Journal of Public Policy and Administration
2025, Vol. 9, No. 2, pp. 111-125
https://doi.org/10.11648/j.jppa.20250902.16

SciencePG
Science Publishing Group

Research Article

The Impact of Cybersecurity Training Policy Initiative on Cybercrime Prevention in Kenya

Kennedy Obumba Ogutu[*], **Joseph Okeyo Obosi**, **Henry Amadi Odongo**

Department of Political Science and Public Administration, University of Nairobi, Nairobi, Kenya

Abstract

Cybercrime had been a serious challenge in Kenya, threatening digital infrastructure, economic stability, and public trust in technology. It had led to financial loss, data loss, disruption, document damage, and psychological stress among others. In recognizing this, the government brought the cybersecurity training as a capacity building initiative through the Kenya National ICT Policy Despite the policy initiative being brought, Kenya continued to experience recurring incidents of system breaches, data theft, and disruptions to essential services thereby undermining public trust in digital infrastructure and highlighting the growing gap between policy intentions and the realities of cybercrime prevention and control. This study was therefore necessitated to assess the actual impact of the cybersecurity on cybercrime prevention and identify reasons for its limited effectiveness. The paper therefore evaluated how Kenya's ICT Policy on cybersecurity training contributed to the prevention of Cybercrime in Kenya. Descriptive research design alongside sequential explanatory mixed methods approach were employed. Primary data was obtained from officers working with the cybercrime prevention institutions as well as mobile communications providers such as Safaricom and Airtel in Kenya. A simple linear regression and thematic analysis were used to analyze responses collected from officers working with the cybercrime prevention institutions in Kenya. The paper established that cybersecurity training enhanced officers’ skills and aided cybercrime prevention; however, its impact varied across institutions due to differences in commitment, resources, content relevance, and integration, with key contextual and institutional factors shaping effective-ness. The paper concluded that cybersecurity training improved officers’ skills and cybercrime prevention, but its impact differs by institution, shaped by resource allocation, commitment, content relevance, and integration into operations. The paper recommended that the government and telecommunication institutions to prioritize funding, leadership support, role-specific customization, interactive delivery, robust evaluations and integration of training into operations to enhance the effectiveness and sustainability of cybersecurity training initiatives.

Keywords

Cybersecurity Training, Multi-agencies, Cybercrime Prevention

1. Introduction

Cybersecurity had become a critical issue in the digital age, with cyber threats evolving rapidly and affecting individuals, businesses, and government institutions worldwide [1]. As Kenya underwent a digital transformation, the need for robust cybersecurity measures had never been more urgent. The increasing reliance on digital platforms, mobile banking,

[*]Corresponding author: kenobumba@gmail.com (Kennedy Obumba Ogutu)

Received: 29 May 2025; **Accepted:** 12 June 2025; **Published:** 30 June 2025

e-commerce, and online government services had amplified the risks associated with cybercrime [19]. For instance, Between April 2011 and December 2019, Kenya experienced a sharp rise in cyber threats despite government interventions. Reports indicated widespread web-borne and local threats, with millions of cyber-attacks recorded annually [14]. Notable incidents included SIM card swapping, DoS attacks, and system intrusions. Threats escalated from 22.1 million in 2012–2013 to 51.9 million by 2013–2014, and by late 2019, cyber threats rose by 47.3% in just one quarter. Financial losses reached approximately Sh18 billion by 2016, highlighting a growing cybersecurity crisis [9]. Recognizing these challenges, the Kenyan government integrated cybersecurity training into its broader ICT policy framework as a key initiative to combat cyber threats. The cybersecurity training policy initiative, as outlined in Section 15.1 of the National ICT Policy, aims to strengthen the capacity of law enforcement officers, IT professionals, and other stakeholders in mitigating cyber risks [12].

The National ICT Policy highlights cybersecurity as a fundamental aspect of Kenya's digital ecosystem. Section 15.1 under-scores the importance of capacity building and skills development to ensure that cybersecurity professionals are adequately trained to prevent, detect, and respond to cyber threats. This policy framework reflects the government's commitment to ad-dressing the rising cases of cybercrime, which have been exacerbated by increased internet penetration, the proliferation of smart devices, and the growing sophistication of cybercriminals. Prioritizing cybersecurity training was envisioned to enhance Kenya's resilience against cyber threats while promoting a safe digital environment for economic and social development (Government of Kenya, 2016).

Cybercrime on the other hand has emerged as a significant threat to national security, financial stability, and individual privacy in Kenya [28]. Criminal activities such as phishing, ransomware attacks, identity theft, and financial fraud have become increasingly prevalent, targeting both private and public institutions. The Communications Authority of Kenya (CA) and the National Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC) have reported a steady rise in cyber incidents, with millions of attempted attacks detected annually [16]. Without well-trained personnel to counteract these threats, Kenya remains vulnerable to data breaches, financial losses, and reputational damage [22]. The cybersecurity training policy initiative is, therefore, a proactive response envisioned by the government to address these challenges, ensuring that stakeholders across various sectors are equipped with the knowledge and skills necessary to combat cybercrime [6].

One of the primary objectives of the cybersecurity training policy initiative was to enhance the technical capabilities of law enforcement agencies, and IT security professionals in responding to cyber threats. Law enforcement as well as cybercrime prevention officers play a crucial role in cybercrime prevention, as they are responsible for investigating and prosecuting cyber-related offenses [13]. However, the dynamic nature of cyber threats requires continuous training and skills development. Traditional law enforcement methods have been seen to be inadequate in addressing cybercrimes, necessitating a specialized approach that includes digital forensics, cyber threat intelligence, and ethical hacking techniques [17]. Therefore, the policy would ensure that officers are well-prepared to track, investigate, and apprehend cybercriminals through provision of targeted training programs.

In addition to law enforcement, the cybersecurity training initiative did target IT professionals working in both the public and private sectors. This was because cybersecurity is not only a government concern but also a business imperative. Organizations, particularly financial institutions, telecommunications companies, and e-commerce platforms, are prime targets for cybercriminals. The policy thus advocated for training programs that enhance the capacity of IT teams to implement robust security measures, conduct risk assessments, and develop incident response strategies.

Despite the Kenyan government's recognition of cybersecurity threats and its efforts to mitigate them through the cybersecurity training policy initiative, there had been a notable lack of empirical studies assessing the impact of these interventions. While the National ICT Policy underscored the importance of cybersecurity training in building capacity of officers working in the cybercrime prevention institutions, little research had been conducted to evaluate the effectiveness of cybersecurity training. The absence of comprehensive studies on this subject had made it difficult to determine whether the training initiative had significantly improved the ability of cybersecurity professionals to prevent, detect, and respond to cyber threats in Kenya. Without systematic evaluation, it remained unclear whether the policy had led to measurable improvements in cyber-crime prevention, incident response times, inter-agency coordination, and the adoption of best practices within organizations. This research gap highlighted the need for an in-depth analysis of the extent to which the cybersecurity training initiative had enhanced Kenya's cyber resilience, particularly in the face of increasingly sophisticated cyber threats.

