Business Education Journal 11 (2025)

journal homepage: https://bej.cbe.ac.tz

Cybersecurity Readiness in Local Government Authorities: A Case Study of Municipal Councils in Tanzania's Dar es Salaam Region

Edwin Marco Kwesigabo[a*] , Lusajo Gidion[a]

[a]Institute of Finance Management, P.O Box 3918, Dar es Salaam, Tanzania.

*Corresponding author

E-mail address: edwin.kwesigabo@ifm.ac.tz

Abstract

Local Government Authorities (LGAs) in Tanzania have increasingly relied on shared ICT infrastructure, which heightens exposure to cyber risks. This study examines how cybersecurity policies, risk management, human factors, and technology and infrastructure shape cybersecurity readiness in five Dar es Salaam Municipal Councils, while also assessing the mediating role of Cybersecurity Implementation Effectiveness (CIE). An exploratory qualitative design was employed, with purposive sampling of 25 ICT staff and system administrators. Data were collected through semi-structured interviews and documentary reviews, and thematically analysed with codes formulated into themes. The findings reveal that readiness is associated with clear government and internal policies, active risk management, human-factor enablers such as staff training and user compliance, and infrastructure sophistication, including security tools and backup systems. However, these determinants translate into higher readiness only where implementation is effective—through regular audits, continuous training, enforcement, timely updates, and practiced incident-response drills. Respondents also identified obsolete systems and inconsistent policy adherence as critical barriers. The study concludes that strong policies, skilled personnel, and advanced infrastructure are necessary but insufficient without effective implementation, making CIE the decisive factor in turning plans into real preparedness. The study recommends that LGAs institutionalize audits and compliance checks, invest in sustained staff training, manage system life-cycles to retire outdated assets, and allocate dedicated budgets for cybersecurity tooling and capability development.

Keywords: *cyber-attacks; Cybersecurity Implementation Effectiveness; Cyber Security Readiness; Key Factors; Local Government,*

1.0 Introduction

The incorporation of Information and Communication Technology (ICT) in the dissemination of information for data management on a large scale is tied to the operational ability of such a mechanism (Dube & Mohanty, 2020). In the corporate world, ICT expertise is entrusted with the task of ensuring zero cybersecurity breaches. Encryption skills have always been a mandatory qualification for one to be considered for the management of the ICT Department (Kshetri, 2019). Some laws govern cybersecurity breaches based on the importance of the information contained. Stronger laws are evidenced in the USA, UK, and China, characterized by their large data and subsequent operation (Global Militarization Indices, 2020).

However, major concern revolves around cybersecurity threats propagating through transnational, globally interconnected cyberspace, which has constantly been making it very complicated to maintain its relevance using conventional state instruments (Shaaban & Athumani, 2020). The details from the Global Cyber Security Index 2015 ranked the USA as the 1st with 0.824 satisfactory level of preparedness in cyber security (Global Militarization Indices, 2020), considering legal, technical, institutional, capacity, and international cooperation measures. This elaboration provides that the aforementioned country has the most adequate set of cybersecurity systems as an international requirement basis (Abiodun & Ogunlana, 2020). This realization implies that ICT expatriates must ensure readiness in addressing potential risks.

Cite paper: *Kwesigabo, E.M. & Gidion, M. (2025). Cybersecurity Readiness in Local Government Authorities: A Case Study of Municipal Councils in Tanzania's Dar es Salaam Region. Business Education Journal, vol(11), Issue 2; 10 pages.*

In Africa, for instance, the country's governing authority in Nigeria is very categorical on rules and regulations on cybersecurity practice, the establishment of Local Government Administration incorporated laws governing data management; such reforms were meant to investigate functionality of the administration, ranging from economic planning, tax collection, and the provision of social amenities (Abiodun & Ogunlana, 2020). Thus, cybersecurity was necessary to abate a probable menace. Here, both the federal and state governments were obliged to carry down to the grassroots, ensuring viable data management (Versify, 2019). Reforms were foremost in the protection of the functionality of the administration and that data management mechanism was certain against possible censure (Kshetri, 2019). This provision confirms the country's policy for comprehensive interests in the cyber domain.

