# Assessing Cybersecurity Preparedness for Enhanced Digital Transformation; A Case of Selected Public TVET Institutions in Kenya

**Kithungu Rose Mwikali (PhD)[1], Gideon Mutuku Kasivu (Ed.D)[2]**

**[1]Lecturer-Comparative and International Education-South Eastern Kenya University**

**[2]Senior Lecturer - Educational Administration - South Eastern Kenya University**

**DOI: https://doi.org/10.47772/IJRISS.2026.100700214**

**Received: 09 July 2026; Accepted: 14 July 2026; Published: 29 July 2026**

## ABSTRACT

Technical and Vocational Education and Training (TVET) institutions play a pivotal role in equipping the Kenyan workforce with the knowledge, skills and competencies required in the digital era. The increasing digitalization of institutional procedures and the extensive adoption of technologies have exposed TVET institutions to cybersecurity threats. These threats compromise institutional integrity, protection of data and sensitive information, and disrupt teaching and learning processes. This study assessed cybersecurity preparedness in selected public TVET institutions in Kenya by investigating the internal cybersecurity policies, practices, technologies, incident response and recovery procedures of identifying existing vulnerabilities and areas of improvement. The study embraced mixed-methods research approach, integrating quantitative surveys with qualitative interviews involving the key stakeholders. Random sampling techniques was used to select fifty TVET institutions, questionnaires were used as data collection tools.

The findings revealed some TVET institutions had made significant progress in developing and implementing internal cybersecurity policies and controls. The study also found that many institutions were inadequately prepared to address advancing cyber threats. Key challenges identified by the researcher include the absence of comprehensive cybersecurity preparedness strategies, insufficient financial and technical resources, limited staff in-service training, and inadequate cybersecurity awareness programmes. The recommendations were; TVET institutions to develop comprehensive internal cybersecurity strategies and policies, management to ensure implementation of the policies, conduct regular cybersecurity risk assessments, strengthen incident retort and recovery competences, and ensure continuous cybersecurity preparedness and capacity-building programmes for staff and students. This measures will ensure safeguarding of institutional data and information, protect critical information technology resources, and enhance digital transformation.

**Keywords:** Cyber Security, Digital Transformation, Preparedness, TVET.

## INTRODUCTION

### Background to the Study

Globally education has become increasingly digital, with higher learning and TVET institutions worldwide facing cases of data breaches, ransomware, and phishing attacks by scammers which calls for cybersecurity preparedness and audits. The Kenya's digital transformation agenda, anchored in Vision 2030, envisages a globally competitive economy powered by a digitally skilled and competent workforce. Technical and Vocational Education and Training (TVET) institutions occupy a pivotal position in ensuring actualization and achievement of this vision, because they are tasked with producing graduates equipped with competencies that meet the demands of an increasing digital economy (TVET CDACC.2025). These institutions offer programs

that are specifically designed to equip individuals with practical skills and competencies needed by industries in various sectors across the globe (Korir, S., & Ngetich, P. 2026).

A study done in Canada to assess the effectiveness of cyber domain controls at three Canadian higher education institutions found that the institutions had detailed continuous auditing of system vulnerabilities, which was compliant with security policies, and well-structured incident response management (Sabillon, R., et al, 2024). In United Kingdom a study on cybersecurity maturity assessment framework specifically for higher education institutions showed that universities lacked comprehensive cybersecurity preparedness despite existing security policies. The study recommended a comprehensive framework to enable continuous evaluation of cybersecurity preparedness across supremacy, expertise, conformity and risk management (Aliyu, A., et al, 2020).

A study done by Nkambule, M., et al (2025) in South Africa whose objective was to develop a cybersecurity framework for African higher education institutions, revealed that African institutions face cybersecurity challenges due to lack of preparedness, inadequate funding, limited digital infrastructure, and increasing cyber threats. This shows the need to have internal cybersecurity policies, strong technical controls, and continuous staff capacity building.

The Kenyan government has accelerated this agenda through expansive digital infrastructure investment, including the establishment of digital hubs nationwide, and championing the establishment of TVET institutions, and boosting operationalization through installation of fiber connectivity. TVET institutions handle sensitive student data, financial information, manage digital learning platforms, research data, and deliver majority of services through online platforms which make them targeted by cybercriminals. According to Kiarie, N. (2024), an institutional cyberattack can have far-reaching and devastating consequences that extend beyond technical disruptions. It can result in unauthorized access, loss of sensitive and confidential information, including students' records, employees' personal data, financial information. Such breaches compromise the privacy of institutions, cause reputational harm and expose the institution to legal and regulatory risks (Musila, 2023).