Moreover, the lack of empirical data on the cybersecurity training policy initiative raised concerns about its practical implementation and long-term sustainability. While government agencies such as the Communications Authority of Kenya (CA) and the Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC) had reported rising cyber incidents and the importance of cybersecurity preparedness, there was limited documentation on the actual outcomes of the training programs. This article therefore argues that while cybersecurity training has enhanced officers' digital skills and contributed to improved cybercrime prevention in Kenya, significant gaps remained in the consistency, relevance, and institutional sup-port for such training.

2. Theoretical Framework

Rational Choice Theory (RCT), originating from Adam Smith in 1776, provides a suitable framework for analyzing the im-pact of cybersecurity training policy initiatives on cybercrime prevention in Kenya. The theory posits that policy decisions are made after a thorough evaluation of their costs, benefits, and potential risks, ensuring that the selected option yields the highest societal gains [23]. RCT operates on several core assumptions: first, that individuals whether policy-makers or actors within a system are rational agents who seek to maximize utility while minimizing cost; second, that these agents possess sufficient information to make informed choices; and third, that preferences remain stable and consistent over time. These assumptions suggest that governments or institutions will support cybersecurity training policies only if the perceived bene-fits (e.g., reduced cybercrime, increased security, and national resilience) outweigh the investment costs.

RCT has been applied in diverse contexts of crime prevention and policy evaluation. For instance, in the United States, it was used to explain the effectiveness of deterrence-based policies in reducing economic crimes [20]. Similarly, [30] employed the theory to analyze offender decision-making, showing how perceived risks and consequences influence compliance. In a digital context, [29] utilized RCT to explore how cyber offenders weigh the likelihood of detection and punishment before en-gaging in online criminal behavior. These studies demonstrate how RCT can be operationalized to understand both institutional decision-making and individual behavioral patterns in crime prevention.

According to RCT, an optimal policy should ensure sustained and maximized benefits; hence, addressing these gaps is crucial for enhancing the effectiveness of cybersecurity training [15]. In the case of cybersecurity training policy in Kenya, the government's decision to integrate it into the National ICT Policy was based on a rational assessment of its necessity in mitigating cyber threats. The policy aimed to enhance the digital expertise and practical skills of law enforcement officers and IT professionals, ensuring they could effectively detect, prevent, and respond to cyber threats such as ransomware, phishing, and data breaches. The article argues that cybersecurity training can significantly improve officers' ability to handle cyber incidents by reducing the Mean Time to Detect and Respond (MTTDR) and the Mean Time to Investigate and Resolve (MTTIR). Through equipping officers with advanced cybersecurity skills, the training can strengthen cybercrime prevention efforts, aligning with RCT's principle of maximizing benefits for society. Similarly, a culture of continuous learning can ensure that officers remain well-prepared to tackle emerging cyber threats, thereby reinforcing the overall effectiveness of cybercrime prevention initiatives. The structured and consistent implementation of cybersecurity training aligns with Rational Choice Theory, as it seeks to optimize the benefits derived from policy initiatives, ultimately securing a safer digital environment for economic and social progress.

3. Research Design and Methodology

The article employed a descriptive research design. A sequential explanatory mixed-methods approach, incorporating both quantitative and qualitative data, was utilized to achieve the article's objectives. The choice of mixed methods was based on the need to gather statistical data through questionnaires and textual insights via Key Informant Interviews. Primary quantitative data were collected from seventy-two (72) officers working in cybercrime prevention institutions and telecommunications companies in Kenya. Additionally, qualitative data were obtained through open-ended questions and interviews with eleven (11) Key Informants. These informants included department heads from key agencies such as the Cyber Crime Unit-Investigation (CCU-I), the Digital Forensic Laboratory of Kenya (DFLK), the Ministry of ICT, the Anti-Counterfeit Unit (ACU), the Communications Authority of Kenya (CAK), the Central Bank of Kenya's Cybercrime Prevention Unit (CBK-CPU), the National Intelligence Service's Cyber Security Unit (NIS-CSU), the Kenya Computer Incident Response Team and Coordination Centre (KE-CIRT/CC), the National Cyber Command Centre (NC3), as well as representatives from Safaricom and Airtel. Table 1 shows the number of officers selected in each institution.

Table 1. *Respondent's Working Institution.*

		Frequency	Percent
Valid	CCU-I	14	19.4
	DFLK	4	5.6
	ACU	6	8.3
	CAK	5	6.9
	NIS-CSU	4	5.6
	KE-CIRT/CC	11	15.3
	NC3	13	18.1
	Ministry of ICT	5	6.9
	CBK	4	5.6
	Safaricom	4	5.6
	Airtel	2	2.8
	Total	72	100.0

This section presents an in-depth analysis of the impact of cybersecurity training on cybercrime prevention across selected institutions in Kenya. These institutions included the Cyber Crime Unit-Investigation (CCU-I), the Digital Forensic

Laboratory of Kenya (DFLK), the Ministry of ICT, the Anti-Counterfeit Unit (ACU), the Communications Authority of Kenya (CAK), the Central Bank of Kenya’s Cybercrime Prevention Unit (CBK-CPU), the National Intelligence Service’s Cyber Security Unit (NIS-CSU), the Kenya Computer Incident Response Team and Coordination Centre (KE-CIRT/CC), the National Cyber Command Centre (NC3), as well as representatives from Safaricom and Airtel. These organizations were purposefully selected due to their strategic roles in detecting, investigating, prosecuting, and adjudicating cybercrime-related offenses in Kenya. The respondents included officers/ cybersecurity professionals working in government, regulatory, law enforcement, intelligence, and telecommunications institutions and actively engaged in combating cybercrime in the above institutions.

The analysis of quantitative data collected through survey questionnaires was conducted using the Statistical Package for Social Sciences (SPSS) version 26. Univariate analysis, incorporating descriptive statistics, was performed, and the findings were presented in tables. Additionally, simple linear regression was applied to test the hypothesis. The use of use of regression analysis was justified by its ability to examine the impact of the policy on cybercrime prevention from the perspective of officers working in Kenya’s cybercrime prevention institutions. The article tested the hypothesis that, “Cybersecurity training had not played a role in preventing cybercrime by enhancing officers’ digital expertise and skills.”

Qualitative data collected through key informant interviews was analyzed thematically. It began with familiarization, where the researcher read through the qualitative data multiple times to gain a comprehensive understanding and noted initial im-pressions. This was followed by coding, in which meaningful segments of the data were systematically identified and labeled based on their relevance to the research objective. After coding, the researcher generated themes by grouping similar codes that reflected broader patterns or significant ideas within the dataset. The next step involved reviewing these themes to ensure they were coherent, internally consistent, and accurately represented both the coded extracts and the dataset as a whole. Once refined, each theme was clearly defined and named to capture its essence and ensure clarity. Finally, the researcher wrote the report by weaving together the themes into a coherent narrative, incorporating supporting quotes from the data, and linking the findings to the research objective. This process simply followed [5] framework which entails a six-phase process: familiarization with data, generating initial codes, searching for themes, reviewing themes, defining and naming themes, and producing the final report.