Similarly, other African nations have also recognized the importance of strengthening cybersecurity at both national and local government levels. For example, one of the main reasons behind Kenya's incorporation of cybersecurity measures into her legal frame-work was to safeguard organizational assets that are vulnerable to both external and internal threats (Versify, 2019). External threats often involve physical damage to ICT infrastructure, while internal threats include cyber intrusions such as malware and phishing (Shaaban & Athumani, 2020). To mitigate these risks, Kenya's policies required ICT staff managing e-Government data to possess fundamental cybersecurity knowledge. This encompassed the handling of data acquisition equipment, cash control systems, virus scanners, networking infrastructure, and supporting systems such as uninterruptible power supplies (UPS) (Paganini, 2021).

In Tanzania, the adoption of cybersecurity in government ICT infrastructure has been instrumental in ensuring that data privacy for various departments within government institutions is maintained (Kweka & Sooi, 2022). The application of cybersecurity is getting more pronounced with the rate at which several organizations adopt the use of ICT for their core business functions (Shaaban & Athumani, 2020). The country's Local Government Authority is one of the leading institutions relying on ICT infrastructure, more so, highly concerned with the data security for important information contained therein. Departments within LGA that concern cybersecurity extends to education, agriculture, health, and human resource, among others. Of the Each of the aforementioned departments has cybersecurity personnel for its respective ICT infrastructures (URT, 2022); thus, the preparedness depends on the weight of the encompassed data details While cybersecurity adoption in Tanzania's LGAs has been instrumental in safeguarding sensitive departmental data, the scope of concern extends even further.

The LGAs in Tanzania have many different departments, including education, health, public works, sports and culture, the environment, and economic planning (URT, 2022). These departments manage large volumes of personal and institutional information, such as demographic details (age, health, gender, disability status, marital status, and education) and financial records, all of which must be protected (URT, 2022). It is very important to protect these types of data because they are vulnerable to several hazards, such as malicious exposure and the risk of being made public during a cyber-attack (Manda & Mkhai, 2019). However, the available evidence of how ready LGAs are for cybersecurity shows that there is little if any consistency in practice. For example, there are differences in how consistently cybersecurity measures are applied across departments (URT, 2022), how hiring procedures are based on qualification requirements (Shaaban & Athumani, 2020), and how staffing patterns are based on immediate demand (Kwe-ka & Sooi, 2022). These gaps show how important it is to quickly check the entire state of cybersecurity readiness in LGAs, especially when it comes to how they safeguard their data.

The Cybersecurity Strategy Plan for 2022–2027 indicates that the Tanzanian Government has promised to protect its institutions from cyber-attacks by working to make the country a democratic and cyber-resilient state in the world that is becoming more tech-driven (URT, 2022). The strategy stresses giving ICT workers in all government agencies, including LGAs, better tools to protect data systems and infrastructure through new cybersecurity technologies, professional training, and awareness initiatives for everyone involved (URT, 2022).

However, a noticeable gap persists between the envisioned readiness of ICT staff and the actual

Cite paper: *Kwesigabo, E.M. & Gidion, M. (2025). Cybersecurity Readiness in Local Government Authorities: A Case Study of Municipal Councils in Tanzania's Dar es Salaam Region. Business Education Journal, vol(11), Issue 2; 10 pages.*

adoption and implementation of cybersecurity practices within LGAs. In the light of this gap, the present study seeks to assess the key factors influencing cybersecurity readiness in Tanzania, focusing on the LGAs of Dar es Salaam. The study aims to identify context-specific factors that are both relevant and feasible, ultimately providing LGAs with tailored tools and recommendations to strengthen their cybersecurity readiness. In addition, the study incorporates Cybersecurity Implementation Effectiveness (CIE) as a mediating variable. CIE captures how well formulated policies, risk controls, human-factor interventions, and technological safeguards are actually executed. This mediating perspective responds to the practical gap between designing cybersecurity measures and achieving genuine organizational readiness.

The main objective of this study is to investigate how cybersecurity policies, risk management, human factors, and technology and infrastructure influence cybersecurity readiness through the mediating role of Cybersecurity Implementation Effectiveness (CIE), and to provide practical insights that will enable ICT employees to effectively implement cyber defences and enhance data protection practices.

2.0 Literature Review

2.1 Theoretical Perspective

The General Deterrence Theory, developed by Cesare Beccaria and Jeremy Bentham during the Cold War, was originally used to explain how the threat of severe consequences, particularly from nuclear weapons, could discourage states from engaging in conflict (Maimon, 2020). Over time, this theory has been extended to cyberspace in the form of cyber deterrence, where it suggests that malicious actors can be discouraged from carrying out harmful activities when strong defences, sanctions, and preventive strategies are in place (Gorwa & Smeets, 2019).

