Enhancing Digital Resilience: A Cybersecurity Readiness Assessment of Kenyan TVET Institutions

Nahashon Kiarie

Nkabune Technical Training Institute, Kenya

kiarienahashon12@gmail.com

https://doi.org/10.62049/jkncu.v5i1.191

Abstract

Technical and Vocational Education and Training (TVET) institutions play a critical role in preparing the Kenyan workforce for the demands of the digital age. The rapid digitalization and widespread adoption of technology in these institutions poses significant cybersecurity threats, potentially compromising sensitive data, disrupting academic activities, and undermining the overall integrity of these institutions. This study aimed to assess the cybersecurity readiness of TVET institutions in Kenya. It analyzed their existing policies, practices, incident response and recovery procedures to identify potential weaknesses and areas for improvement. The research employed a mixed-methods approach, combining qualitative interviews with key stakeholders along with quantitative surveys distributed across multiple TVET institutions. 50 TVET institutions were randomly selected and questionnaires distributed to the Management and IT personnel in these institutions. 39 questionnaires were returned translating to 78% response rate. The design of the questionnaire was based on the four major cybersecurity elements: people, process, policy, and technology. The findings indicate that while some TVET institutions have made progress in developing and implementing cybersecurity policies, many are still lagging, and vulnerabilities remain prevalent. Several factors contribute to these gaps, including the absence of a comprehensive cybersecurity strategy, limited resources and inadequate training programs. This study recommends the development of robust cybersecurity policies, regular risk assessments and the establishment of security awareness programs. As TVET digital landscape continues to evolve, the implementation of effective cybersecurity measures is paramount to guarantee the protection of information and other IT assets.

Keywords: Cyber Security, TVET, Confidentiality, Integrity, Availability.

Introduction

Background

Every aspect of society, including education, has been revolutionized by technological advances in the modern digital age. The digital environment continues to offer tremendous opportunities to students thereby creating new channels for learning, innovation and social interaction among others. Technical and Vocational Education and Training (TVET) institutions play a crucial role in the Kenyan education system by providing vocational training and skills development to students preparing them for the job market. These institutions offer programs that are specifically designed to equip individuals with practical skills needed by industries across various sectors

The vast quantity of sensitive data handled by TVET institutions, including student records, financial information, and research data, makes them attractive targets for cybercriminals. A successful cyberattack can have catastrophic effects, including data breaches, service interruptions, reputational harm, and financial losses.(Musila, 2023). The Kenyan government has acknowledged the significance of strengthening cybersecurity measures in all sectors, including education. The National Cybersecurity Strategy (2018-2022) has been set out which outlines a framework to strengthen the country's cybersecurity resilience (NC4 2022). However, while the strategy acknowledges the importance of securing educational institutions, it does not provide specific guidelines tailored to the unique challenges faced by TVET institutions. A report on evolving cyber security landscape in Africa 2022 reported an 82% increase in cyber-attacks against large and medium size enterprises in Kenya as Compared to 62% in South Africa. In July 2023 a lot of government enterprises experienced cyber-attacks. One of the major attacks was on Kenya's e-citizen portal which hosts thousands of government services with millions of users and personal information was attacked by people claiming to be Sudanese anonymous hackers. Although the attack was contained, there has been no report on the extent of the damage caused. According to the report Kenya's losses to cyber criminals reached an all-time high of Ksh 3.6 billion (USD 36 million) in 2022. (Zwilling et al., 2022).

Recent cyberattacks on Kenyan educational institutions highlight the increasing risks and difficulties of the digital age. As technology evolves, so do the strategies of the cybercriminals. To protect their students, staff, and vital data from cyber threats, educational institutions must maintain vigilance, employ proactive cybersecurity measures, and foster a cyber-awareness culture. Educational institutions are also caretakers of vast amounts of personally identifiable information (PII) that can be monetized by criminals. These factors provide enough incentive for criminals to take advantage of this sector

Problem Statement

As technology continues to advance, Technical and Vocational Education and Training (TVET) institutions in Kenya are increasingly relying on digital infrastructure to enhance their educational processes and administrative operations(Musila, 2023). While this digital transformation offers numerous benefits, it also exposes these institutions to a range of cybersecurity risks. Cyber threats such as data breaches, ransomware attacks, and phishing attempts have become prevalent in recent years, posing significant challenges to the security and integrity of TVET institutions' systems and sensitive information.