4. Results/Data Analysis

Data analysis was based on testing the hypothesis that cybersecurity training had not played a role in preventing cybercrime by enhancing officers’ digital expertise and skills. This analysis sought to determine the impact of cybersecurity training pol-icy initiatives on cybercrime prevention in Kenya, focusing on the extent to which training interventions had contributed to building technical capacity among officers. A simple linear regression model was employed to test the significance of the relationship between cybersecurity training and cybercrime prevention. This approach enabled a quantitative evaluation of whether increased training efforts had translated into improved cybercrime prevention outcomes, as aligned with the broader policy objective of enhancing national cybersecurity readiness.

To test the hypothesis that cybersecurity training had not played a role in preventing cybercrime by enhancing officers’ digital expertise and skills, respondents were asked to indicate their level of agreement with a set of statements reflecting key dimensions of effective cybersecurity training. These included whether the cybersecurity training provided by their institution was of high quality and equipped staff with practical skills to prevent cybercrime effectively; whether the institution offered training frequently enough to keep staff updated on emerging cyber threats and prevention strategies; and whether the delivery methods used such as in-person sessions, online modules, and simulations enhanced understanding and application of cybercrime prevention techniques. Additionally, respondents assessed whether the content of the training was tailored to ad-dress real-world cybercrime challenges relevant to their job responsibilities, whether their institution provided adequate sup-port mechanisms (such as policy backing, resources, and time allocation) to implement training outcomes effectively, and whether regular evaluations and feedback were used to improve future training sessions. These questions formed the basis for analyzing the impact of cybersecurity training on cybercrime prevention.

In examining the relationship between cybersecurity training and cybercrime prevention, simple linear regression analysis, a robust statistical tool for hypothesis testing was utilized. In this context, the aggregates of statements reflecting key dimensions of effective training (cybersecurity training) served as the independent variable (IV), while cybercrime prevention functioned as the dependent variable (DV). The two variables were afterwards regressed through simple linear regression and the outcomes presented in the successive tables below.

Null Hypothesis (H_0): Cybersecurity training has not played a role in preventing cybercrime by enhancing officers’ digital expertise and skills.

4.1. The Model Summary Table

The Model Summary Table gives a snapshot of how well the independent variable i.e. cybersecurity training (CT) predicts the dependent variable i.e. cybercrime prevention (CP). It includes key metrics such as the correlation coefficient (R), the coefficient of determination (R^2), Adjusted R^2, Standard

Error of the Estimate, and the significance of the model (Sig. F Change). In Table 2, the R value was 0.891, showing a strong positive relationship between cybersecurity training and cybercrime prevention. The R ^{2}value was 0.794, meaning that about 79.4% of the variation in cybercrime prevention could be explained by cybersecurity training. The Adjusted R ^{2}, which accounts for the number of predictors in the model, was 0.791 supporting the reliability of the results. The small standard error suggested that the model closely matched the actual data. The significance value (Sig. F Change = 0.000) confirmed that the model was statistically valid. Overall, the results demonstrate that cybersecurity training plays a key role in improving cybercrime prevention.

Table 2. Model Summary Table.

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.891[a]	.794	.791	.67723	.794	269.526	1	70	.000

a. Predictors: (Constant), ct

b. Dependent Variable: cp

4.2. The ANOVA Table

The ANOVA (Analysis of Variance) table was used to assess whether the overall regression model was statistically significant specifically, whether cybersecurity training (CT) predicted cybercrime prevention (CP). It partitioned the total variation in CP into two parts: the variation explained by the model (Regression) and the unexplained variation (Residual/Error). Key elements in the table included the Sum of Squares, Degrees of Freedom, Mean Squares, F-value, and its corresponding p-value. A p-value below 0.05 indicated that the model significantly improved prediction compared to a model with no predictors. As shown in Table 3, the Sum of Squares for Regression (123.614) reflected the variation in CP explained by CT, while the Residual Sum of Squares (32.105) represented unexplained variation. The p-value (0.000) confirmed that the model was statistically significant at the 0.05 level. Therefore, the results supported the conclusion that cybersecurity training had a significant effect on cybercrime prevention. The null hypothesis stating that cybersecurity training had no impact was rejected, confirming that such training contributed to enhancing officers' digital skills and reducing cybercrime.

Table 3. ANOVA Table.

ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	123.614	1	123.614	269.526	.000[b]
	Residual	32.105	70	.459		
	Total	155.719	71			

a. Dependent Variable: cp

b. Predictors: (Constant), ct

4.3. The Coefficients Table

The Coefficients Table in regression analysis was used to provide a detailed information about the individual predictors (in-dependent variables) and their specific contribution to the dependent variable. It was used to show the unstandardized coefficients (B), which indicated the expected change in the dependent variable for a one-unit change in the predictor. The table also included the standard error, t-values, and p-values, which tested whether each coefficient was statistically significant. A p-value less than 0.05 typically indicated that the predictor had a meaningful effect on the outcome variable.

Table 4 below on Coefficients Table therefore presented the estimated values for the regression model, assessing the impact of cybersecurity training (CT) on cybercrime prevention (CP). The coefficient for cybersecurity training was statistically significant ($p < 0.05$) with a high standardized Beta value of 0.891, signifying a strong positive relationship between the two variables. This meant that an increase of one unit in cybersecurity training was associated with a predicted increase of 1.481 units in cybercrime prevention.

Table 4. CoefficientsTable.

Coefficients[a]									
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations		
		B	Std. Error	Beta			Zero-order	Partial	Part
1	(Constant)	-2.312	.330		-7.016	.000			
	Ct	1.481	.090	.891	16.417	.000	.891	.891	.891

a. Dependent Variable: cp

The findings showed that cybersecurity training played a significant role in enhancing officers' digital expertise and skills, which in turn contributed to stronger cybercrime prevention efforts. Based on the evidence, the article confirmed that well-structured training initiatives were crucial in supporting the fight against cyber threats.

This analysis builds on the tested hypothesis by examining how various dimensions of cybersecurity training influenced its effectiveness across institutions. It moves beyond identifying statistical associations to explore how different government and security-sector agencies implemented training programs and what set successful efforts apart. Key areas of focus included training quality, frequency, delivery methods, content relevance, evaluation and feedback mechanisms, and institutional support. Institutional performance was assessed through a comparative analysis using aggregated mean scores, offering a clear view of the extent and impact of training initiatives. Qualitative insights from institutional heads provided critical context, highlighting underlying motivations, structural challenges, and real-world implementation dynamics.

