International Journal of Scientific Research and Management (IJSRM)
||Volume||12||Issue||8||Pages||7027-7035||2024||
Website: https://ijsrm.net ISSN: 2321-3418
DOI: 10.18535/ijsrm/v12i08.em04

Influence of Organizational Security Learning Practices on Insider Security Threats in SoCs in Kenya

Charles Mwenda Ikiara[1], Dr. Boniface Ratemo, PhD[2], Dr. George Musumba, PhD[3]

[1] Student, Master of Science in Forensic and Security Management, Security Management Option, Institute of Criminology, Forensics and Security Studies, Dedan Kimathi University of Technology, Nairobi Campus, Loita Street, Pension Towers, 2nd Floor, Kenya

[2] Lecturer Institute of Criminology, Forensics and Security Studies, Dedan Kimathi University of Technology, Nairobi Campus, Loita Street, Pension Towers, 2nd Floor, Kenya

[3] Lecturer Institute of Criminology, Forensics and Security Studies, Dedan Kimathi University of Technology, Nairobi Campus, Loita Street, Pension Towers, 2nd Floor, Kenya

Abstract:
Insider threats have consistently been identified as key threats to State-owned Corporations and governments (SoCs). Research has shown that huge amounts of resources go towards safeguarding organizations' assets and information systems from external threats in total disregard of potential threats from malicious and compromised insiders. Recent studies indicate that insider threats are on the rise and have cost the Kenyan economy $ 36Million USD. In addition, investigations show that these threats are increasing in scale, scope, and sophistication. The general objective of the study was to investigate on the organizational factors influencing insider security threats in State-owned Corporations in Kenya. Specifically, the study evaluated the influence of organizational security policies, organizational security learning practices and organizational communication practices on insider security threats in State-owned Corporations in Kenya. The study was anchored on the CISA Insider Threats Risk Score Model, deterrence theory, social learning theory and the communication privacy management theory. The study adopted descriptive correlational research design. The target population was 187 State-owned Corporations in Kenya. A census sampling design was used targeting the Security managers or their equivalent in SoCs. The researcher utilized a self-administered questionnaire as the data collection method. Data was analyzed through quantitative techniques using the SPSS. The study established that organizational security policies have significant influence on insider security threats in SoCs in Kenya. The study also established that organizational security learning practices have significant influence on insider security threats in SoCs in Kenya. In addition, the study revealed that organizational communication practices have significant influence on insider security threats in SoCs in Kenya. The study also deduced that the combined influence of organizational security policies, learning practices and communication practices (organizational factors) significantly influence insider security threats in SoCs in Kenya. The study recommends that SoCs consider conducting a comprehensive review of their existing security policies, ensuring clarity on the severity of consequences for insider threats. Further, the study recommends that SoCs work on strengthening their learning policies to emphasize the importance of observational learning, role modeling, and positive reinforcement in the context of security awareness to address insider security threats. Additionally, the study recommends that SoCs provide training programs that emphasize effective communication practices surrounding privacy management.

Keywords: Insider Threats, organizational security learning practices, observational learning, imitation and modelling, reinforcement learning and self-efficacy.

1. Introduction

1.1. Background of the Study

Insider threats have consistently been identified as key threats to organizations and governments. According to a 2020 global report by Warkentin and Willison (2020), the average global cost of insider threats rose by

31% in the last two years to $11.45 million, and the occurrence of incidents spiked by 47% in that period. Additionally, the report indicates that these threats are increasing in scale, scope, and sophistication; thus, emphasizing the critical need for organizations to apply current security techniques. Many organizations invest in security defenses to strengthen their network against outside malicious attacks but fail to deploy protection against potential threats by malicious or compromised insiders (Spear, Beyer, Cittadini, & Saltonstall, 2018).

Insiders, which refers to any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and system (CISA, 2020), can abuse their authorized access to critical systems and eventually steal or modify organizations' assets for malicious intent or financial gain (Alsowail & Al-Shehari, 2020). Insider threats targets not only private sector enterprises, but also government institutions and critical infrastructures for motives, ranging from monetary gains and industrial espionage to business advantage and sabotage. Other ways in which insider threats manifest include disgruntled employees and revenge as well as theft. According to Homoliak, Toffalini, Guarnizo, Elovici, and Ochoa, (2019), because insiders have access to valuable information assets that are unavailable to outsiders, damages resulting from insider attacks can be devastating.