The Kenyan government has realized the significance of immensely strengthening cybersecurity measures in all sectors including education. One of the strategies was setting The National Cybersecurity Strategy (2018-2022) which outlines a framework to strengthen the country's cybersecurity resilience (NC4 2022). Although the strategy recognizes the importance of strengthening cybersecurity within educational institutions TVET included, it does not stipulate the specific guidelines and implementation frameworks to approach and resolve cybersecurity challenges and operational needs (National KE-CIRT/CC, 2022).

Research from the Evolving Cybersecurity Landscape in Africa 2022 indicated that Kenya recorded an 82% increase in cyberattacks targeting large and medium-sized enterprises, compared to a 62% increase in South Africa. These statistics demonstrate an increasing complexity and rate of recurrence of cyber threats in Kenya, highlighting the need for institutions, including Technical and Vocational Education and Training (TVET) institutions, to strengthen their cybersecurity preparedness and resilience (KPMG., 2022). In July 2023 many government enterprises experienced cyber-attacks and threats. One of the major attacks was the hacking of Kenya’s e-citizen portal which attracts million of users and houses thousands of government services and personal information. This is an indication that cybersecurity preparedness and digital transformation is of paramount importance not only in TVET institutions but in Kenya as a country (Koros, H. K., et al 2024).

Kenyan educational institutions have recorded cyber-attacks and indication of the increasing risks and challenges of the digital age, which implies that evolvement of technology require advanced strategies to curb cybercriminals. For institutions to protect their clients, students, personnel, and data from cyber threats, they must maintain vigilance, employ practical cybersecurity measures, and foster a cyber-preparedness and awareness culture (Sang, M., 2023). TVETs and other educational institutions bank vast amounts of personally identifiable information (PII) that can be misused and minted by criminals in case of hacking.

This digital expansion has superficially outpaced the development of comparable cybersecurity competencies in many TVET institutions. Empirical studies on cybersecurity preparedness in Kenyan TVET institutions reveal concerns and gaps between digital transformation and cybersecurity preparedness. This study examined that gap

through the lens of cybersecurity preparedness and competency, maintaining the argument that enhanced digital transformation, TVET institutions capacity to adjust, respond, and prosper in a digitally complex environment necessitates foundational cybersecurity competency.

### Statement of the Problem

Kenya's TVET institutions are experiencing rapid digital revolution, creating unique opportunities for enhanced pedagogical activities, administrative efficiency, and production of globally competitive graduates. Due to technology advancements, Technical and Vocational Education and Training (TVET) institutions in Kenya are heavily relying on digital tools to heighten their educational activities, administrative operational structures, and data management. However, this digital transformation introduces significant cybersecurity risks which can endanger institutional integrity, data safety and protection, operational stability, and the broader goal of creating digitally competent individuals. This poses significant challenges to the security and integrity of TVET institutions' technology systems and sensitive information.

Cybersecurity preparedness and digital transformation among TVET institutions in Kenya remains largely unexplored which exposes them to survival threats in the digitally complex environment. With the Competency Based Education TVET skill and knowledge remain of great importance towards attainment of the national educational goal, hence the need to ensure technological compliance. A comprehensive assessment of TVETs' cybersecurity preparedness, identification of all potential vulnerabilities, and development of operational strategies to protect the institutions against cyber threats is of great importance. Identification of the prevailing gaps in cybersecurity practices and preparedness is critical to the formulation of institutional cyber-security policies, data handling and safety procedures, and personnel training initiatives that can strengthen the information security carriage and data transformation of these institutions. This justifies the need to assess cybersecurity preparedness for enhanced digital transformation; a case of selected public TVET institutions in Kenya.

### Specific Objective of the Study

The main objective of this study assess cybersecurity preparedness for enhanced digital transformation; a case of selected public TVET institutions in Kenya.

## REVIEW OF RELATED LITERATURE

### Cybersecurity Preparedness and Digital Transformation

Cybersecurity preparedness refers to an institution's readiness and ability to effectively detect, prevent, and respond to, cyber-attacks as well as the ability to recover information. It encompasses institutional policies, procedures, technologies, and personnel training programs aimed at ensuring proficiency and integrity in handling data systems (Owino, B., 2025). Key elements of effective cybersecurity preparedness include; regulations on institutional preparedness, assessment of risk vulnerability, management incident response plans, cybersecurity awareness training, regular audits and monitoring, compliance with relevant laws to ensure sustainable implementation (Robert P et al., 2024).

The cybersecurity frameworks are structured guidelines or sets of best practices designed to help organizations protect their information systems, networks, and data from cyber threats. These frameworks offer a systematic approach to managing cybersecurity risks, enhancing preparedness, resilience, and improving overall cybersecurity strength of institutions. Educational institutions ought to follow the guidelines when developing their cybersecurity policies and strategies.