To gauge the effectiveness of these training dimensions, respondents from government, regulatory, law enforcement, intelligence, and telecommunications institutions rated their level of agreement with specific statements under the six thematic areas. The results, presented in Table 5, enabled a cross-institutional comparison that identified both strong practices and gaps. This analysis informs evidence-based recommendations by illustrating how institutional policy, infrastructure, and commitment shape the success of cybersecurity training in combating cybercrime.

Table 5. Ranking the Impact of CT Dimensions per Institution by Mean Scores.

Respondent's working institution		Minimum	Maximum	Mean	Std. Deviation
CBK	Ct	2.33	4.67	3.7262	.88096
	Cp	1.25	5.00	3.1607	1.55541
	Valid N (listwise)				

Respondent's working institution		Minimum	Maximum	Mean	Std. Deviation
NC3	Ct	2.33	4.33	3.3750	.94648
	Cp	1.75	5.00	3.5000	1.74404
	Valid N (listwise)				
NIS-CSU	Ct	2.67	4.67	4.2500	.77996
	Cp	2.00	5.00	3.8750	1.02164
	Valid N (listwise)				
ACU	Ct	2.33	3.00	2.8000	.27386
	Cp	1.25	1.75	1.4000	.22361
	Valid N (listwise)				
DFLK	Ct	2.33	4.33	3.3750	.94648
	Cp	1.75	5.00	3.2500	1.51383
	Valid N (listwise)				
KE-CIRT/CC	Ct	2.33	4.67	3.7121	.95479
	Cp	1.25	5.00	3.0455	1.58831
	Valid N (listwise)				
Safaricom	Ct	2.33	4.67	3.6795	.89872
	Cp	1.25	5.00	3.2115	1.47848
	Valid N (listwise)				
Ministry of ICT	Ct	2.33	3.00	2.6667	.31180
	Cp	1.25	1.75	1.3500	.22361
	Valid N (listwise)				
CCU-I	Ct	2.67	4.67	4.1250	.97539
	Cp	2.00	4.50	3.6250	1.10868
	Valid N (listwise)				
CAK	Ct	2.33	3.00	2.7917	.31549
	Cp	1.25	2.25	1.6875	.42696
	Valid N (listwise)				
Airtel	Ct	2.83	4.00	3.4167	.82496
	Cp	1.75	5.00	3.3750	2.29810
	Valid N (listwise)				

Table 5 presents an institutional analysis of how different government, regulatory, and security-sector institutions in Kenya structured, delivered, and integrated cybersecurity training (CT) into their operations, based on mean scores reported by cybersecurity professionals. The table ranks eleven institutions according to the perceived effectiveness of their training programs in enhancing cybercrime prevention (CP).

The National Intelligence Service's Cyber Security Unit (NIS-CSU) ranked highest with a mean score of 4.25, indicating deeply embedded training practices tailored to organizational security needs. The high rating suggests practical, frequent, and role-specific training integrated into real-time operations and supported by strong leadership. Close behind was the Cyber Crime Unit – Investigation (CCU-I), scoring 4.125. Respondents highlighted this agency's emphasis on post-training evaluations, tailored modules, and operational follow-up ensuring knowledge gained translates directly into action. In third place, the Central Bank of Kenya's Cybercrime Prevention Unit (CBK-CPU) registered a score of 3.7262. Training here was supported by infrastructure such as security operation centers (SOCs), with a strong emphasis on scenario-based learning and quarterly refresher courses. Institutions like KE-CIRT/CC and Safaricom, with mean scores of 3.7121 and 3.6795 respectively, showed moderately effective training frameworks. However, gaps emerged in translating acquired knowledge into preventive action especially where hands-on application lagged. Mid-ranking institutions, including Airtel (3.4167), DFLK (3.3750), and National Cyber Command Centre (3.3750), demonstrated modest outcomes. Their training programs, while present, lacked the consistency and operational integration observed in top-performing institutions. At the lower end, the Anti-Counterfeit Unit (2.8000), Communications Authority of Kenya (2.7917), and Ministry of ICT (2.6667) reflected limited training effectiveness. These scores point to irregular training schedules, outdated content, poor institutional support, and a lack of structured feedback mechanisms. In many cases, cybercrime prevention was constrained by systemic underinvestment and the absence of clear long-term strategies.

Key Insights (Summary Bullets):

1) Top performers (NIS-CSU and CCU-I) integrate cybersecurity training into core operations with strong institutional backing.
2) CBK-CPU and KE-CIRT/CC demonstrate consistent training practices supported by infrastructure and refresher mechanisms.
3) Mid-tier institutions show moderate impact due to uneven training delivery and weaker operational integration.
4) Bottom-tier institutions face systemic challenges such as infrequent, outdated training, and limited follow-up leading to poor cybercrime prevention performance.
5) Overall trend: Training effectiveness varies significantly across institutions depending on leadership commitment, training relevance, delivery frequency, and post-training integration into daily tasks.

Given these observed variations, it became necessary to explore the underlying reasons behind them. This led to asking the respondents this central question: Why were there variations in the impact of cybersecurity training on cybercrime prevention across various institutions in Kenya? The responses were analyzed using descriptive statistics, particularly mean scores, to reflect the perceived reasons for variations in the impact of cybersecurity training dimensions across the institutions. The mean scores were derived from analysis of data from the officers across eleven cybercrime prevention institutions in Kenya. The scores (ranging from 1 = Strongly Disagree to 5 = Strongly Agree) reflected perceptions of institutional strength in six thematic areas: leadership commitment, budgetary support, technological infrastructure, training frequency, trainer expertise, and collaboration culture. The perceived variations, identified through descriptive statistical analysis of mean scores, were further supported by qualitative data obtained from key informant interviews (11 heads of departments in the cybercrime prevention institutions). These interviews provided deeper insights into the identified contextual factors thereby reinforcing and enriching the interpretation of the quantitative findings. The analysis of the responses is as shown in Table 6 below.

Table 6. *Descriptive Statistics on Reasons for Variations.*

Institution	Leadership Commitment	Budgetary Support	Technological Infrastructure	Training Frequency	Trainer Expertise	Collaboration Culture
NIS-CSU	4.37	4.95	4.73	4.60	4.16	4.16
CCU-I	4.06	4.87	4.60	4.71	4.02	4.97
CBK-CPU	4.83	4.21	4.18	4.18	4.30	4.52
KE-CIRT/CC	4.43	4.29	4.61	4.14	4.29	4.37
Safaricom	3.46	3.79	3.20	3.51	3.59	3.05
Airtel	3.61	3.17	3.07	3.95	3.97	3.81
DFLK	3.30	3.10	3.68	3.44	3.12	3.50
NCCC	3.03	3.91	3.26	3.66	3.31	3.52
ACU	2.55	2.18	2.97	2.78	2.94	2.89
CAK	2.60	2.92	2.09	2.20	2.05	2.33
Ministry of ICT	2.39	2.27	2.83	2.36	2.28	2.54

Table 6 presents a detailed comparative analysis of institutional-level factors such as leadership commitment, budgetary support, infrastructure, training frequency, trainer expertise, and collaboration culture that influenced the effectiveness of cybersecurity training across selected organizations in Kenya.