In Kenya, according to Gathu (2020), the public sector, including government entities and related organizations, was identified as having the highest risk levels in terms of information security. In 2019, cyber-attacks initiated from within, targeting government ministries created widespread panic throughout the country. These intrusions involved unauthorized access to websites that were expected to contain state secrets, as well as sensitive security and financial information and the affected websites included those operated by the government's banker (CBK), the Registration of Persons and Immigration Department, the government's financial accounting system (IFMIS), the Attorney General's office, and the Kenya Defense Forces (Gathu, 2020).

According to Walumbe, Ogalo and Wasike (2019) insider threat attacks cost the public sector in Kenya over Ksh5 billion, not accounting for the expenses incurred in system recovery. These cyber-attacks also had a detrimental impact on stakeholders' confidence in e-government initiatives, consequently hindering service delivery by the public sector. Therefore, there was a pressing need to conduct a study to explore the organizational factors that influence insider security threat in the public service, specifically in the SoCs in Kenya

1.2. Problem Statement

Organizations have always put forward superior tools, procedures, and policies in the process of protecting assets and information systems from attackers and infiltration from outside. Despite the amount of investment channelled towards development of infrastructure and manpower in guarding against the external aggressors, Kenyan SoCs still experience significant attacks causing substantial loses (Ndeda & Odoyo, 2019). These loses can be attributed to organizations' failure to deploy sufficient preventive measures against potential threats by malicious or compromised insiders (Spear et al., (2018). According to Gathu (2020), insider threats have been on the rise and have cost the Kenyan economy about $36 million USD, with 40% of these threats targeting known vulnerabilities that have remained largely unaddressed by various SoCs in Kenya. This is further evidenced by the PwC (2019) study which stated that less than half (49%) of corporations surveyed demonstrated that they have actualized blueprints to tackle insider threats with 51% only guarding against attackers and infiltration from outside. According to the Kenya Cyber security Report (2021) Kenya had 72 million threat detections in 2020/2021 alone.

Though efforts have been made by the Kenyan SoCs to work closely with law enforcement agencies to investigate and address insider threats when they occur by ensuring that appropriate legal actions are taken, these efforts are always a reaction after the insider security breaches have happened and thus do minimally at reducing the insider threats thus calling for more preventive measures (Haidar & Gaber, 2019). In spite of this, Kisutsa and Shiyayo (2020) observed that there are few statistics on insider attacks in Kenyan SoCs because they are rarely reported to the authorities. This is when management of most SoCs feel that the harm from reporting insider attacks outweighs the benefit of public prosecution of the perpetrators. Resultantly, insider attacks escalate hence remaining key security threats in Kenyan SoCs. Hence, Walumbe, Ogalo and Wasike (2020) avers that not only has the scope of insider threats become heightened, the attacks have developed in complexity, are much more constant and utilize witty tactics than before.

In addition, the extant body of literature has hardly examined organizational factors influencing insider security threats in SoCs in Kenya. Even so, many researchers such as Wapukha (2020), Cooley, (2021) and Liu, et al., (2018) have proposed a layered defense approach involving policies, procedures, and behaviour controls as an effective way to address insider security threats. However, there are limited studies on the specific link between organizational security learning practices and insider security threats. This study therefore sought to close this knowledge gap by investigating on the organizational security learning practices influencing insider security threats in SoCs in Kenya.

1.3. Purpose of the Study

To evaluate the influence of organizational security learning practices on insider security threats in SoCs in Kenya.

1.4. Research Hypothesis

H_{01}: Organization learning practices have no significant influence on insider security threats in SoCs in Kenya

2. Literature Review

2.1. Theoretical Literature

The study used the social learning theory as developed by Bandura (1977) in exploring the influence of organizational security learning practices on insider security threats in SoCs. The social learning theory suggests that individuals learn through observation, modelling, and imitation of the behavior of others. It states that learning is a cognitive procedure that happens within a social environment and can transpire solely through observation or explicit instruction, even without physically imitating or receiving immediate rewards. Besides observing behavior, learning also transpires through witnessing the consequences of actions, such as rewards or punishments, which is termed as vicarious reinforcement (Baykara & Das, 2019). If a behavior is consistently rewarded, it is likely to continue, whereas if a behavior is consistently punished, it is likely to cease.