Cyber security preparedness frameworks include comprehensive guidelines or structures that help institutions establish a robust cybersecurity posture. They provide a methodical approach to identifying cyber vulnerabilities, implementing controls, detecting cyber threats, responding to hacking incidents, and recovering information

from attacks. The purpose of these frameworks is to provide organizations and educational institutions with a blueprint for improving their overall cybersecurity preparedness to enhance digital transformation.

As study conducted in China to examine the drivers of digital transformation and cybersecurity preparedness in Technical and Vocational Education and Training (TVET) found that digital transformation in TVET is driven by industrial demands, technological structures, digital governance and economy, and changing labour market demands. TVET institutions therefore require sufficient digital infrastructure, cybersecurity preparedness skills, competent personnel, and operative governance to productively implement digital transformation (Robert P. et al., 2024)

A study on evaluation of cybersecurity maturity among universities within Nairobi County adopted descriptive survey design and used questionnaires administered to IT staff from 25 universities found that most universities had basic cybersecurity controls, only 32% had formal and practical cybersecurity policies. The study also revealed lack of staff cybersecurity preparedness and awareness, inadequate digital protection training, and weak incident response systems. It recommended adaptation of cybersecurity frameworks and guidelines alongside continuous capacity building (Owino, B., et al., 2025).

The aforementioned studies emphasizes that TVET institutions require relevant cybersecurity preparedness, and cybersecurity measures for effective digital transformation. Evidently, most empirical research was done on universities, leaving a significant research gap related to cybersecurity preparedness. digital challenges, institutional cybersecurity policy formulation, and readiness of TVET institutions to attain remarkable digital transformation. This study sought to assess cybersecurity preparedness for enhanced digital transformation; a case of selected public TVET institutions in Kenya.

# METHODOLOGY

### Research Design

This study adopted a descriptive survey research design to collect data. This is because the design enables collection of data involving description of the characteristics, views, attitudes, behaviours, and environments of respondents. It enabled the representative sample of TVET institutions in Kenyan describe the current level of cybersecurity preparedness and digital transformation. The design was appropriate as it facilitated the collection of standardized data through questionnaires without manipulating the study variables (Creswell, J. W., 2023)

### Target Population

The study selected only 50 public TVET institutions out of the 1,432 institutions in Kenya based on the knowledge needed for the research. The target population were Heads of ICT departments, ICT managers and ICT technicians of the TVET institutions.

### Sampling Techniques and Sample Size

Simple random sampling technique was used to select the 50 public TVET institutions. Purposive sampling technique was employed for respondent's selection at institutional level. This is because the respondents were only the Heads of ICT departments, ICT managers and ICT technicians because they were in possession of the information needed. The researcher shared out 70 questionnaires online. Only 58 questionnaires were filled completely and returned, which gave a questionnaire response rate of 83%. A return rate of 50% is suitable for analysis and reporting; a rate of 60% is good; and a rate of 70% or more is excellent (Mugenda & Mugenda, 2003).

### Research Instruments

The study embraced structured online questionnaire to collect data. The online questionnaires enabled collection of voluminous data within a short time, thus avoiding transport costs. The tools were issued to the ICT, Heads

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue VII July 2026

of ICT departments, ICT managers (12%) and the systems administrators, being the individuals mandated to manage and oversee the ICT systems in the institutions.

**Validity of Research Instruments and**

Validity is the extent to which scores from an instrument represent the intended variables or accuracy of measurement (Creswell & Creswell, 2023). The researcher established content and face validity of the research instrument. To establish face validity, the researcher ensured that all questionnaires were developed in line with the study objectives. To enhance content validity, piloting will be done in10 public TVET institutions selected using simple random sampling.

**Reliability of Research Instrument**

The reliability of the instrument in this study was achieved through a test-retest procedure. Reliability was computed. To ensure the reliability of the questionnaires used in this study, an internal consistency analysis was conducted.

The questionnaire were administered to a pilot group of respondents drawn from TVET institutions not part of the main study sample. After a two-week interval, the same instrument were administered to the same respondents. The two sets of scores were correlated using Pearson's Product Moment Correlation Coefficient to determine the stability of the instrument over time. A reliability of 0.642 for respondent's questionnaires was realized; hence the researcher considered the instrument reliable (Creswell & Creswell, 2023).

**Data Analysis Techniques**

Data analysis involved organizing the responses from the questionnaires in to themes, cleaning the data, coding the variables, and preparing them for statistical interpretation with the aid of statistical package SPSS for social sciences version 29. The data was presented using frequency tables, standard deviation and percentages to illustrate the distribution of responses and highlight emerging trends.