The National Intelligence Service – Cyber Security Unit (NIS-CSU) led with consistently high scores across all dimensions, including leadership commitment (4.37), budget (4.95), infrastructure (4.73), and training frequency (4.60). These scores indicated strong executive prioritization, robust funding, and a culture of continuous, applied training. Respondents confirmed that cybersecurity training is viewed as a strategic imperative within the agency.

The Cyber Crime Unit – Investigation (CCU-I) followed closely, particularly excelling in training frequency (4.71) and collaboration (4.97), reflecting structured engagement with both domestic and international actors. Strong support in budget (4.87), infrastructure (4.60), and trainer expertise (4.02) pointed to a high-quality and operationalized training system.

The Central Bank of Kenya – Cybercrime Prevention Unit (CBK-CPU) performed well in leadership commitment (4.83) and trainer expertise (4.30). Although budget (4.21) and infrastructure (4.18) were slightly lower, the unit's quarterly training model, aligned with organizational risk assessments, reinforced its strategic approach.

KE-CIRT/CC also showed institutional strength, especially in infrastructure (4.61), leadership (4.43), and collaboration (4.37). Trainer expertise (4.29) and frequency (4.14) reflected a data-driven, real-time training model focused on responsiveness to evolving threats.

Moderate performers such as Safaricom and Airtel posted mean scores between 3.0 and 3.9 across most dimensions. While both demonstrated some investment in training infrastructure and expertise, weaker leadership commitment and inconsistent collaboration limited their impact. Safaricom scored especially low on collaboration culture (3.05), and Airtel struggled with budget (3.17) and infrastructure (3.07).

DFLK and NCCC had mixed results. DFLK showed promise in infrastructure (3.68) and trainer expertise (3.12), but modest scores in leadership (3.30) and budget (3.10) limited training continuity. NCCC, despite decent budget support (3.91), suffered from low leadership commitment (3.03) and weak collaboration (3.52), indicating bureaucratic inertia.

At the lowest tier, the Anti-Counterfeit Unit (ACU), Communications Authority of Kenya (CAK), and Ministry of ICT exhibited serious institutional deficiencies. ACU's scores were all below 3.0, with particularly weak budget (2.18) and leadership (2.55). CAK's performance was hampered by outdated infrastructure (2.09), minimal internal training efforts, and overreliance on external partners. The Ministry of ICT had the lowest scores across all categories: leadership (2.39), budget (2.27), and training frequency (2.36) signaling poor prioritization and planning.

Key Insights (Summary Bullets):

1) High-performing institutions (e.g., NIS-CSU, CCU-I) exhibited strong leadership, consistent budgetary support, and training frequency, resulting in effective, integrated cybersecurity training.
2) CBK-CPU and KE-CIRT/CC had structured training strategies supported by infrastructure, skilled trainers, and risk-aligned learning models.
3) Mid-tier institutions (e.g., Safaricom, Airtel, DFLK) showed sporadic investment and partial commitment, with training efforts diluted by weak strategic alignment and limited collaboration.
4) Bottom-tier organizations (ACU, CAK, Ministry of ICT) faced systemic challenges: underfunding, lack of leadership support, and fragmented implementation leading to minimal impact from cybersecurity training.
5) Overall Conclusion: The effectiveness of cybersecurity training is directly tied to institutional prioritization, investment, and organizational integration. Strong systems outperform ad hoc or externally dependent models.

Building on the finding that institutional-level factors significantly influenced the effectiveness of cybersecurity training, it became apparent that the presence or absence of enabling conditions within organizations played a critical role in shaping training outcomes. As the analysis highlighted the stark contrasts between institutions that reaped substantial benefits and those that did not, questions naturally arose regarding the specific barriers hindering progress in less effective agencies. This prompted a deeper investigation into the challenges facing cybersecurity training initiatives across the various institutions. Understanding these obstacles was essential not only for explaining the observed disparities in training impact, but also for identifying systemic weaknesses that must be addressed to enhance future training programs and ensure more consistent national outcomes in cybercrime prevention.

In lieu of this, the respondents were asked, "what are the challenges that faced cybersecurity trainings in cybercrime prevention institutions in Kenya?" The responses were analyzed using descriptive statistics, particularly mean scores, to reflect the perceived challenges affecting cybersecurity training across the institutions. The mean scores were derived from analysis of data from the officers across eleven cybercrime prevention institutions in Kenya. The scores (ranging from 1 = Strongly Disagree to 5 = Strongly Agree) reflected perceptions of challenges in eight thematic areas: irregular training schedules, punitive training approaches, generic content & lack of customization, inadequate budgetary support, lack of training infrastructure, monotonous delivery, no pre/post training evaluation and poor inter-agency coordination. The perceived challenges, identified through descriptive statistical analysis of mean scores, were further supported by qualitative data obtained from key in-formant interviews (11 heads of departments in the cybercrime prevention institutions). The analysis of the responses was as shown in table 7 below.

Table 7. Descriptive Statistics on Challenges Affecting Cybersecurity Training.

Institution	Irregular Training Schedules	Punitive Training Approaches	Generic Content & Lack of Customization	Inadequate Budgetary Support	Lack of Training Infrastructure	Monotonous Delivery	No Pre/Post Training Evaluation	Poor Inter-Agency Coordination
Ministry of ICT	3.11	4.72	2.89	4.66	2.80	4.59	2.48	2.30
CAK	4.67	4.35	3.09	4.71	3.89	2.34	4.27	3.07
ACU	4.08	2.67	3.33	4.28	2.94	2.63	2.30	2.41
NIS-CSU	3.72	2.59	4.22	2.92	3.50	2.22	4.76	4.43
CCU-I	2.52	2.60	2.64	2.36	3.58	2.98	4.19	3.78
KE-CIRT/CC	2.52	2.92	3.49	3.95	2.60	3.15	2.64	2.99
CBK-CPU	2.26	3.52	3.70	3.29	4.72	2.83	2.11	2.27
Safaricom	4.44	3.27	2.23	2.43	4.19	4.34	4.30	2.94
Airtel	3.72	2.89	3.74	3.44	4.64	3.06	4.01	2.98
DFLK	4.01	3.75	2.56	2.19	4.52	2.86	4.07	4.07
NCCC	2.16	2.48	2.28	4.56	3.71	3.57	4.18	3.82

The Ministry of ICT showed deep dissatisfaction with punitive training approaches (mean = 4.72) and monotonous delivery methods (4.59), reflecting a heavy reliance on fear-based models that demotivate learners. A respondent stated, “Most of our training feels like punishment instead of empowerment.” The Ministry also rated budgetary support as highly inadequate (4.66), though showed relatively low concern about inter-agency coordination (2.30) and training evaluations (2.48), indicating these are not priority concerns internally.