The current landscape of cybersecurity readiness among TVET institutions in Kenya remains largely unexplored. There is a need to comprehensively assess their cybersecurity preparedness, identify potential vulnerabilities, and develop effective strategies to protect against cyber threats. Understanding the existing gaps in cybersecurity practices is critical to developing targeted policies, procedures, and training initiatives that can strengthen the security posture of these institutions.

Objectives

Main Objective

The main objective of this study is to assess the cybersecurity readiness of TVET institutions in Kenya.

Specific Objectives

The primary objectives of this study are as follows:

i. To assess the current state of cybersecurity in TVET institutions in Kenya.
ii. To evaluate the level of cyber security preparedness of TVET institutions in Kenya
iii. To evaluate the factors influencing the cybersecurity readiness of TVET institutions in Kenya.
iv. To propose best practices for enhancing the cybersecurity readiness of TVET institutions.

Literature Review

Cybersecurity Readiness

Cybersecurity readiness refers to an institution's preparedness and ability to effectively prevent, detect, respond to, and recover from cyber threats or attacks. It encompasses policies, procedures, technologies, personnel training programs aimed at ensuring the confidentiality integrity availability of data systems (Makato 2022). Key elements of effective cybersecurity readiness include risk assessment vulnerability management incident response plans security awareness training regular audits monitoring compliance with relevant laws regulations (Kiremu et al., 2022).

Cyber security frameworks are comprehensive guidelines or structures that help organizations establish a robust cybersecurity posture. They provide a systematic approach to identifying vulnerabilities, implementing controls, detecting threats, responding to incidents, and recovering from attacks. The purpose of these frameworks is to provide organizations with a blueprint for improving their overall cyber resilience(Sang, n.d.).

Cybersecurity Frameworks

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 resilience, and improving overall cybersecurity posture. Here are four main cybersecurity frameworks:

NIST Cybersecurity Framework:

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is one of the most widely adopted frameworks globally. The NIST framework consists of five core functions: Identify,

Protect, Detect, Respond, and Recover. Each function is broken down into categories and subcategories that offer specific guidance for cybersecurity practices. The framework encourages organizations to assess and manage risks, establish protective measures, detect and respond to incidents, and establish recovery plans. The NIST framework is highly flexible and adaptable, making it suitable for organizations of all sizes and sectors. It can be tailored to meet specific organizational needs regardless of size or industry sector(KPMG, 2022).

SO/IEC 27001:2013 (Information Security Management System - ISMS)

ISO/IEC 27001 is an international standard that defines requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS)(Mukiibi, 2019). The ISMS provides a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability. The standard includes a risk-based approach, requiring organizations to identify and address information security risks through risk assessments and risk treatment plans. ISO/IEC 27001 is especially relevant for organizations handling sensitive data and is highly respected for its global recognition and certification process.

CIS Critical Security Controls (CSC)

The CIS Critical Security Controls (CSC), formerly known as the SANS Top 20, is a prioritized set of best practices developed by the Center for Internet Security (CIS). It focuses on essential cyber defense actions that organizations should implement to mitigate common threats effectively. One strength of the CIS CSC framework is its practicality. It provides actionable guidance that organizations can readily implement to improve their security posture. The prioritization aspect allows organizations to focus on critical controls first before addressing less critical ones

COBIT (Control Objectives for Information and Related Technologies)