In the context of organizational security, the social learning theory suggests that insiders can learn to engage in secure behaviors by observing and modelling the behavior of their peers and superiors. According to the social learning theory, four key factors can influence an individual's decision to engage in a particular behavior: attention, retention, reproduction, and motivation (Liu, et al., 2018). In the context of security learning practices, this means that insiders are more likely to engage in secure behaviors if they are paying attention to the information presented, can retain and recall that information, can reproduce the behavior, and are motivated to do so. The theory thus has key guiding concepts that include.

Observational Learning: is a fundamental mechanism through which individuals learn by observing others' behaviors and the outcomes of those behaviors. This type of learning allows individuals to acquire new knowledge, skills, attitudes, and behaviors without direct personal experience, making it a powerful form of learning and behavior change.

Imitation and modelling: Imitation and modelling are integral components of observational learning, playing a significant role in shaping individuals' behaviors and promoting social learning within communities and cultures. Both processes involve the replication of behaviors observed in others, but they differ in terms of who performs the behavior and who observes it.

Reinforcement: Reinforcement is a critical concept in social learning theory, which emphasizes the role of consequences in shaping behavior. It refers to the process by which the consequences of a behavior influence the likelihood of that behavior being repeated in the future. Reinforcement can be positive, where a reward or favorable outcome follows a behavior, or negative, where the removal of an aversive stimulus strengthens the behavior. Both types of reinforcement can influence social learning and the likelihood of imitation.

Self-efficacy: Self-efficacy is a key concept in social learning theory that refers to an individual's belief in their own ability to successfully perform a specific behavior or accomplish a particular task. In other words, self-efficacy is the confidence a person has in their own capabilities to achieve desired outcomes.

Vicarious reinforcement and punishment: Vicarious reinforcement and punishment are essential concepts in social learning theory, proposed by psychologist Albert Bandura. These processes illustrate how individuals can learn from the experiences of others, even without directly experiencing the consequences of a behavior themselves. Through observation, individuals can acquire new knowledge, attitudes, and behaviors based on the rewards and punishments others receive for their actions.

Organizations can use the social learning theory to develop and implement effective security learning practices that encourage insiders to engage in secure behaviors and reduce the risk of insider security threats. These practices should manifest clear and concise conduct on security policies and procedures, including how to identify and report potential security threats.

2.2. Conceptual Framework

A conceptual framework is a theoretical structure or model that provides a foundation for understanding and analyzing a particular subject or phenomenon (Paul & Criado, 2020). It establishes the key concepts, variables, and relationships involved in a research study or theoretical framework. Figure 1 presents the study's conceptual framework which shows the relationship of the variables.