The Communications Authority of Kenya (CAK) registered high concern over irregular training schedules (4.67) and budget inadequacies (4.71), with reports of frequent cancellations due to lack of funds. Pre/post-evaluation was also a significant gap (4.27). Interestingly, CAK rated monotonous delivery methods lower (2.34), suggesting more engaging training delivery compared to peers.

The Anti-Counterfeit Unit (ACU) struggled with irregular training (4.08) and budget issues (4.28), which caused scheduling uncertainties. However, punitive methods (2.67) and infrastructure challenges (2.94) were not viewed as severe. The unit rated evaluation mechanisms (2.30) and coordination (2.41) among the lowest, suggesting limited strategic reflection.

At the top tier, NIS-CSU flagged major challenges in content customization (4.22), evaluation (4.76), and inter-agency coordination (4.43), reflecting its awareness of deeper technical and structural shortcomings. Budget was not a key issue (2.92), but delivery style was criticized as outdated (2.22), with one noting, “The delivery style feels outdated and uninspiring.”

The Cyber Crime Unit – Investigation (CCU-I) showed minimal concern about punitive methods (2.60) or irregular schedules (2.52), but emphasized serious gaps in evaluation (4.19) and coordination (3.78). Engagement and infrastructure were viewed as moderately problematic.

KE-CIRT/CC reflected moderate concern with content relevance (3.49), budgetary limitations (3.95), and delivery quality (3.15). Trainers mentioned outdated modules that failed to reflect current cyber threats. Evaluation (2.64) was not a major concern, though coordination (2.99) was more pressing.

CBK-CPU stood out for its critical lack of infrastructure (4.72), citing insufficient practical tools like simulation labs. Concerns with punitive methods (3.52) and content (3.70) were moderate, while evaluation (2.11) and coordination (2.27) were ranked low in concern.

Safaricom reported significant issues with irregular training (4.44), monotonous delivery (4.34), and lack of evaluation (4.30), indicating inconsistent and uninspiring training cycles. Budget (2.43) and content customization (2.23) were not viewed as major problems.

Airtel identified infrastructure (4.64) and content (3.74) as major concerns, with additional dissatisfaction in evaluation (4.01), training delivery (3.06), and budget (3.44). A respondent emphasized the need for more interactive formats. Punitive methods (2.89) were not viewed as problematic.

DFLK cited issues with irregular training (4.01), infrastructure (4.52), and punitive methods (3.75), painting a picture of operational inefficiency. High concern was also expressed for evaluation (4.07) and inter-agency coordination (4.07), revealing a siloed and under-supported training system.

Lastly, the NCCC rated budget (4.56) and infrastructure (3.71) as critical challenges. Although irregular training (2.16), punitive approaches (2.48), and content customization (2.28) were rated as lesser concerns, evaluation (4.18) and coordination (3.82) were flagged as needing significant improvement.

Key Insights (Summary Bullets)

1) Ministry of ICT, CAK, and ACU face entrenched issues in budgetary support and irregular training, with Ministry of ICT particularly burdened by punitive methods and uninspiring delivery.
2) Top-tier agencies like NIS-CSU and CCU-I reveal advanced introspection, identifying technical gaps such as content irrelevance, lack of evaluation, and coordination weaknesses indicating room for strategic refinement despite strong funding.
3) CBK-CPU and DFLK highlight acute infrastructure deficits, limiting hands-on, applied training particularly in institutions otherwise equipped with technical knowledge.
4) Private sector actors (Safaricom and Airtel) exhibit inconsistencies in training regularity, delivery quality, and content dynamism, with Airtel also reporting infrastructural shortcomings.
5) Coordination and evaluation gaps are recurrent across institutions, reflecting a systemic lack of integrated frameworks and feedback mechanisms for cybersecurity capacity-building.
6) Budgetary constraints remain a top obstacle, especially in public-sector agencies, directly affecting scheduling, trainer quality, and content updating.
7) Punitive training models and outdated delivery styles persist in multiple institutions, reducing motivation and lowering learning outcomes especially within Ministry of ICT and DFLK.
8) Conclusion: Effective cybersecurity training requires more than just financial support; it demands strategic content customization, dynamic delivery, infrastructure enhancement, inter-agency synergy, and continuous evaluation to ensure adaptive resilience.

Whilst exploring the challenges, it became evident that cybersecurity training on its own regardless of how regularly it is implemented or not cannot fully account for its effectiveness in preventing cybercrime. This realization prompted a deeper inquiry into the broader ecosystem within which cybersecurity training takes place. As a result, respondents were asked to identify the specific contextual elements that influence the success or limitations of cybersecurity training efforts in Kenya through the question, “What were these contextual factors influencing the impact of cybersecurity training in Kenya?” The responses were analyzed using descriptive statistics, particularly mean scores, to reflect the perceived contextual factors in which the impact of cybersecurity training was dependent. The mean scores were derived from analysis of data from the officers across eleven cybercrime prevention institutions in Kenya. The scores (ranging from 1 = Strongly Disagree to 5 = Strongly Agree) reflected perceptions of challenges in six thematic areas: the type of training approach used, the level of staff engagement, the degree to which training is customized to specific roles, availability of funding, dependence on training as a sole intervention, and the presence of effective evaluation and feedback mechanisms. The perceived contextual factors, identified through descriptive statistical analysis of mean scores, were further supported by qualitative data obtained from key informant interviews (11 heads of departments in the cybercrime prevention institutions). The analysis of the responses was as shown in table 8 below.

Table 8. Contextual Factors Influencing the Impact of Cybersecurity Training.

Institution	Type of Training Approach	Customization to specific roles	Funding	Engagement	Evaluation and Feedback	Training Reliance
NIS-CSU	4.5	4.3	4.7	4.4	4.4	4.2
CCU-I	4.3	4.7	4.6	4.1	4.5	4.3
CBK-CPU	4.1	4.4	4.5	3.9	4.2	4.1
KE-CIRT/CC	4.2	4.4	4.9	3.8	4.3	4.2
Safaricom	4.0	4.2	4.3	3.7	4.0	4.0
Airtel	4.1	4.1	4.2	3.9	4.1	4.0
DFLK	4.3	4.5	4.4	4.0	4.3	4.2
NCCC	4.2	4.6	4.5	4.1	4.2	4.3

Institution	Type of Training Approach	Customization to specific roles	Funding	Engagement	Evaluation and Feedback	Training Reliance
ACU	4.4	4.5	4.6	4.0	4.3	4.3
CAK	4.1	4.3	4.4	4.0	4.8	4.1
Ministry of ICT	4.3	4.6	4.5	4.1	4.4	4.3

Funding emerged as the top contextual factor, receiving the highest scores overall, with KE-CIRT/CC scoring it at 4.9, the strongest agreement. This aligned with their observation that "Limited budgets mean we often have to make do with outdated tools and insufficient training, which hampers our ability to combat cyber threats effectively." Institutions like NCC3 and ACU also ranked funding issues very high, reinforcing this shared concern.

