nevertheless, technical attacks remain more common than non-technical ones. Therefore, there is an urgent need for innovative methods of threat detection and preventive measures, along with cybersecurity

initiatives aimed at educating employees. State corporations must allocate resources to cybersecurity education and training in order to cultivate skilled and well-prepared staff.

The study found that phishing attacks (68.5%) are the most prevalent type of social engineering attack and represent a highly effective cybercrime tactic in state corporations. This threat paves the way for further malicious activities, such as ransomware attacks (52.3%). Moreover, the categories of SE threats identified in the study include Phone or Email Scams, Reverse Social Engineering, and Pretexting attacks.

The study also revealed that although various critical security measures are in place, employee understanding of information security and training practices (61.1%) plays a more crucial role in the overall management of social engineering in state corporations in Kenya. This includes cybersecurity training and awareness programs, continuous improvement initiatives, cybersecurity awareness campaigns, reporting of suspicious activity, and the integration of information security into other training programs.

In terms of current security measures, the actions implemented include multi-factor authentication (MFA), two-factor authentication (2FA), access controls, strong password policies, IT security standards and frameworks, regular security audits, periodic scanning of users' PCs, phishing simulation exercises, the use of secure communication protocols such as HTTPS, and the deployment of security software such as antivirus and other anti-malware programs. Organizational culture and policies primarily consist of implemented information security policies, clear IT security procedures, incident response mechanisms, the adoption of a risk management framework, and defined collaboration between departments. The study's observations highlight that state corporations remain vulnerable if any of these social engineering techniques are employed during an actual attack.

Finally, employee compliance with established security policies, practices, and procedures, together with adequate user skills, plays a vital role in mitigating social engineering attacks on business assets. The types of social engineering attacks, the current security measures, the level of employee information security awareness and training, as well as organizational culture and policies, are all crucial factors in securing business assets against social engineering attacks in Kenyan state corporations.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

1. ENISA (2021). Social Engineering: Exploiting the weakest links. Enisa.europa.eu. Retrieved from: http://www.enisa.europa.eu/publications/archive/social-engineering. Retrieved on: 14/06/2024.
2. Jamshed, & Jahangir (2021). Cultural Implications of China Pakistan Economic Corridor. Vol. 2. no. 4.
3. Carey, B. (2017). Protect or disclose? Confidential information in the Cayman Islands. Trusts and Trustees. ttw229. doi:10.1093.
4. Garcia-Alfaro, J., & Navarro-Arribas, G. (2009). A Survey on Cross-Site Scripting Attacks. Retrieved from: http://arxiv.org/abs/0905.4850.

5. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Vol. 22. Journal of Information Security and Applications. https://doi.org/10.1016/j.jisa.2014.09.005.
6. Pathak et. al (2014). E-governance, Corruption and Public Service Delivery: A Comparative Study of Fiji and Ethiopia. Joaag, vol. 3. no. 1.
7. Cheruiyot, K. (2023). CS Owalo admits cyberattack on eCitizen portal insists data secure. Daily Nation. Retrieved from: https://www.nation.africa.
8. Gooding, M. (2023). Anonymous Sudan DDoS cyberattacks cripple Kenya's new e-Citizen digital infrastructure. Retrieved from https://techmonitor.ai/technology/cybersecurity/anonymous-sudan-kenya-ddos-cyberattack-ecitizen.
9. Matthews, B., & Ross, L. (2014). Research methods. Pearson Higher Ed.
10. Berg, B. (2009). Qualitative Research Methods. 7 ed. Boston: Allyn and Bacon.
11. Cooper, C. R., & Schindler, P. S. (2008). Business Research Methods. 10 ed. McGraw-Hill.
12. Kombo, D. K., & Tromp, D. L. (2006). Proposal and thesis writing: An introduction. Nairobi: Paulines Publications Africa. pp10-45.
13. Tongco, M. D. (2007). Purposive sampling as a tool for informant selection. vol. 5. Ethnobotany Research and applications.
14. Mugenda, O. & Mugenda, A. (2019). Research methods: quantitative and qualitative approaches.
15. Padgett, D. K. (2016). Qualitative methods in social work research. Sage Publications vol. 36.
16. Anastasiadou, S. D. (2011). Reliability and Validity Testing of a New Scale for Measuring Attitudes Toward Learning Statistics with Technology. Acta Didactica Napocensia. vol. 4. no. 1. pp 1–10.
17. Fienberg, S. E. (2012). Statistics for Social and Behavioral.
18. Creswell, J. W. & Clark, V. P. (2007). Designing and conducting mixed methods research.
19. Nunnally, J. (1978). Psychometric theory. New York: McGraw-Hill 2nd ed.
20. Miryala, N., & Gupta, D. (2022). Data Security Challenges and Industry Trends. International Journal of Advanced Research in Computer and Communication Engineering. https://doi.org/10.17148/ijarcce.2022.111160.
21. Mphatheni, M., & Maluleke, W. (2022). Cybersecurity as a Response to Combating Cybercrime. International Journal of Research in Business and Social Science.
22. Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.
23. Mitnick, K., & Simon, W. (2011). The Art of Deception: Controlling the Human Element of Security. Wiley, New York.
24. Mang'ira, R. (2014). Towards establishment of a full-fledged disaster management department for Moi University libraries.
25. Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity Threats in Fintech: A Systematic Review. Expert Systems with Applications. 241, Article ID: 122697.
26. Aldawood, H., & Skinner, G. (2020). Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. 26th International Conference on Systems Engineering. Sydney, 8-20 December, 1-6. https://doi.org/10.1109/ICSENG.2018.8638166.
27. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers and Security. vol. 98. Retrieved from: https://doi.org/10.1016/j.cose.2020.102003.
28. Kimwele, M. M. (2011). Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs). Int. J. Comput. Sci. Secur. vol. 5.