COBIT is a comprehensive IT governance framework designed to align IT activities with business objectives and ensure effective IT management and control. While not exclusively a cybersecurity framework, COBIT includes a set of control objectives and management practices that encompass cybersecurity. COBIT emphasizes risk management, information security, and compliance with relevant laws and regulations. It provides a holistic approach to managing IT risks and aligning IT strategy with organizational goals(Kshetri, 2019). COBIT is particularly valuable for organizations seeking to improve their IT governance and cybersecurity integration. One strength of COBIT is its emphasis on aligning IT with business objectives. It helps organizations ensure that their IT systems support strategic goals while maintaining effective control environments. However, one potential weakness of this framework lies in its complexity. Similar to ISO/IEC 27001, COBIT requires significant knowledge and resources for successful implementation

The Evolving Threat Landscape

During the COVID-19 pandemic, many educational institutions in Kenya shifted to online learning platforms to ensure continuity of education. Consequently, there was an increase in Distributed Denial of Service (DDoS) attacks on e-learning platforms. Cyber attackers overwhelmed the platforms' servers with a massive volume of traffic, causing temporary service disruptions, preventing students from accessing their classes and learning materials(Macharia Njoroge, 2021).

In early 2022, a prominent university in Kenya fell victim to a sophisticated cyber-attack that resulted in a massive data breach. The attackers infiltrated the university's systems and gained unauthorized access to sensitive student records, academic information, and financial data. The stolen data included personally identifiable information (PII) such as names, addresses, phone numbers, and social security numbers(Kshetri, 2019). The incident compromised the privacy and security of thousands of students and staff members, leading to concerns about identity theft and fraud.

Phishing attacks have become prevalent in Kenya's education sector, specifically targeting students, faculty, and staff members. Cybercriminals craft convincing emails disguised as official communications from the institution or educational service providers. These emails often contain malicious links or attachments that, when clicked, deploy malware or request login credentials, thereby gaining unauthorized access to sensitive accounts. Such attacks can lead to data breaches, financial theft, and even compromise the institution's network(KPMG, 2022).

According to Verizon's 2022 Data Breach Investigations Report, the educational services sector experienced 1,241 incidents in 2021, with 282 involving confirmed data disclosure. Of those attacks, 75% were from external sources, while the remainder involved insiders (Verizon 2022). These attacks were overwhelmingly motivated by monetary rewards, with 95% involving a financial motive. ransomware topped the list of the attacks the attack is particularly problematic for the educational sector, with institutions of all sizes around the globe experiencing ransomware attacks with varying degrees of severity and cost. In a December 2020 attack, hackers exploited a vulnerability in third-party software to insert ransomware and extract personal data from government agencies, businesses, and educational institutions, including the University of California

Methodology

Research Design

This research employed a quantitative research design to gather data that was used for this study. According to Mugenda and Mugenda (2003) quantitative approach focuses on technique, design, and measures to produce quantifiable or numerical discreet data.

Population and Sampling

The target population were Heads of ICT departments, ICT managers and technicians of various TVET institutions. The 50 target population were selected based on the knowledge needed for the research. Simple random sampling was used to select TVET institutions while purposive sampling was employed for respondent's selection. The researcher sent out 50 online questionnaires, and 39 of them were returned, for a response rate of 78%. According to Mugenda & Mugenda (2003), a response rate of 50% is suitable for analysis and reporting; a rate of 60% is good; and a rate of 70% or more is excellent.

Data Collection Instruments

The study relied on the use of structured online questionnaire to collect data. Online questionnaires were selected for this study since one can collect voluminous data within a short time and also it is less costly.

Validity and Reliability of The Instrument

The validity of the questionnaire in this study was ensured by going through the questionnaire in relation to set objectives to ensure that it contains all necessary information that answers the objectives. The reliability of the instrument in this study was achieved through a test-retest procedure. Reliability was computed. A reliability of 0.642 for respondent's questionnaires was realized; hence the researcher considered the instrument reliable.

Data Analysis, Presentation and Discussion

Data was analyzed with statistical tools using frequency, percentages, mean, and standard deviation while the results were presented using tables and Likert scale. Both descriptive and inferential analysis methods were used for the analysis of results.