Customization to department-specific threats was also strongly acknowledged. CCU-I (4.7) and Ministry of ICT (4.6) recognized that training must be tailored to be effective. As ACU noted, "Generic training sessions fail to address the unique challenges we face in our department, making it hard to apply the lessons in our daily operations." Similarly, the CBK-CPU and NCCC echoed the necessity of aligning training with actual threats and duties.

Evaluation mechanisms received the highest individual score from CAK (4.8), with support across the board. This supports CAK’s insight: "Without assessing our team's competencies before and after training, we can't truly measure its impact or identify areas needing improvement." Most institutions scored this issue above 4.0, showing strong agreement that post-training assessments are critical for continuous improvement.

Type of training approach was also viewed negatively, with NIS-CSU scoring it at 4.5, reinforcing the sentiment that such measures breed fear. As one officer noted, "Punitive measures for example create an environment of fear, causing staff to avoid reporting mistakes and, in some cases, to bypass security protocols altogether." There was a general consensus that this adversarial environment stifled transparency and learning.

Engagement in training delivery were noted but received slightly lower averages than other factors, particularly by Safaricom (3.7) and KE-CIRT/CC (3.8). However, even these institutions acknowledged its relevance, with NIS-CSU stating, "Training sessions that are purely lecture-based without interactive elements tend to lose our attention."

Finally, reliance on training alone (without considering structural or behavioral change components) was consistently flagged across institutions, with most scoring it at or above 4.0. As highlighted in the article, effective cybersecurity required more than repeated sessions, it demanded a thoughtful strategy that integrated training with organizational processes and culture.

The findings revealed that across all 11 institutions, cybersecurity training alone, regardless of its frequent practice/implementation, was insufficient to prevent cybercrime unless it was shaped by key contextual factors. Funding was identified as the most critical constraint, followed closely by the need for role-specific customization and robust evaluation mechanisms. The use of punitive approaches undermined learning, while engagement through interactive methods and reducing over-reliance on training alone were necessary for impact. Ultimately, the training’s effectiveness hinged on how well these factors were integrated into organizational strategies.

5. Discussion of Findings

The findings of the current article align with and reinforce the conclusions drawn by several scholars in the field of cybersecurity capacity building. Consistent with the work of [4], who emphasized that cybersecurity training significantly enhances the operational readiness of personnel, this article confirms that such training is instrumental in improving officers’ digital competencies, thereby strengthening cybercrime prevention strategies. Similarly, [24] highlighted the role of context-specific and role-tailored training programs in fostering a proactive cybersecurity culture within institutions, an observation echoed in the current research. Moreover, these results correspond with findings by [18], which reported that the effectiveness of national cybersecurity efforts is largely dependent on institutional investment in workforce training and development. However, while most literature concurs on the importance of training, this article extends this by emphasizing not only the frequency, structure and quality of training but also its institutional integration and sustainability. Thus, the article advances existing scholar-ship by demonstrating how well-structured and contextually grounded training programs serve as pivotal tools in combating cybercrime in Kenya.

The findings of the current article, which reveal significant institutional variations in the impact of cybersecurity training on cybercrime prevention, diverge from the prevailing consensus in existing literature that tends to present cybersecurity training as uniformly effective across sectors. For instance, scholars such as [21] have argued that structured training programs consistently lead to improved cyber resilience, regardless of organizational context. However, the present article challenges this generalized assumption by demonstrating that training effectiveness is not homogenous, but rather contingent on a range of institutional factors such as leadership commitment, contextual relevance of training content, and integration of learned skills into operational practices. This contention aligns more closely with the critical perspectives offered by scholars like [11], who emphasized the role of institutional ecosystems in mediating the success of cybersecurity interventions. Therefore, while acknowledging the foundational importance of training, this article argues for a more differentiated and context-sensitive approach, suggesting that institutional readiness and resource allocation among others are decisive in determining training outcomes.

The current article's findings highlighting inadequate funding, poor infrastructure, generic training content, and weak evaluation mechanisms as persistent challenges to cybersecurity training stand in partial contention with previous literature that presents a more optimistic view of training efficacy. For example, [8] argue that cybersecurity training, when institutionalized, leads to improved threat readiness across sectors, often overlooking the granular challenges faced by individual organizations. Similarly, [2] emphasize the transformative potential of awareness programs, but they understate the importance of organizational readiness, customization, and evaluation structures that this article finds to be critical. By contrast, the current article aligns more closely with the critiques raised by [27], who stress that without context-specific design and institutional commitment, training efforts risk becoming ceremonial rather than functional. Therefore, while the literature broadly supports training as a cornerstone of cyber resilience, this article adds depth by illuminating the structural and procedural deficiencies that undermine impact. These findings suggest that effectiveness hinges not only on training provision but also on the eco-system within which it is implemented.

While foundational works such as [10, 25, 26, 7], and [3] underscore the value of regular and continuous cybersecurity training outlining that cybersecurity training if done continuously will always be effective. They often approach it with the implicit assumption that increased frequency directly correlates with enhanced cyber preparedness. The current article con-tends this perspective by demonstrating that the success of cybersecurity training is highly contingent upon contextual and organizational conditions. In contrast to earlier studies that emphasized frequency and coverage, this work contributes new insights by showing that training whether conducted regularly or not may not always be effective or even productive when implemented in environments characterized by punitive cultures, inadequate funding, disengaging content, or poor alignment with specific job roles. Furthermore, it argues for the necessity of robust evaluation frameworks to measure impact, an area often underdeveloped in previous literature thus enriching ongoing scholarly conversations on cybersecurity capacity-building.

6. Conclusion

This study set out to examine the impact of cybersecurity training policy initiatives on cybercrime prevention in Kenya, with a particular focus on government, regulatory, intelligence, telecommunications, and security-sector institutions. The findings confirmed that cybersecurity training significantly enhanced officers' digital expertise and operational skills, thereby contributing positively to cybercrime prevention. However, the study also revealed that the effectiveness of such training is far from uniform across institutions. Notable variations were observed, largely influenced by institutional-level factors such as leader-ship commitment, sustainable investment, the quality and frequency of training, content relevance, and the extent to which training outcomes were operationalized. Furthermore, critical challenges including inadequate funding, weak infrastructure, generic training content, poor evaluation mechanisms, and inter-agency coordination gaps were found to undermine training outcomes. Importantly, the study concluded that cybersecurity training, while vital, was insufficient on its own to sustainably prevent cybercrime unless embedded within a supportive ecosystem characterized by role-specific customization, interactive delivery, strategic alignment, and adequate resourcing. Thus, a holistic, context-sensitive approach was essential to optimize the impact of training policies on cybercrime prevention in Kenya.