**Data Analysis, Interpretation and Presentation**

**Questionnaire Return Rate**

Out of the 70 questionnaires shared online only 58 were filed completely and returned. This translated to a questionnaire return rate of 83%. Therefore, the collected questionnaires were considered sufficient for the study because they provided adequate data which could yield reliable results**.**

**Table 4.1. Questionnaire Return Rate**

| **Position** | **Frequency** | **Percent** |
|---|---|---|
| System administrators | **6** | **10%** |
| Heads of ICT Departments | **20** | **35%** |
| ICT Technicians | **25** | **43%** |
| ICT managers | **7** | **12%** |
| **Total** | **58** | **100%** |

From the table the ICT technicians formed the largest percentage of response (43%) followed by the heads of ICT department (35%) and ICT managers (12%) and the systems administrators (10%). These are the individuals mandated to manage and oversee the ICT systems in the institutions.

**Cybersecurity Preparedness and Digital Transformation**

**Table 4.2 System User's Preparedness in Relation to Cyber Security**

| Level | None | | Basic | | Moderate | | High | | |
|---|---|---|---|---|---|---|---|---|---|
| **Responses** | **No** | **%** | **No** | **%** | **No** | **%** | **No** | **%** | **Total** |
| Cybersecurity preparedness/awareness trainings are conducted termly to educate employees on emerging cyber security attacks | 43 | **74%** | 10 | **17%** | 3 | **5%** | 2 | **4%** | 58 |
| Periodic review of employee system activity logins is done to inspect device use | 16 | **28%** | 18 | **31%** | 13 | **22%** | 7 | **11%** | 58 |
| Does your institution have a Computer Incident Response Team (CIRT) with a formal process to respond to incidents /threat/ attacks | 50 | **86%** | 5 | **9%** | 1 | **2%** | 2 | **3%** | 58 |
| All staff/ users and devices undergo a standard approval process prior to use with minimum data access required to do their jobs. | 0 | **0%** | 16 | **28%** | 18 | **31%** | 24 | **41%** | 58 |
| Are there restrictions in place to prevent users from downloading and installing software or altering operating system configurations on their workstations or devices | 22 | **38%** | 25 | **43%** | 9 | **16%** | 2 | **3%** | 58 |

The data captured in Table 4.2 indicated that most TVET institutions 74 percent did not have any cyber security preparedness trainings to educate employees on emerging cyber security attacks. Further, only 17 percent of the TVET institutions had conducted some basic form of training and less than 5 percent and 4 percents conducting the training moderately and highly on termly basis respectively.

Cumulatively most of the institutions 72 percent of the TVET institutions did some periodic review of employee system activity logins, however 28 percent do not do any review. This was an indication that some TVET institutions are proactive in monitoring user activities for security purposes. Majority of the TVET institutions 87 percent, or 50 out of 58 indicated not having a Computer Incident Response Team (CIRT) with a formal process to respond to attacks/incidents. This is a strong indication of lack preparedness in case of cybersecurity incidents.

In addition, none of the institutions reported not having all staff/users and devices undergo a standard approval process prior to use with minimum data access required to do their jobs. Only 28 percent, 31 percent, and 41 percent of the institutions reported having minimal, basic, and high standard approval process for users and devices required for job functions respectively. This is a strong sign of strict access control which is fundamental to cybersecurity preparedness and digital transformation.

Further, a significant number of TVET institutions 62% percent reported having some form of restrictions in place to prevent users from downloading and installing software or altering operating system configurations on their workstations or devices. However, 38 percent indicated not having restrictions which can pose security risks to the equipment.

**Table 4.3. Institutional Procedures of Operation and Monitoring Cybersecurity**

| Level | None | | Basic | | Moderate | | High | | |
|---|---|---|---|---|---|---|---|---|---|
| **Responses** | **No** | **%** | **No** | **%** | **No** | **%** | **No** | **%** | **Total** |
| The institution has mapped movement of information through the organizational structures | 42 | **72%** | 13 | **22%** | 1 | **2%** | 2 | **4%** | 58 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| There is proper coordination of roles and responsibilities for managing cybersecurity processes to avoid duplication and alignment to the employees position | 24 | **41%** | 22 | **38%** | 8 | **14%** | 4 | **7%** | 58 |
| There is periodical review of user activity on the network to identify questionable behavior. | 30 | **52%** | 13 | **22%** | 12 | **21%** | 3 | **5%** | 58 |
| Your institution has a network segmentation and segregation strategy in-place to limit the impact of an intrusion. | 7 | **12%** | 19 | **33%** | 21 | **36%** | 11 | **19%** | 58 |
| There is regular back up plan to a secure, encrypted, and off-site location that can aid in information recovery in case of a cyberattacks. | 2 | **3%** | 25 | **45%** | 22 | **38%** | 9 | **16%** | 58 |

The information captured in Table 4.3 indicated that majority of the TVET institutions, 72 percent, had not mapped movement of information through the organizational structures. This indicates a poor management and understanding of data flow within the institutions which is fundamental for effective cybersecurity. In addition, 22 percent, 2 percent , and 4 percent recorded basic, moderate and high mapping movement of information through the organizational structures respectively.