Response Rate

It was noted that 39 out of 50 of the questionnaires were returned which translated to a return rate of 78%. The collected questionnaires were therefore used for the study because they were considered to be enough for providing adequate results**.**

Position Held

Table 1: Position held

Position	Frequency	Percent
System administrators	1	3%
Heads of ICT Departments	13	33%
ICT Technicians	21	54%
ICT managers	4	10%
Total	39	100%

Majority of the respondents were ICT technicians (54%) followed by the heads of ICT department (33%) and ICT managers (10) and finally systems administrators (3%). These are the people who are mandated to manage and oversee the ICT systems in their organizations.

People: System User's Awareness with Regard to Cyber Security

Table 2: system user's awareness with regard to cyber security

	None		B		M		H		
	No	%	No	%	No	%	No	%	total
Cyber security awareness trainings are conducted annual basis to educate employees on emerging cyber security threats	29	74%	7	18%	2	5%	1	3%	39
Periodic review of employee system activity logs is done to inspect use devices	11	28%	12	31%	9	23%	7	18%	39

Does your organization have a computer incident response team (CIRT) with a formal process to respond to incidents	34	87%	3	8%	1	3%	1	3%	39
All users and devices undergo a standard approval process prior to use and only have the minimum data access required to do their jobs.	0	0%	11	28%	12	31%	16	41%	39
Are there restrictions in place preventing users from downloading and installing software or altering operating system configurations on their workstations or devices	15	38%	17	44%	6	15%	1	3%	39
Mean	15	45%	10	26%	7.8	15%	6.2	14%	39

Most institutions (74%) do not have any Cyber security awareness trainings to educate employees on emerging cyber security threats, only 18% have conducted some form of training and less than 5% conducts the training on an annual basis. regular training helps in educating employees about emerging cybersecurity threats.

Cumulatively most of the institutions (72%) are able to do some Periodic review of employee system activity logs, however 28% do not do any review. While there is room for improvement, it shows that some institutions are proactive in monitoring user activities for security purposes.

A majority of institutions (87%, or 34 out of 39) indicated not having a Computer Incident Response Team (CIRT) with a formal process to respond to incidents. This is a strong sign of lack preparedness in case of cybersecurity incidents.

Interestingly, only 28% of institutions (11 out of 39) reported not having a standard approval process for users and devices, and these institutions grant minimum data access required for job functions. This is a strong sign of strict access control which is fundamental to cybersecurity.

A substantial number of institutions (62%) reported having some form of restrictions in place to prevent users from downloading software or altering system configurations. However, 38% (15 out of 39) indicated otherwise, which can pose security risks

Process: Laid Down Procedures of Operation for Monitoring Cybersecurity

Table 3: Laid down procedures of operation for monitoring cybersecurity

Level	**None**		**Basic**		**Moderate**		**High**		
	No	**%**	**No**	**%**	**No**	**%**	**No**	**%**	**Total**
The organization has mapped how information and data moves through the organization	28	72%	9	23%	1	3%	1	3%	39
All roles and responsibilities for managing cybersecurity processes are coordinated to avoid duplication and are aligned to the employees' position	16	41%	15	38%	5	13%	3	8%	39

Do you periodically review user activity on your network to identify suspicious behavior?	20	51%	9	23%	8	21%	2	5%	39
Your organization has a network segmentation and segregation strategy in-place to limit the impact of an intrusion.	5	13%	13	33%	14	36%	7	18%	39
We have a regular back up plan to a secure, encrypted, and off-site location that can aid in recovery from a cyberattack?	1	3%	17	44%	15	38%	6	15%	39
Mean	14	36%	12.6	32%	8.6	22%	3.8	10%	39

A significant majority of institutions (72%, or 28 out of 39) have not mapped how information and data move through their organization. This indicates a poor understanding of data flow, which is fundamental for effective cybersecurity.

Coordination of roles and responsibilities for managing cybersecurity processes varies, with 41% and 38% indicating none or basic coordination respectively. There is need for improvement in ensuring alignment with employees' positions.

Slightly over half of the institutions (51%, or 20 out of 39) reported to not having any form of periodic review of user activity on their network to identify suspicious behavior. Regular user activity review is a crucial aspect of threat detection.