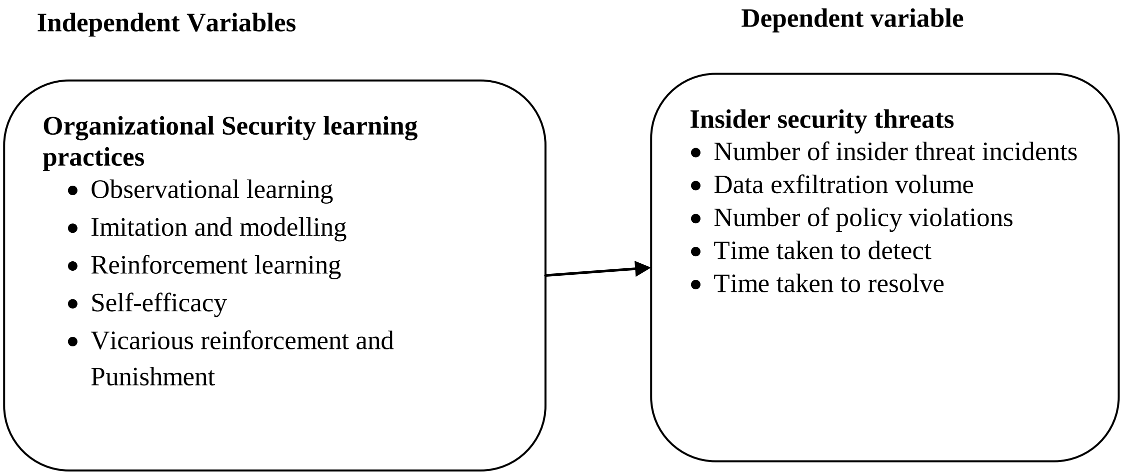

Figure 1: Conceptual Framework

Figure 2: Conceptual Framework

2.3. Empirical Literature

Dhillon (2018) investigated on the influence of security learning practices on insider threats. The research showed that regular security learning and education increase awareness of security risks and best practices, which in turn reduce the likelihood of insider security threats. The literature suggests that organizations can reduce the risk of insider security threats by implementing clear security policies and procedures, providing regular security training and education, and fostering a culture of security awareness and communication (Maalem, Caulkins, Mohapatra, & Kumar, 2020).

Torto and Fernandez (2022) in their study in the USA established that organizational security learning practices play a crucial role in shaping and influencing the behaviour of employees when it comes to insider security threats. These learning programs are designed to educate and empower individuals within the organization to recognize and respond to security risks effectively (Pieterse, 2021). Organizations significantly mitigate the potential impact of insider threats by instilling a culture of security consciousness. One of the primary ways in which security learning programs influence insider security threats is through prevention (Rodbert, 2020). The security awareness programs provide comprehensive education and training, thus enabling employees become more knowledgeable about the various types of security risks they may encounter. They learn about common attack vectors, such as phishing emails, social engineering tactics, or unauthorized access attempts (Pieterse, 2021). Armed with this knowledge, insiders are better equipped to identify and avoid potential threats, thus reducing the likelihood of falling victim to malicious activities.

In their study in the UK, Bell, Rogers and Pearce (2019) averred that organizational security learning programs emphasize best practices and secure behaviors. Employees are educated about the importance of creating strong passwords, regularly updating software and applications, and adhering to data classification policies. As they promote these secure practices, organizations create a robust security foundation that makes it harder for insiders to exploit vulnerabilities or gain unauthorized access to sensitive information (Bell, et al., 2019). Security learning practices also focus on the early detection of insider threats. Employees are encouraged to be vigilant and report any suspicious activities they observe (Chattopadhyay, et al., 2018). Organizations can tap into their most valuable resource, their employees, to act as an early warning system, by establishing clear reporting channels and providing guidance on what constitutes a potential security incident. Timely reporting enables security teams to investigate and respond to potential threats promptly, minimizing the potential damage that an insider threat can cause.

In their study in South Africa, Silaule, Makhubele and Mamorobela (2022) postualted that organizational security learning practices help foster a culture of trust and responsibility within the organization. A sense of accountability is instilled by emphasizing the shared responsibility of all employees in maintaining the security of the organization's systems and data. Employees understand that their actions have a direct impact on the organization's overall security posture (Schoenherr & Thomson, 2021). This culture of security consciousness encourages individuals to be more cautious, responsible, and vigilant in their day-to-day activities, reducing the likelihood of accidental or intentional security breaches. Von Solms and Van Niekerk (2018) averred that learning programs act as a deterrent to potential insider threats. When employees are well-informed about the consequences of engaging in malicious activities or violating security policies, they are less likely to take such risks. The learning programs highlight the legal, financial, and reputational ramifications associated with insider threats, reinforcing the importance of adhering to security protocols (Al-Shanfari, Yassin, & Abdullah, 2020).

3. Methodology

This study used a descriptive correlational research design. The study's target population was 187 SoCs in Kenya. A sample was selected from a population of 187 using a stratified random sampling technique. The purpose of stratified random sampling is to ensure that various sub-groups within the population are adequately represented. Within each stratum, the study employed simple random sampling for selecting the IT managers.