7. Recommendations

In light of the study's findings, several strategic recommendations were proposed to enhance the effectiveness of cybersecurity training as a policy tool for cybercrime prevention in Kenya. First, there was a need for the government and relevant institutions to adopt a system-wide, well-resourced approach to cybersecurity training. This included ensuring adequate and sustained budgetary allocation specifically earmarked for capacity building and training infrastructure. Without sufficient financial support, even well-designed training programs would continue to underperform. Second, institutional leadership had to prioritize cybersecurity training by integrating it into core organizational strategies and aligning it with operational goals. Training programs should not be treated as one-off events but rather as continuous, evolving processes that are embedded into the daily functioning of cybersecurity units. Third, to improve relevance and effectiveness, training content had to be customized to specific roles and functions. A one-size-fits-all approach undermines the impact of training, especially in technical domains like cybersecurity. Tailoring content ensures that officers acquire practical, job-relevant skills needed to counter contemporary cyber threats. Fourth, institutions had to adopt interactive and engaging delivery methods such as simulations, real-time exercises, and scenario-based learning. These methods were more likely to foster skill retention and application compared to traditional didactic sessions. Fifth, monitoring and evaluation mechanisms had to be strengthened. Pre- and post-training assessments, as well as feedback loops, were essential for tracking progress, identifying gaps, and continuously improving training modules. Sixth, the government had to promote cross-agency coordination and knowledge-sharing platforms to harmonize cybersecurity practices, reduce duplication of efforts, and leverage collective institutional expertise. Finally, there had to be a conscious move away from punitive training cultures toward more supportive, learner-centered approaches that fostered trust, openness, and a culture of continuous learning. This shift was critical to ensure that officers engaged fully with training and applied their knowledge constructively.

Abbreviations

ACU	Anti-counterfeit Unit
ANOVA	Analysis of Variance
CAK	The Communications Authority of Kenya
CBK-CPU	Central Bank of Kenya’s Cybercrime Prevention Unit
CCU-I	Cyber Crime Unit-investigation
CP	Cybercrime Prevention
CT	Cybersecurity Training
DFLK	Digital Forensic Laboratory of Kenya
DV	Dependent Variable
ICT	Information and Communication Technology
IV	Independent Variable
KE-CIRT/CC	Kenya Computer Incident Response Team and Coordination Centre
KNBS	Kenya National Bureau of Statistics
MTTDR	Mean Time to Detect and Respond
MTTIR	Mean Time to Investigate and Resolve
NC3	National Cyber Command Centre
NIS-CSU	National Intelligence Service’s Cyber Security Unit
RCT	Rational Choice Theory
SPSS	Statistical Package for Social Sciences

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecuri-ty strategies on the improvement of cybersecurity education. Computers & Security, 119, 102754.

[2] Alruwaili, A. (2019). A Review of the Impact of Training on Cybersecurity Awareness. International Journal of Ad-vanced Research in Computer Science, 10(5).

[3] Alsalamah, A., & Callinan, C. (2021). Adaptation of Kirkpatrick’s four-level model of training criteria to evaluate train-ing programmes for head teachers. Education Sciences, 11(3), 116.

[4] Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspec-tive. Computers & Security, 98, 102003.

[5] Clarke, V., & Braun, V. (2017). Thematic analysis. The journal of positive psychology, 12(3), 297-298.

[6] Communications Authority of Kenya (2023). Cyber Security. Ministry of Information, Communications and the Digital Economy: https://www.ca.go.ke/cyber-security

[7] Deloitte (2014). "Meet the Modern Learner." Retrieved from https://www.bersin.com/contents/meet-the-modern-learner/

[8] Eero, E. & Mei S. (2023). The Effectiveness of Cybersecurity Training Programs in Nigeria. ResearchGate.

[9] Gitari, S. M. (2020). Reforming the institutional and legal frameworks of E-commerce in Kenya; consumer rights pro-tec-tion in the digital economy (Doctoral dissertation, Strathmore University).

[10] Goldstein, I. L., & Ford, J. K. (2002). "Training in Organizations: Needs Assessment, Development, and Evaluation." Wadsworth Publishing.

[11] Gordon, L A; Loeb, M. P & Zhou, L. (2020). "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model". Journal of Cybersecurity.

[12] Government of Kenya (2016). The National ICT Policy-2016. Ministry of Information, Communications and the Digital Economy.

[13] Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., & Koshutanski, H. (2020). Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. Applied Sciences, 10(16), 5702.

[14] Kenya National Bureau of Statistics Economic Survey, (2020). Cyber-attacks in Kenya up by half to hit 56 m in three months. Business Daily.

[15] Krstić, M. (2022). Rational choice theory–alternatives and criticisms. Socijalna ekologija. Časopis za ekološku misao i sociologijska istraživanja okoline, (31), 1.

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

[17] Nevmerzhitskaya, J., Norvanto, E., & Virag, C. (2019). High Impact Cybersecurity Capacity Building. ELearning & Software for Education, 2.

[18] Nurse, J. R., Adamos, K., Grammatopoulos, A., & Di Franco, F. (2021). Addressing the EU cybersecurity skills shortage and gap through higher education. European Union Agency for Cybersecurity (ENISA) Report.

[19] Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity strategy's role in raising Kenyan awareness of mobile secu-rity threats. Information & Security, 32(2), 1.

[20] Paternoster, R., Bachman, R., Bushway, S., Kerrison, E., & O'Connell, D. (2015). Human agency and explanations of criminal desistance: Arguments for a rational choice theory. Journal of Developmental and Life-Course Criminology, 1, 209-235.

[21] Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training meth-ods. Computers & Security, 136, 103585.

[22] Sitienei, J. C., & Kandiri, J. (2024). Evaluating Cybersecurity Threats, Measures, and Effective Factors for Enhancing the Security of Kenya's E-citizen Platform. Reviewed Journal of Social Science & Humanities, 5(1), 463-480.

[23] Stalans, L. J., & Donner, C. M. (2018). Explaining why cybercrime occurs: Criminological and psychological theo-ries. Cyber Criminology.

[24] Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRT s and global cybersecurity: How technical experts support science diplomacy. Global Policy.

[25] The American Society for Training and Development (2019). "Designing Learning: Clear Objectives." Retrieved from https://www.td.org/insights/designing-learning-clear-objectives

[26] The Association for Talent Development (2021). "The State of the Industry: Training by the Numbers." Association for Talent Development. Retrieved from https://www.td.org/insights/the-state-of-the-industry-training-by-the-numbers

[27] Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training meth-odologies. Heliyon, 5(6).

[28] Wekundah, R. N. (2015). The effects of cyber-crime on e-commerce; a model for SMEs in Kenya (Doctoral disserta-tion, University of Nairobi).

[29] Whitmire, T. (2020). The Arrest and Prosecution of Cyber Stalkers: How" Rational" are Criminal Justice Decision Mak-ers?

[30] Zhao, J., Wang, X., Zhang, H., & Zhao, R. (2021). Rational choice theory applied to an explanation of juvenile offender decision making in the Chinese setting. International Journal of Offender Therapy and Comparative Criminolo-gy, 65(4), 434-457.