The analysis further showed that 41 percent and 38 percent of TVET institutions had none and basic coordination of roles and responsibilities for managing cybersecurity processes to avoid duplication and alignment to the employees position respectively. This implies that there is need for improvement in ensuring management of cybersecurity processes and alignment with employees' positions.

Slightly over half of the TVET institutions 52 percent reported to not having any form of periodical review of user activity on the network to identify questionable behavior. This exposes the data and information to risks since user activity review is an essential aspect of cyber threat detection. Further the information indicated that approximately 36 percent and 19 percent of TVET institutions have a moderate to high forms of network segmentation and segregation strategy in-place to limit the impact of an intrusion. This is a strong indicator of cybersecurity preparedness thus notable digital transformation.

Further analysis revealed that a significant number of TVET institutions 45 percent, 38 percent, and 15 percent undertook basic, moderate and high regular back up plan to a secure, encrypted, and off-site location that can aid in information recovery in case of a cyberattacks respectively. However, 3percent of the TVET institutions did not have regular back up plan to a secure, encrypted, and off-site location that can aid in information recovery in case of a cyberattacks.

**Table 4.4. Adoption of Cybersecurity Internal TVET Policy**

| **Level** | **None** | | **Basic** | | **Moderate** | | **High** | | |
|---|---|---|---|---|---|---|---|---|---|
| **Responses** | **No** | **%** | **No** | **%** | **No** | **%** | **No** | **%** | **Total** |
| The institutions have cybersecurity or ICT policies, procedures and standards based on required standards | 3 | **5%** | 42 | **72%** | 6 | **10%** | 7 | **12%** | 58 |
| The institutional policy includes an operational continuity and disaster recovery plan | 19 | **33%** | 21 | **36%** | 10 | **17%** | 8 | **14%** | 58 |
| Cybersecurity policies are continuously tested to determine their usefulness against emerging cyber threats | 50 | **86%** | 6 | **10%** | 2 | **4%** | 0 | **0%** | 58 |
| The institution performs formal internal and external IT audits | 8 | **14%** | 10 | **17%** | 19 | **33%** | 21 | **36%** | 58 |
| Cybersecurity risk assessments are regularly performed and documented for reference | 11 | **19%** | 19 | **33%** | 21 | **36%** | 7 | **12%** | 58 |

The data contained in Table 4.4 showed that 72 percent of the TVET institutions have established basic cybersecurity or ICT policies, procedures and standards based on required standards. These findings suggest that the institutions had made progress in developing cybersecurity policies, procedures and standards, however, further enhancements are necessary to align the institutions with recognized industrial best practices. Further, the analysis revealed that 36 percent of the TVET institutions had basic policies which include an operational continuity and disaster recovery plan while 17 percent, and 14 percent indicated moderate and high policies which include an operational continuity and disaster recovery plan respectively

A significant majority of TVET institutions 86 percent reported lack of cybersecurity policies which are continuously tested to determine their usefulness against emerging cyber threats. While 14 percent of the institutions registered minimal cybersecurity policies which are continuously tested to determine their usefulness against emerging cyber threats, an implication of extensive improvement in all institutions. The analysis also indicated that 36 percent, 33 percent, and 17 percent of TVET institutions perform formal internal and external IT audits, with 14 percents indicating none. This is commendable because formal internal and external IT audits are essential in identification of vulnerabilities and weaknesses.

Further, 12 percent of the TVET institutions indicated that they highly perform regular cybersecurity risk assessments and document them for reference, while 36 percent and 33 percent showed moderate and basic levels that cybersecurity risk assessments are regularly performed and documented for reference respectively. On the contrary 19 percent indicated no compliance to the practice. This demonstrates lack of commitment in cyber threats identification and mitigation procedures posing potential risks to the institutions data.

The findings suggest that TVET institutions have made considerable progress in developing cybersecurity and ICT policies, procedures and standards. However, considerable improvements are required, like conducting regular cybersecurity risk assessments and constantly testing these procedures to ensure their efficiency in countering evolving cyber threats.