Table 1: Sample Size

Agency Category	**Population (N)**	**Sample**
State Corporations with Commercial Strategic Functions	21	14
Commercial State Corporations	34	23
Regulatory Agencies	25	17
Public Universities, Research Institutions, Training Institutions and Tertiary Education	45	30
Executive Agencies	62	42
Total	**187**	**126**

The primary method of data collection in this study involved using a structured questionnaire. Closed-ended questions were included in the questionnaire. The use of questionnaires enabled the researcher to ensure consistency in the way questions were posed, leading to greater compatibility in the responses obtained. The questions were structured and were designed to address specific objectives and offer a variety of possible responses. Some of the questionnaires were hand-delivered by the researcher, while others were sent to the respondents electronically. For the questionnaires delivered in person, the researcher distributed them and later collected them. The respondents completed the questionnaires and left them for the researcher to collect at a later agreed-upon time. The study produced a quantitative data. Quantitative data was categorized and inputted into Statistical Packages for Social Scientists (SPSS Version 26) for analysis, utilizing descriptive statistics. Descriptive statistics entailed the utilization of absolute and relative percentages, as well as measures of central tendency and dispersion (mean and standard deviation, respectively). Additionally, the study employed a linear regression model to explore the connection between the dependent variable and the independent variable.

The following regression model was adopted:

$Y = \beta\ 0 + \beta_1\ X_1 + \varepsilon$

Where:

Y = Employee insider threat; X 1 = Organizational security learning practices; β 0 = Constant

β 1 = coefficient of variable; ε = error term

4. Study Findings And Discussion

The aim of this study was to investigate on the influence of organizational security learning practices on insider security threats in SoCs in Kenya.

4.1. Descriptive Statistics

The study also explored organizational security learning practices and their influence on insider security threats. The findings revealed a consensus among respondents on the importance of observational learning, with agreement that it was a critical mechanism in shaping employees' values and social skills. Role models and leaders within organizations were found to be influential figures, and observational learning was established as a valuable tool in training and educational settings. The significance of imitation and modelling in learning new skills related to threat avoidance was also revealed. Positive reinforcement, including praise, compliments, recognition, and tangible rewards, was identified as a prevalent practice within organizations.

The study highlighted that individuals with high self-efficacy were more inclined to seek learning opportunities and take on challenges, contributing to skill development and enhanced belief in their ability to avoid insider threats. The role of vicarious reinforcement and punishment was established, with revelation that observed punishment served as a deterrent, making undesirable behaviors less likely to be replicated. Vicarious reinforcement and punishment were found to be influential factors in behavior change, contributing to the development and maintenance of positive norms within organizations.

4.2. Univariate Regression Analysis

Univariate regression analysis guided the study in testing the research hypothesis. The predictive power of the model was based on R^2 while F-statistic was used to determine the fitness of the model at $P < 0.05$. The significance of the study variables was also based on P-values at 0.05 significance level. The following null hypotheses tested was:

> Ho_1: There is no significant influence of organizational security learning practices on insider security threats in SoCs in Kenya.

A univariate analysis was conducted to test the null hypothesis.

R is the correlation coefficient, which indicates the strength and direction of the relationship between the predictor and outcome variables. In this case, R = .843 suggests a strong relationship between organizational security learning practices and the outcome variable (insider security threats in SoCs in Kenya). R Square is the coefficient of determination, which indicates the proportion of variance in the outcome variable that can be explained by the predictor variable. In this case, R Square = .711 suggests that 71.1% of the variation in the insider security threats in SoCs in Kenya can be explained by organizational security learning practices.

Table 2: Model Summary for Organizational Security Learning Practices

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.843[a]	.711	.712	.44086
a. Predictors: (Constant), Organizational security learning practices				

The analysis of variance was used to determine whether the regression model is a good fit for the data. From the analysis of variance (ANOVA) findings in Table 4.11, the study found out that Prob>F (1, 103) = 0.000 was less than the selected 0.05 level of significance. This suggests that the model as constituted was fit to predict insider security threats in SoCs in Kenya. Further, the F-calculated, from the table (11.50) was greater than the F-critical, from F-distribution tables (3.933) supporting the findings that organizational security learning practices can be used to predict insider security threats in SoCs in Kenya.