Approximately 36% and 18% of institutions have a moderate to high forms of network segmentation and segregation strategy in place, which helps limit the impact of intrusions. This is a strong indicator of preparedness, However, further efforts are needed in this area

A significant number of institutions (44%, or 17 out of 39) reported having regular backup plans to secure their data, however most of the institutions do not have encrypted backups in off-site locations, this is essential for data recovery in case of cyberattacks.

Policy: Adoption of Cyber Security Policy

Table 4: Adoption of cyber security policy

	None		**Basic**		**Moderate**		**High**		
	No	**%**	**No**	**%**	**No**	**%**	**No**	**%**	**Total**
The organization have a cyber-security or ICT policies, procedures and standards based on industry standards	2	5%	28	72%	4	10%	5	13%	39
The organization policy includes or separately have a business continuity and disaster recovery plan	13	33%	14	36%	7	18%	5	13%	39

Cybersecurity policies are continuously tested to determine their usefulness against new and emerging threats	34	87%	4	10%	1	3%	0	0%	39
The organization performs formal IT audits by internal or external 3rd parties	33	85%	2	5%	3	8%	1	3%	39
Cyber security Risk assessments are performed and documented on a regular basis.	36	92%	1	3%	1	3%	1	3%	39
Mean	23.6	61%	9.8	25%	3.2	8%	2.4	6%	39

The majority of institutions (72%, or 28 out of 39) have established cybersecurity and ICT policies, procedures, and standards, however quite a few of them have been established based on best industry standards. This is a positive sign though some improvement is needed to ensure the policies adhere to recognized industry best practices. A significant majority of institutions (87%, or 34 out of 39) reported lack continuously testing of their cybersecurity policies to evaluate their effectiveness against new and emerging threats.

Approximately (50%) of institutions have integrated business continuity and disaster recovery plans into their policies. This is a crucial component for ensuring business resilience.

Most institutions (85%) do not undergo formal IT audits, either by internal or external third parties. IT audits are essential for identifying vulnerabilities and weaknesses

An overwhelming majority of institutions (92%, or 36 out of 39) do not conduct and document regular cybersecurity risk assessments. This demonstrates a lack of commitment to identifying and mitigating potential risks.

The data suggests that institutions have made significant progress in terms of having cybersecurity and ICT policies, however a lot of improvement is needed in conducting regular risk assessments, and continuously testing their policies against emerging threats.

Technology: Safeguard of IT Systems against Cyber Attacks

Table 5: Safeguard of IT Systems against Cyber Attacks

	None		**Basic**		**Moderate**		**High**		
	No	**%**	**No**	**%**	**No**	**%**	**No**	**%**	**Total**
There is a strong password policy in place with multi-factor authentication to increase security.	0	0%	31	79%	6	15%	2	5%	39
The organization performs regular vulnerability scanning and penetration testing	36	92%	2	5%	1	3%	0	0%	39
IT systems are protected by limiting changes to the system, software installation, connection of external devices, monitoring electronic communications, and users of the system	10	26%	23	59%	3	8%	3	8%	39

Your computers' applications and operating systems are up to date with the latest security patches?	7	18%	18	46%	10	26%	4	10%	39
Protective tools in place including anti-malware, firewall, IDS/IPS systems to prevent and detect unauthorized access and activity	2	5%	29	74%	6	15%	2	5%	39
Mean	11	28%	20.6	53%	5.2	13%	2.2	6%	39

A significant majority of institutions (79%, or 31 out of 39) reported having a basic password policy in place, however only a few institutions (20%) have integrated multi-factor authentication (MFA) to enhance security leaving them vulnerable to unauthorized access. institutions should implement a robust password policy and enforce multi-factor authentication for all user accounts. This includes requiring complex passwords, regular password changes, and implementing MFA for enhanced security.

An overwhelming majority of institutions (92%) do not engage in regular vulnerability scanning and penetration testing, exposing them to unidentified vulnerabilities. To improve, institutions should establish a routine schedule for vulnerability assessments and penetration tests. They should work with cybersecurity experts or services to identify and remediate vulnerabilities proactively.