29. Peltier, T. R. (2005). Implementing an Information Security Awareness Program. Information Systems Security. Vol. 14. no. 2. pp 37-49.
30. Hu, Q. D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decision Sciences. vol 43. no. 4. pp 615-660.
31. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.

Список використаних джерел

1. ENISA (2021). Social Engineering: Exploiting the weakest links. Enisa.europa.eu. Retrieved from: http://www.enisa.europa.eu/publications/archive/social-engineering. Retrieved on: 14/06/2024.
2. Jamshed, & Jahangir (2021). Cultural Implications of China Pakistan Economic Corridor. Vol. 2. no. 4.
3. Carey, B. (2017). Protect or disclose? Confidential information in the Cayman Islands. Trusts and Trustees. ttw229. doi:10.1093.
4. Garcia-Alfaro, J., & Navarro-Arribas, G. (2009). A Survey on Cross-Site Scripting Attacks. Retrieved from: http://arxiv.org/abs/0905.4850.
5. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Vol. 22. Journal of Information Security and Applications. https://doi.org/10.1016/j.jisa.2014.09.005.
6. Pathak et. al (2014). E-governance, Corruption and Public Service Delivery: A Comparative Study of Fiji and Ethiopia. Joaag, vol. 3. no. 1.
7. Cheruiyot, K. (2023). CS Owalo admits cyberattack on eCitizen portal insists data secure. Daily Nation. Retrieved from: https://www.nation.africa.
8. Gooding, M. (2023). Anonymous Sudan DDoS cyberattacks cripple Kenya's new e-Citizen digital infrastructure. Retrieved from https://techmonitor.ai/technology/cybersecurity/anonymous-sudan-kenya-ddos-cyberattack-ecitizen.
9. Matthews, B., & Ross, L. (2014). Research methods. Pearson Higher Ed.
10. Berg, B. (2009). Qualitative Research Methods. 7 ed. Boston: Allyn and Bacon.
11. Cooper, C. R., & Schindler, P. S. (2008). Business Research Methods. 10 ed. McGraw-Hill.
12. Kombo, D. K., & Tromp, D. L. (2006). Proposal and thesis writing: An introduction. Nairobi: Paulines Publications Africa. pp10-45.
13. Tongco, M. D. (2007). Purposive sampling as a tool for informant selection. vol. 5. Ethnobotany Research and applications.
14. Mugenda, O. & Mugenda, A. (2019). Research methods: quantitative and qualitative approaches.
15. Padgett, D. K. (2016). Qualitative methods in social work research. Sage Publications vol. 36.
16. Anastasiadou, S. D. (2011). Reliability and Validity Testing of a New Scale for Measuring Attitudes Toward Learning Statistics with Technology. Acta Didactica Napocensia. vol. 4. no. 1. pp 1–10.
17. Fienberg, S. E. (2012). Statistics for Social and Behavioral.
18. Creswell, J. W. & Clark, V. P. (2007). Designing and conducting mixed methods research.
19. Nunnally, J. (1978). Psychometric theory. New York: McGraw-Hill 2nd ed.
20. Miryala, N., & Gupta, D. (2022). Data Security Challenges and Industry Trends. International Journal of Advanced Research in Computer and Communication Engineering. https://doi.org/10.17148/ijarcce.2022.111160.

21. Mphatheni, M., & Maluleke, W. (2022). Cybersecurity as a Response to Combating Cybercrime. International Journal of Research in Business and Social Science.
22. Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.
23. Mitnick, K., & Simon, W. (2011). The Art of Deception: Controlling the Human Element of Security. Wiley, New York.
24. Mang'ira, R. (2014). Towards establishment of a full-fledged disaster management department for Moi University libraries.
25. Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity Threats in Fintech: A Systematic Review. Expert Systems with Applications. 241, Article ID: 122697.
26. Aldawood, H., & Skinner, G. (2020). Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. 26th International Conference on Systems Engineering. Sydney, 8-20 December, 1-6. https://doi.org/10.1109/ICSENG.2018.8638166.
27. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers and Security. vol. 98. Retrieved from: https://doi.org/10.1016/j.cose.2020.102003.
28. Kimwele, M. M. (2011). Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs). Int. J. Comput. Sci. Secur. vol. 5.
29. Peltier, T. R. (2005). Implementing an Information Security Awareness Program. Information Systems Security. Vol. 14. no. 2. pp 37-49.
30. Hu, Q. D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decision Sciences. vol 43. no. 4. pp 615-660.
31. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.