Table 3: Analysis of Variance for Organizational Security Learning

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	5.742	1	5.742	11.50	.000[b]
	Residual	42.68	103	.414		
	Total	48.422	104			
a. Dependent Variable: insider security threats						
b. Predictors: (Constant), organizational security learning practices						

From the results in Table 3, the following regression model was fitted.

$$Y = 1.161 - 0.812 X_1$$

(X_1 is Organizational Security Learning Practices)

The coefficient results showed that the constant had a coefficient of 1.161, suggesting that if organizational security learning practices was held constant at zero, insider security threats in SoCs in Kenya would be 1.161 units. In addition, results showed that the organizational security learning practices coefficient was -0.812, indicating that a unit increase in organizational security learning practices would result in an 81.2% decrease in insider security threats in SoCs in Kenya. It was also noted that the P-value for organizational security learning practices coefficient was 0.000, which is less than the set 0.05 significance level, indicating that organizational security learning practices was significant. Based on these results, the study rejected the null hypothesis (H_{02}) and concluded that there is significant inverse influence of organizational security learning practices on insider security threats in SoCs in Kenya.

This means that as organizations improve and implement more robust security learning practices, the likelihood of insider security threats decreases. These findings align with the research by Jeong and Zo (2021) who also posited that organizational security learning practices significantly reduce the occurrence of insider security threats. Organizations that create an environment where security awareness and practices are continuously learned and reinforced, mitigate the risks posed by insiders who may compromise security, intentionally or unintentionally. This correlation underscores the critical role of ongoing security education and training within organizations to safeguard against internal threats.

5. Conclusion And Recommendations

5.1. Conclusion

There was a very strong inverse relationship between organizational security learning practices and insider security threats in State-owned Corporations in Kenya (r = -0.809, p value =0.000). Consequently, the research hypothesis (H_{02}) suggesting that organizational learning practices have no significant influence on insider security threats was rejected. Additionally, R Square = .711 suggested that 71.1% of the variation in the insider security threats in SoCs in Kenya can be explained by organizational security learning practices. This implies that stringent organizational security learning practices play a significant role in mitigating insider security threats in SoCs in Kenya.

The findings underscore the significant influence of the organizational security learning practices in shaping employee behaviour and mitigating insider security threats. The study revealed the critical role of observational learning, emphasizing its importance in shaping employees' values and social skills. Role models and leaders were identified as influential figures, and the study established the value of observational learning as a tool in training and educational settings. Additionally, the significance of imitation and modelling in learning skills related to threat avoidance was emphasized, reinforcing the idea that learning from positive examples contributes to threat mitigation. Positive reinforcement emerged as a prevalent practice within organizations, with praise, compliments, recognition, and tangible rewards playing a crucial role in influencing employee behaviour. The study highlighted the importance of self-efficacy, indicating that individuals with high self-efficacy are more inclined to seek learning opportunities and actively contribute to skill development, fostering a belief in their ability to avoid insider threats. This implies that stringent organizational security learning practices play a crucial role in mitigating insider security threats within SoCs in Kenya.

5.2. Recommendations

Organizations should strengthen their learning policies to emphasize the importance of observational learning, role modelling, and positive reinforcement in the context of security awareness. They should clearly outline expectations for employees to engage in continuous learning to enhance their threat avoidance skills.

Organizations should also implement initiatives to boost employees' self-efficacy, emphasizing their capability to contribute to organizational security. Provide opportunities for skill development and encourage a sense of empowerment in navigating security challenges. They should establish recognition programs that acknowledge and reward employees for exemplary security practices. Positive reinforcement through praise, compliments, and tangible rewards can further motivate employees to prioritize security.

Further studies should investigate the influence of individual learning styles on the effectiveness of security awareness programs. Tailor learning practices to accommodate diverse learning preferences, enhancing overall engagement and knowledge retention.