Applied to cybersecurity, the theory emphasizes that organizations should strengthen their cyber defences to make attacks costly, difficult, and less rewarding. At the same time, successful at-tackers must face strict consequences to dissuade others from attempting similar actions. Preventive measures such as staff education, regular training, data backups, insurance, and disaster recovery plans further reduce risks by either eliminating certain threats or minimizing their impact.

For organizations such as Local Government Authorities, which handle sensitive administrative data, the theory provides both a conceptual and practical framework for building resilience against cyber threats. It highlights the importance of deterrent systems that not only protect critical IT assets but also discourage potential attackers, thereby ensuring secure and efficient operations in an era where information technology is central to service delivery.

The addition of CIE aligns with General Deterrence Theory by recognizing that deterrence depends not only on the presence of sanctions and technical controls but also on the effectiveness of their implementation. This perspective highlights that poorly implemented controls fail to deter attackers even when policies appear comprehensive.

2.2 Empirical Review

A study by Pereia and Bobbert (2019) in Belgium on factors influencing cyber-security readiness looked at how effective cybersecurity practices are for industrial control systems. The study employed Design Science Research (DSR) to connect activities of the research project with design science activities. In order to ascertain the reliability of data, the Group Support System (GSS) tool was used in documenting every step, ensuring repeatability, and that all activities were time-bound. The study engaged 188 participants, including Industrial Control System (ICS) practitioners, ICS experts, and Information Security Practitioners and Executives from several industries. The study findings revealed that priority, resources, and structure greatly influenced cybersecurity readiness among employees in Belgium. Also, the study revealed further that the technology level influenced cybersecurity readiness among employees, whereas 50per cent admitted that the urge to minimize risk influenced them to tighten their cybersecurity practices.

Moreover, Ganin et al. (2020) conducted a study on the influence of cybersecurity readiness within the Gulf countries, particularly Saudi Arabia and the United Arab Emirates. This study sought

Cite paper: *Kwesigabo, E.M. & Gidion, M. (2025). Cybersecurity Readiness in Local Government Authorities: A Case Study of Municipal Councils in Tanzania's Dar es Salaam Region. Business Education Journal, vol(11), Issue 2; 10 pages.*

to trace the influence and genesis of cybersecurity measures that have taken shape in the subsequent years from 2017 within the Gulf Council Countries (GCC). Participants involved in the study included ICT experts managing large corporations. These were subjected to questions designed to find out input strategies, which they deemed fruitful in ensuring cybersecurity against attacks or external threats. The findings revealed that out of 32 respondents , 23per cent maintained that there are high chances of a cyber-attack on key documents. Therefore, their influence on cybersecurity readiness heavily hinges on securing corporate data against fraudsters from competitors.

Elsewhere, Kitena and Mshana (2022) carried out a study on cybersecurity management strategy. A qualitative research approach was adopted to collect views from respondents about mechanisms of strengthening cybersecurity measures. Their provision maintains that the move will allow the use of modern strategies, as well as approaches that are aligned with technological changes. In the study context, cybersecurity readiness is influenced by the approaches used in containing cybersecurity threats. The threats stem from malware attacks and attempts by fraudsters to access personal and organizational information within organizations (Borgman & Choo, 2019). The notion presented herein means that the Government of Tanzania can capitalize on the study findings and introduce the strategic plan for cybersecurity within LGAs.

Furthermore, several studies highlight the centrality of human factors in cybersecurity readiness. For example, Radanliev and Burnap (2021) emphasize that the human component poses a significant challenge, as it strongly influences how prepared organizations are for cyber threats. They show how risks such as weak passwords, phishing, and user negligence can undermine readiness, while a culture of vigilance and responsibility can lower the chances of successful attacks. This aligns with other scholars who stress staff training and awareness as core elements of resilience (Borgman & Choo, 2019).

Aliyu et al. (2020) conducted a study in Europe on a holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. The study was carried out to establish a framework for cybersecurity readiness among ICT personnel within the selected institution.

A case study research design was used to understand a viable framework for which data on cybersecurity can be adapted. Interviews with experts in the field of security and data protection of state officials depicted that there is a great need for the identification of different regulations that comply with the best practices that may follow how organizations manage overlap by exhibiting the best framework for cybersecurity readiness for the ensuing data protection mechanism. The findings from this study justify the focus of the current study, which seeks to assess the cybersecurity readiness of Local Government Authorities on the adoption of shared ICT infrastructure.