Approximately 59% of institutions lack comprehensive system protection measures, potentially exposing them to various threats.

Institutions generally do not keep their computers' applications and operating systems up to date with the latest security patches. Approximately 46% reported this practice, and 26% had a moderate approach. To address this issue, institutions should establish a robust patch management process. To ensure all software and operating systems, is regularly updated to mitigate known vulnerabilities.

Although a majority of institutions (74%) have some anti-malware programs. A large majority of institutions do not have advanced protective tools in place, such as firewalls, and IDS/IPS systems, leaving them susceptible to unauthorized access and activity. To bolster their security posture, institutions should urgently deploy intrusion detection and prevention systems to monitor and respond to threats.

Factors affecting cyber security readiness

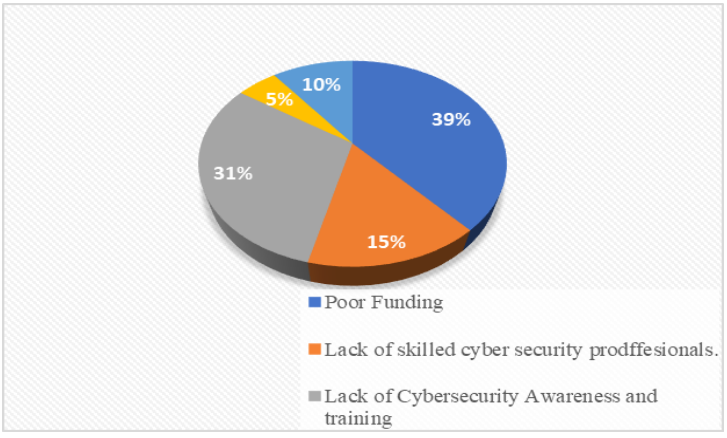

Figure 1: Factors affecting cyber security readiness

The data indicates that a significant proportion of institutions (39%) cite poor funding as a key factor affecting their cybersecurity readiness. Insufficient financial resources can severely limit an organization's ability to invest in robust cybersecurity measures, leading to vulnerabilities.

Approximately 31% of institutions identify a lack of cybersecurity awareness and training as a factor affecting readiness. Insufficient awareness and training can result in employees being unaware of common threats like phishing.

A notable percentage of institutions (15%) report a shortage of skilled cybersecurity professionals as a challenge. The shortage of expertise in cybersecurity can leave organizations vulnerable to threats.

A smaller percentage of institutions (5%) highlight inadequate security policies and governance as a challenge. This can lead to inconsistent security practices. The data shows that 10% of institutions struggle with outdated hardware and software, which are prone to vulnerabilities.

Organizations Level of Cyber Security Readiness

Finally, institutions were categorized according to their level of readiness. The data was organized and categorized into four stages of readiness where respondents were ranked from Beginner (Less than 10)-Organizations at the initial stages of deployment of solutions, Formative (11 – 40)-Organizations that have some level of deployment but performing below average, Progressive (41 – 70): -Organizations with considerable level of deployment and performing average and slightly above average on cybersecurity readiness -, and finally Mature(71 and above): - Organizations that have achieved advanced stages of deployment and can be considered ready to address security risks.