References

1. Al-Shanfari, I., Yassin, W., & Abdullah, R. (2020). Identify of Factors Affecting Information Security Awareness and Weight Analysis Process. *International Journal of Engineering and Advanced Technology (IJEAT)*, 9(3), 534-42.
2. Alsowail, R., & Al-Shehari, T. (2020). Empirical Detection Techniques of Insider Threat Incidents. *IEEE Access*, 1-1.
3. Baykara, M., & Das, R. (2019). A novel honeypot-based security approach for real-time intrusion detection and prevention systems. *Journal of Information Security and Applications*, 41, 103-116.
4. Bell, C., Rogers, M., & Pearce, M. (2019). The insider threat : Behavioral indicators and factors influencing likelihood of intervention. *International Journal of Critical Infrastructure Protection*, 24, 166-176.
5. Chattopadhyay, P., Wang, L., & Tan, Y. (2018). Scenario-based insider threat detection from cyber activities. *IEEE Transactions on Computational Social Systems*, 5(3), 660-675.
6. Cooley, G. C. (2021). *Insider Threats' Behaviors and Data Security Management Strategies.* Minneapolis, Minnesota: Walden Dissertations and Doctoral Studies.
7. Dhillon, B. (2018). *Insider security awareness training: A guide for security professionals.* Boca Raton, Florida, United States: CRC Press.
8. Gathu, K. (2020). *Insider Threat Detection Model For Organizations: A Case Study Of Manufacturing Companies In Thika.* Nairobi: Unpublished Masters in Information Systems and Technology thesis, United States International University-Africa.
9. Haidar, D., & Gaber, M. M. (2019). Data stream clustering for real-time anomaly detection: an application to insider threats. *Clustering Methods for Big Data Analytics*, 115-144.
10. Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insiderthreat taxonomies, analysis, modeling, and countermeasures. *ACM Comput. Surv.*, 12, 101–117.
11. Kisutsa, C., & Shiyayo, B. (2020). *The kenya cyber security report.* Nairobi: Communications Authority of Kenya.
12. Liu, L., de Vel, O., Han, Q., Zhang, J., & Xiang, Y. (2018). Detecting and preventing cyber insider threats: A survey. *IEEE Commun. Surv. Tutor*, 20, 1397–1417.
13. Maalem, A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Journal of Cybersecurity*, 3, 1-18.
14. Myeongki, J., & Hangjung, Z. (2021). Preventing insider threats to enhance organizational security: The role of opportunity-reducing techniques. *Telematics and Informatics*, 63, 1-15.
15. Ndeda, L. A., & Odoyo, C. O. (2019). *Cyber threats and cyber security in the Kenyan business context.*

16. Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *The African Journal of Information and Communication*, 28, 1-21.
17. Rodbert, M. (2020). Why organisational readiness is vital in the fight against insider threats. *Network Security,* 8(8), 7-9.
18. Schoenherr, J., & Thomson, R. (2021). The cybersecurity (CSEC) questionnaire : Individual differences in unintentional insider threat behaviours. *Journal of Information Security and Applications*, 4, 8-28.
19. Silaule, C., Makhubele, L., & Mamorobela, S. (2022). A model to reduce insider cybersecurity threats in a South African telecommunications company. *South African Journal of Information Management*, 24(1),1-8.
20. Spear, B., Beyer, B. A., Cittadini, L., & Saltonstall, M. (2018). Changing mechanisms of enterprise security (comparing beyond corp with prevalent network security mechanisms). *International Journal of Engineering & Technology*, 7(3), 72-81.
21. Torto, S., & Fernandez, F. (2022). Decrease Insider Risk with Effective Security Awareness Training. *Security Awareness Training* , 1-12.
22. Von Solms, R., & Van Niekerk, J. (2018). From information security to cyber security. *Computers and Security*, 38, 97-102.
23. Walumbe, D., Ogalo, J., & Wasike, J. (2019). The Security Mechanisms Put in Place against Insider Information Systems Security Threat in Public Universities in Kenya. *The International Journal Of Science & Technoledge*, 5(6), 50-56.
24. Wapukha, W. D. (2020). *An Update To The Insider System Security Attack Prediction Model To Suit Selected Public Universities In Kenya.* Kisii: Thesis, School of Information Science and Technology, Kisii University.
25. Warkentin, M., & Willison, R. (2020). *Cost of Insider Threats Global Report, Observer IT*. Michigan: Ponemon Institute.