Emerging empirical studies increasingly emphasize the implementation gap—the difference between written cybersecurity policies and their actual enforcement. Incorporating CIE as a mediator addresses this gap by examining how implementation quality converts planned policies and infrastructures into real readiness.

3.0 Research Methodology

3.1 Study Area and Population

This study adopted an exploratory research design and employed a qualitative approach to generate deeper insights that complemented the available quantitative data. In this study, Cybersecurity Implementation Effectiveness (CIE) is treated as a mediating construct. Accordingly, data collection and analysis explicitly examined not only the presence of policies, risk controls, human-factor practices, and technologies, but also how effectively these measures are enforced, monitored, and improved over time to produce readiness outcomes. The combination of qualitative and quantitative evidence enabled a thorough examination and well-informed conclusions concerning the research problem. The research was conducted at Local Government Authority (LGA) offices in Dar es Salaam, notably in Kinondoni, Ilala, Kigamboni, Ubungo, and Temeke, focusing on ICT Departments. These departments were purposeful chosen since they are in charge of protecting and maintaining enormous amounts of data, particularly sensitive information such as people's personal information, financial records, and private government conversations. Because they are so important,

ICT departments need to have good data management and cybersecurity policies to keep LGAs running smoothly and safely.

3.2 Sampling

This study examines the population of ICT staff and system administrators working within five LGAs in Dar es Salaam. Data from Dar es Salaam region office (2023) showed that there are 128 ICT employees within the five LGA offices in Dar es Salaam. The sample size was obtained using a nonprobability sampling method where the saturation point was reached after interviewing 25 respondents from the five LGAs. The researcher used purposive sampling to select ICT employees to provide relevant information for this study. This sampling technique was instrumental in finding ICT staff within LGAs in Dar es Salaam, since the assessment of cybersecurity readiness of Local Government Authorities revolves around them. The purposive approach also ensured information-rich participation for CIE, prioritizing ICT staff who are directly involved in implementing and enforcing cybersecurity controls (e.g., policy enforcement, incident handling, configuration management), so that the mediating role of implementation effectiveness could be meaningfully assessed.

3.3 Data Collection Methods

Qualitative data were collected through interviews; only the ICT Manager and System Administrator were engaged in interviews. The interview guide included probes on the implementation effectiveness (e.g., evidence of policy enforcement, audit and monitoring routines, incident-response drills, patch/update cycles, and KPI tracking) to operationalize CIE as the mediator linking the four determinants to the overall readiness. Also, the researcher conducted a documentary review to collect secondary data. . According to Kothari et al. (2016), documentary review typically involves conceptualizing, utilizing, and assessing publicly available sources including documents. The researcher extensively review various literature sources, such as reports and journals on cybersecurity readiness and practices in different countries and institutions. The information obtained here was useful in cross-checking what was obtained from interviews. In the documentary review, special attention was paid to implementation artefacts such as SOPs, audit logs, incident reports, training attendance sheets, and change-management records as objective indicators of CIE.

3.4 Data Analysis Methods

Data analysis is a vital research process that involves meticulously examining, refining, modifying, and organizing data to uncover valuable insights, drawing conclusions, and guiding decision-making. Thematic analysis, utilizing coding, was employed for qualitative analysis. The researcher identified and put together similar ideas as codes, for which themes were formed for analysis purposes. Data extracted from the reviewed documentary were organized according to the research theme. The coding scheme explicitly captured CIE through themes such as enforcement intensity, monitoring frequency, corrective action follow-through, incident-response timeliness, and continuous improvement cycles. These CIE themes were then used to interpret how policies, risk management, human factors, and technology and infrastructure translate into cyber-security readiness via implementation effectiveness.

4.0 Findings

4.1 The Influence of Cybersecurity Policies on Cybersecurity Readiness in Tanzania.

Table 1 presents codes and themes aligned to cybersecurity policies on cybersecurity readiness within LGAs in Tanzania.