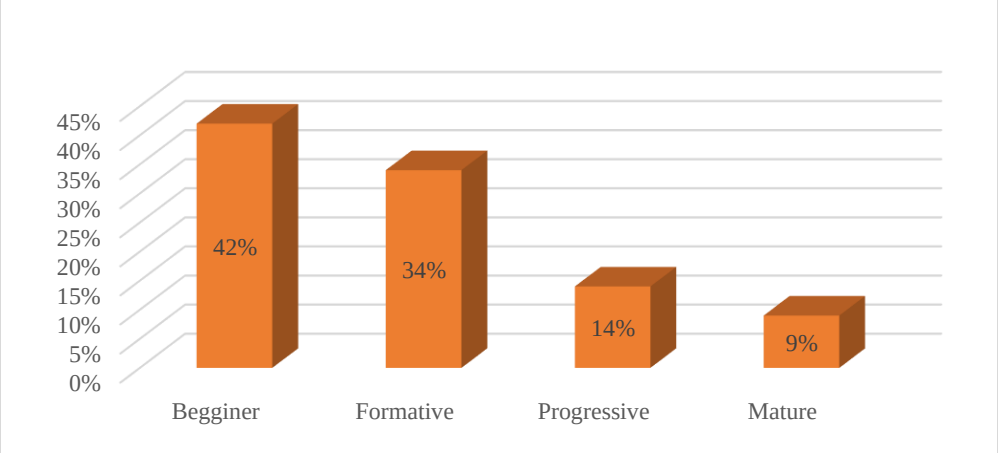

Figure 2: Organizations Level of Cyber Security Readiness

Looking at the overall picture, nearly half of the respondents (42%) and their organizations are classified as "Beginner" in terms of cybersecurity readiness and are at the most vulnerable stage. They often lack a comprehensive cybersecurity strategy and have limited measures in place to protect themselves against emerging cyber-attacks. 34% of the organizations fall under the Formative category, where they have taken some of the much-needed steps to protect themselves but cannot be classified as ready to meet the challenges of our new hybrid world. Progressives form the next cohort at 14%. Only 9% fall into the Mature category, with a high level of readiness.

Conclusion

In conclusion, assessing the cybersecurity readiness of TVET institutions in Kenya is crucial for ensuring the protection of sensitive data and safeguarding against cyber threats. The findings from this research highlight several challenges faced by these educational institutions, including a lack of awareness and resource constraints. Cybersecurity readiness is a multifaceted endeavor, and institutions must continue to enhance their practices and policies to effectively combat cyber threats. By addressing these challenges and implementing the recommended strategies, TVET institutions can enhance their cybersecurity readiness and create a safer digital environment for all stakeholders involved.

Recommendations

Based on the research findings, we propose several recommendations to improve cybersecurity readiness among TVET institutions in Kenya

R1	Institutions should develop clear and comprehensive cybersecurity policies and procedures. They should establish a dedicated cybersecurity governance framework to oversee adherence to these policies, ensure accountability, and enforce compliance.
R2	Insufficient cybersecurity awareness and training can create security vulnerabilities. Institutions should establish regular training programs for their students and faculty covering best practices and common threats like phishing to mitigate these risks.
R3	Institutions should prioritize allocating sufficient budget for cybersecurity measures, including the acquisition of necessary technologies and the hiring of skilled cybersecurity professionals. Additionally, they should explore cost-effective solutions and seek external funding sources or partnerships to bolster their cybersecurity budgets.
R4	TVET institutions should design tailored cybersecurity programs, including short courses, diplomas and post diploma courses to bolster national cybersecurity expertise. Collaborating with external cybersecurity experts can further enhance educational efforts in this vital area.
R5	Outdated hardware and software are susceptible to vulnerabilities. Institutions should prioritize budget allocation for the modernization of their IT infrastructure. This includes upgrading or replacing outdated systems and implementing a regular software update and patch management strategy to keep systems secure
R6	Establish a routine schedule for cybersecurity risk assessments, identifying and prioritizing potential risks and vulnerabilities. Develop mitigation strategies and ensure they are implemented.
R7	Institutions should develop and regularly update a detailed incident response plan that outlines the steps to be taken in the event of a cybersecurity incident. Conduct drills and simulations to ensure preparedness. This will establish effective recovery process in the event of security incidents.
R8	Establish partnerships with industry experts: Collaborating with external organizations specializing in cybersecurity can help bridge knowledge gaps while providing guidance on implementing best practices.
R9	Additionally, they should conduct periodic IT security audits, guided by established standard frameworks, this can be undertaken by internal teams and external third-party entities so as to identify vulnerabilities and weaknesses in good time

References

Chitechi, V. K., Kiprono, B., & Tireito, F. (2020). Cyber-Security Vulnerability and Initiatives in Kenyan County Governments. *African Journal of Computing and Information Systems (AJCIS)*, *4*(3), 17–34.