**Table 4.5. Technical Protection of TVET Institutions IT Systems Against Cyber Attacks**

| **Level** | **None** | | **Basic** | | **Moderate** | | **High** | | |
|---|---|---|---|---|---|---|---|---|---|
| **Responses** | **No** | **%** | **No** | **%** | **No** | **%** | **No** | **%** | **Total** |
| There is a strong password with Multi-Factor Authentication (MFA) to increase security. | 0 | **0%** | 46 | **79%** | 9 | **16%** | 3 | **5%** | 58 |
| IT systems are protected by restricting changes to the system, software installation, connection of external devices, monitoring electronic communications, and system users. | 15 | **26%** | 34 | **59%** | 4 | **7%** | 5 | **9%** | 58 |
| The computers' applications and operation systems are up to date with the latest security patches. | 10 | **17%** | 27 | **47%** | 15 | **26%** | 6 | **10%** | 58 |
| Protective tools in place including anti-malware, firewall, and IDS/IPS systems to prevent and detect unauthorized access and activity | 3 | **5%** | 43 | **74%** | 9 | **16%** | 3 | **5%** | 58 |

From the analysis captured in Table 4.5, a substantial number of TVET institutions, 79 percent reported having a basic strong password with Multi-Factor Authentication (MFA) to increase security, however only a few institutions 20 percent had integrated strong password with Multi-Factor Authentication(MFA) to increase security leaving them vulnerable to unauthorized access while none of the institutions recorded lack of strong

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue VII July 2026

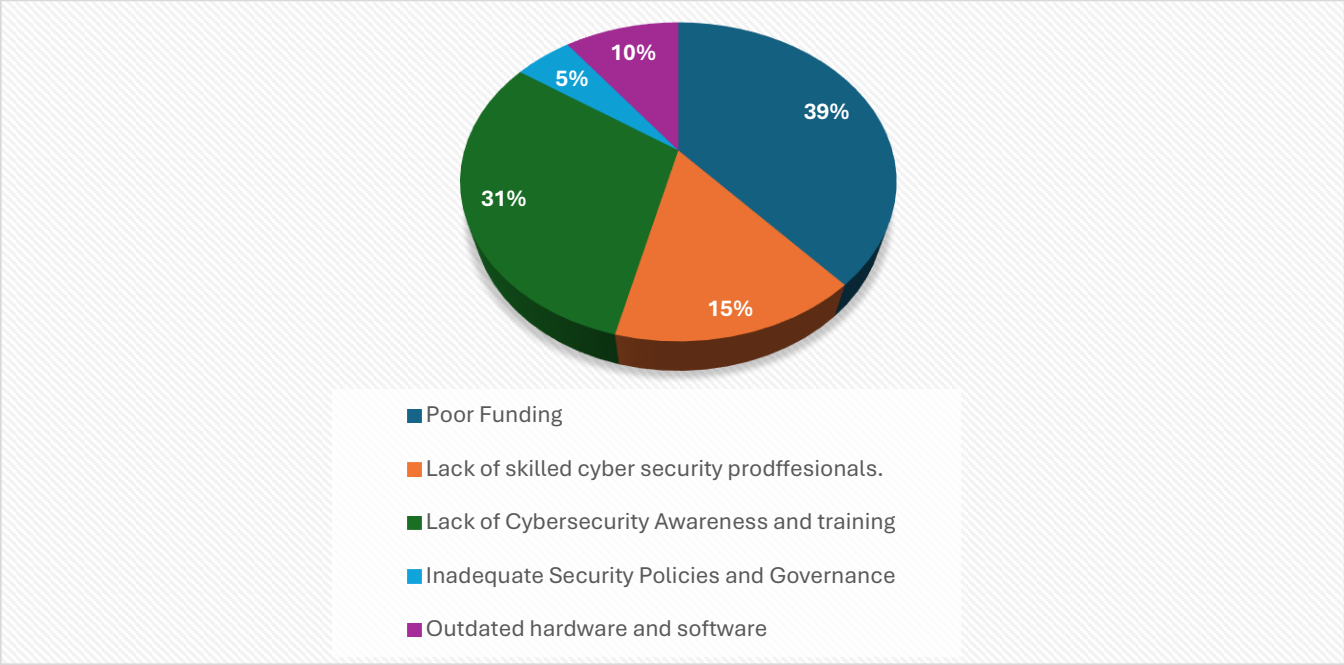
password with Multi-Factor Authentication (MFA). TVET institutions should implement a robust password policy and enforce Multi-Factor Authentication (MFA) for all user accounts. This involves having complex passwords, regular change of password, and implementation of MFA for increased security.

In addition, approximately 59 percent of institutions indicated that they had basic IT systems protection by restricting changes to the system, software installation, connection of external devices, monitoring electronic communications, and system users, while 26 percent recorded none. This is an indication that TVET institutions should endeavor to have strong data protection and restriction measures. The analysis also revealed that 47 percent of the institutions had basic computers' applications and operation systems up to date with the latest security patches, and 26% had a moderate approach while 10 percent showed high. To address this issue, institutions should establish a robust patch management process to ensure all software and operating systems are regularly updated in order to minimise attacks.