Chizanga, M. K., Agola, J., & Rodrigues, A. (2022). Factors Affecting Cyber Security Awareness in Combating Cyber Crime in Kenyan Public Universities. *International Research Journal of Innovations in Engineering and Technology*, *6*(1), 54.

Cyoy, R. B. (2022). Framework for Effective Management of Cyber Security on E-learning Platforms in Public Universities in Kenya (Doctoral dissertation, University of Nairobi).

Fielder, J. D. (2021). Cyber security in Kenya: Balancing economic security and internet freedom. In *Routledge Companion to Global Cyber-Security Strategy* (pp. 543–552). Routledge.

IFC & Google. (2020). *Economy Africa 2020: Africa's $180 Billion Internet Economy Future*. Kenya.

International Telecommunication Union. (2017). *Global Cybersecurity Index (GCI) 2017*.

Kagwiria, C. (2020). Cybersecurity Skills Gap in Africa. AFRALTI.

Kaibiru, R. M., Karume, S. M., Kibas, F., & Onga'nyo, M. L. B. (2023). Closing the Cybersecurity Skill Gap in Kenya: Curriculum Interventions in Higher Education. *Journal of Information Security*, *14*(2), 136–151.

Kaimba, B. (2017a). *Africa Cyber Security Report 2017*. Serianu Cyber-Threat Command Centre, Nairobi. Retrieved from www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

Kenya National Cybersecurity Strategy 2022. Retrieved from https://ict.go.ke/wp/content/uploads/2022/10/KENYA-CYBERSECURITY-STRATEGY-2022.pdf

Kiganda, M. (2022). An Assessment of the Factors Affecting Cyber Resilience in Microfinance Institutions in Kenya (Doctoral dissertation, Strathmore University).

KPMG. (2022). *Africa Cyber Security Outlook*. KPMG South Africa. Retrieved from https://kpmg.com/za/en/home/insights/2022/09/africa-cyber-security-outlook-report-2022.html

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2). https://doi.org/10.1080/1097198X.2019.1603527

Macharia, P. (2021). An Examination of Threats Facing Assets in Use in Kenyan Public Universities. *International Journal of Scientific and Research Publications (IJSRP)*, *11*(5), 687–695. https://doi.org/10.29322/IJSRP.11.05.2021.p11372

Mbithi, J. V. (2022). Impact of Social Media on National Security in Kenya (Doctoral dissertation, University of Nairobi).

Mbugua, S., Chitechi, K. V., & Omieno, K. K. (2021). Cyber-Security Vulnerability Assessment Model for County Governments in Kenya.

Mukiibi, H. (2019). Cybersecurity in Africa: The Boring Technology Story That Matters. *XRDS: Crossroads, The ACM Magazine for Students*, *26*(2), 56–59. https://doi.org/10.1145/3368077

Musila, G. (2023). The State of Cybersecurity in Africa: Current Concerns and Challenges. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4539841

Ndeda, L. A., & Odoyo, C. O. (2019). Cyber Threats and Cyber Security in the Kenyan Business Context.

Otieno, D. (2020, November). Cybersecurity Challenges: The Case of Developing Countries. In *Promoting Creativity, Innovation and Productivity for Sustainable Development.*

Rotich, E. K. (2020). Cyber Terrorism and National Security in Africa: A Case Study of Kenya (Doctoral dissertation, University of Nairobi).

Sang, M. (2023). An Appraisal of Kenya's National Cybersecurity Strategy 2022: A Comparative Perspective. Retrieved from https://ict.go.ke/wp-

Taruvinga, F. (2020). Emerging Cyber Security Threats: A Comparative Study of Kenya and Zimbabwe (Doctoral dissertation, University of Nairobi).

Wambalaba, F., Musuva, P., Ouma, M. J., & Nicos, K. (2021). Cybersecurity Risks and National Policy Implications—East African Experiences.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269