Although majority of institutions, 74% percent, had basic protective tools in place including anti-malware, firewall, and IDS/IPS systems to prevent and detect unauthorized access and activity, while 16 percent and 9 percent indicated moderate and high respectively. Many TVET institutions do protective tools in place including anti-malware, firewall, and IDS/IPS systems to prevent and detect unauthorized access and activity. In order to boost their security strength, TVET institutions should adopt intrusion detection and prevention systems to monitor and respond to cyberattacks and threats.

**Cybersecurity Preparedness**

**Figure 4.1. Factors Affecting Cybersecurity Preparedness**




The data presented in figure 4.1 indicate that 39 percent of TVET institutions cite poor funding as a key factor affecting their cybersecurity preparedness and digital transformation. Insufficient financial resources limit institutions ability to invest in robust cybersecurity measures, leading to exposures. In addition, 31% of institutions pointed out lack of cybersecurity awareness and training as a factor affecting cybersecurity preparedness, this results in employees being uninformed of common threats like phishing.

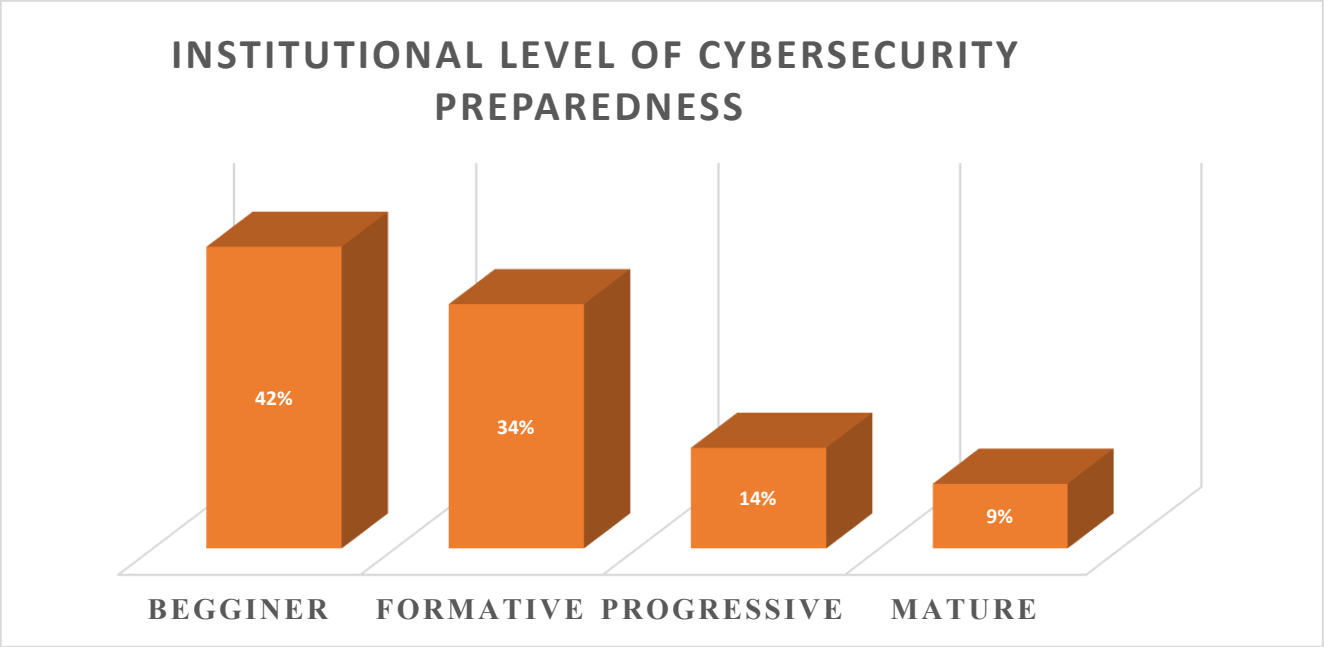
Further, 15 percent of TVET institutions reported a shortage of skilled cybersecurity professionals as a challenge towards their cybersecurity preparedness. The continuous shortage of proficiency in cybersecurity can leave institutions vulnerable to threats. The data also showed that 1 percent of institutions struggle with outdated hardware and software, which are liable to attacks by hackers. Only 5 percent of the institutions highlighted inadequate security policies and governance as a challenge affecting their cybersecurity preparedness.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue VII July 2026

**Institutions Level of Cybersecurity Preparedness**

Finally, the study ranked institutions according to their level of cybersecurity readiness. The data was organized and categorized into four stages of readiness as follows; Beginner, Formative, Progressive and Mature. TVET institutions that have achieved advanced stages of deployment and can be considered ready to address security risks.

**Figure 4.2. Institutions Level of Cybersecurity Preparedness**




Data presented in figure 4.2 indicate that nearly half of the respondents 42 percent classified their institutions as Beginner in terms of the level of cybersecurity preparedness which implies that they are most vulnerable, lack a comprehensive cybersecurity awareness strategy and have limited mitigation measures in place in case of cyberattacks. 34 percent of the institutions fell under the Formative category and indication that they had taken required steps to protect themselves in case of cyberattacks but not fully prepared. Lastly 14 percent of the institutions were captured as Progressives while 9 percent fell under the Mature category of cybersecurity levels of preparedness.

## CONCLUSION

Assessing cybersecurity preparedness and digital transformation of TVET institutions in Kenya is critical for data and information safety. The findings from this study highlight several drawbacks facing these educational institution thus compromising their cybersecurity preparedness. Cybersecurity preparedness is a complex attempt, and TVET institutions must continue to enhance their cybersecurity practice, procedures and policies to effectively tackle cyber threats and create safer digital environments.

**Recommendations from the Study**

Based on the major findings and conclusions of the study, the following recommendations were made to improve cybersecurity preparedness among TVET institutions in Kenya:

i. TVET institutions should develop clear and inclusive cybersecurity policies and procedures, as well as establish cybersecurity governance framework to oversee adherence and compliance to these policies.
ii. TVET institutions should expose staff and students to regular cybersecurity in-service training programs to prevent cyber risks.

iii. TVET institutions should design formal cybersecurity programs, including short courses, diplomas and post diploma courses to strengthen cybersecurity expertise.
iv. The government should prioritize and increase budget allocation to TVET institutions for the modernization of their IT infrastructure.
v. TVET institutions should develop comprehensive incident response plans outlining the steps to be taken whenever a cybersecurity incident occurs and consistently update it.
vi. TVET institutions should conduct drills and simulations to ensure cybersecurity preparedness and establish effective recovery processes.
vii. TVET institutions should partner with industrial experts and specialists in cybersecurity to bridge knowledge gaps and receive advice on implementation of best cybersecurity practices.
viii. TVET institutions should conduct periodic internal and external IT security audits, guided by established standard frameworks to identify vulnerabilities and faults timely.

## REFERENCES

1. Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. Applied Sciences, 10(10), 3660.
2. Creswell, J. W., & J. David Creswell. (2023). Research design: Qualitative, quantitative, and mixed methods approaches (6th ed.). SAGE Publications.
3. Kiarie, N. (2024). Enhancing Digital Resilience: A Cybersecurity Readiness Assessment of Kenyan TVET Institutions. Journal of the Kenya National Commission for UNESCO, 5(1). https://doi.org/10.62049/jkncu.v5i1.191
4. Koros, H. K., Imbwaga, M. S., & Malaki, H. L. (2024). Opportunities and Challenges of Skills Development using AI. KJ-TVET, 7(1).
5. KPMG, (2022). Africa cyber security outlook - KPMG South Africa. KPMG. https://kpmg.com/za/en/home/insights/2022/09/africa-cyber-security-outlook-report-2022.html
6. Mugenda, O. M., & Mugenda, A. G. (2003). Research Methods: Quantitative and Qualitative Approaches. Nairobi: Acts Press
7. Musila, G. (2023). The State of Cybersecurity in Africa: Current Concerns and Challenges. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4539841
8. National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC). (2022). National Cybersecurity Strategy 2022–2027. National Cybersecurity Strategy 2022–2027
9. Owino, B., Oduor, C., & Chege, G. (2025). An Empirical Assessment of Cybersecurity Maturity in Higher Learning Institutions. Kabarak Journal of Research & Innovation, 15(2).
10. Robert Parua, & Wenming Yang. (2024). The driving logic of digital transformation in TVET. Vocational and Technical Education, 1(2), e17. https://doi.org/10.54844/vte.2024.0590
11. Rotich, E. K. (2020). Cyber Terrorism and National Security in Africa: A Case Study of Kenya (Doctoral dissertation, university of Nairobi).
12. Sabillon, R., Bermejo Higuera, J. R., Cano, J., Bermejo Higuera, J., & Sicilia Montalvo, J. A. (2024). Assessing the Effectiveness of Cyber Domain Controls When Conducting Cybersecurity Audits: Insights from Higher Education Institutions in Canada. Electronics, 13(16), 3257.
13. Sang, M. (2023). An Appraisal of Kenya's National Cybersecurity Strategy 2022: A Comparative Perspective. https://ict.go.ke/wp-
14. TVET CDACC, (2025). Competency Based Curriculum for Information Communication Technology KNQF Level 6. Nairobi: TVET Curriculum Development, Assessment and Certification Council.