Table 1. Characteristics of Respondents Participated in the Study

CODES	THEMES
Government regulations	Cybersecurity policies
Internal policies and procedures	
Industry standards compliance	

Cite paper: *Kwesigabo, E.M. & Gidion, M. (2025). Cybersecurity Readiness in Local Government Authorities: A Case Study of Municipal Councils in Tanzania's Dar es Salaam Region. Business Education Journal, vol(11), Issue 2; 10 pages.*

Incident response plans

The data reveal that cybersecurity rules are the most important part of an organization's defence against digital attacks. When done right, these policies provide you with a means of protecting sensitive information, keeping operations running smoothly, and making sure you follow the rules that apply to you. By looking at many organizations' cybersecurity policies, the study found a few important patterns and codes that go with them. The ICT Managers from Kinondoni, Ilala, and Kigamboni Municipal Councils were interviewed, and one of the interviewee said, "*good cybersecurity policies are complex papers that cover a lot of ground and include a lot of specific rules*". Furthermore, he explained that "*these rules cover a lot of ground when it comes to corporate cybersecurity*". Another interviewee said, "*The rules of cybersecurity include data protection, network security, access control, incident response, employee awareness, compliance, and physical security*". Yet another interviewee added, "*Cybersecurity policies act as our first line of defence; without them, it would be difficult to coordinate responses or hold staff accountable."* These rules need to change as does the digital threat landscape , so they can deal with new problems and use new best practices. In a world that is becoming more digital, companies that create and keep strong, well-rounded cybersecurity policies are better able to secure their assets, keep their operations running smoothly, and gain the trust of their stakeholders (Shaaban & Athumani, 2020).

4.2 The Influence of Human Factors on Cybersecurity Readiness in Tanzania

Table 2 provides codes and themes that were formed from respondents' views and opinions towards their understanding of cybersecurity readiness.

Table 2. Codes And Themes for Human Factors Responsible fFor Cybersecurity Readiness

CODES	THEMES
Staff training and education	Human factors
User behaviour and compliance	
Insider threats	
Skills and expertise of IT personnel	

The most difficult part of being ready for cybersecurity might be human aspects. Even with the finest technology, human error is still a big weakness. According to Borgman and Choo (2019), employees can accidentally put security at risk by doing things such as falling for phishing scams, using weak passwords, or not following security rules.

According to one of the interviewees , "*Staff training and education are key components of an effective cybersecurity plan… By investing in a thorough and ongoing training program, an organization can improve its cybersecurity readiness, reduce risks, and build a culture of security awareness*". As cyber risks continue to change, it will be very important to have a watchful, well-informed workforce to protect against the digital age that is always-present and developing problems.

Furthermore, findings revealed that ongoing education fosters a culture where compliance is not merely an obligation but a valued practice. One respondent explained, *"the ongoing education ensures that staff do not just follow rules out of obligation but develop a culture where compliance is valued and practiced consistently"*. This reflects how well employees integrate security rules and best practices into their daily work. Another respondent noted, *"employees are frequently the first line of defence against cyber dangers such as phishing attacks, malware, and attempts to gain unauthorized access"*. A different participant added, *"without continuous training, even the best systems can fail because human error remains the weakest link."* Training on practical measures—such as using strong passwords, updating software regularly, and handling sensitive information carefully—was repeatedly described as vital for reducing risks and preventing breaches. As one ICT Officer put it, *"cybercriminals thrive on weak passwords or repeated use across accounts; with training, staff become more vigilant and proactive in closing those gaps."*

Cite paper: *Kwesigabo, E.M. & Gidion, M. (2025). Cybersecurity Readiness in Local Government Authorities: A Case Study of Municipal Councils in Tanzania's Dar es Salaam Region. Business Education Journal, vol(11), Issue 2; 10 pages.*

4.3 The Influence of Technology and Infrastructure on Cybersecurity Readiness in Tanzania

Findings regarding the influence of technology and infrastructure in relation to cybersecurity readiness are presented in Table 3.

Table 3. Technology and Infrastructure Codes/Themes Related to Cybersecurity Readiness

CODES	THEMES
Infrastructure sophistication	Technology and infrastructure
Security tools and software	
Data backup and recovery systems	
Network architecture	

4.4 Technology Infrastructure

Technology infrastructure forms the backbone of an organization's protection strategy. The more advanced the IT infrastructure is—both in terms of hardware and software—the better it can detect, handle, and respond to cyberattacks. Field interviews revealed that certain security solutions and software, such as next-generation firewalls, intrusion detection systems, and endpoint protection platforms, are considered as essential for maintaining a strong cybersecurity posture. The way a network is structured, particularly how it is segmented and protected, has a major impact on whether breaches spread or are contained. One interviewee described this, , *'without proper network segmentation, an attacker who breaks into one system can easily move across departments; but when the network is partitioned and layered with firewalls, it becomes much harder for breaches to spread.'* Another respondent added, *'our use of endpoint protection tools has been critical; they allow us to spot malware before it gets deeper into the system.'* These practical insights show how infrastructure sophistication directly influences the ability of an organization to contain and neutralize threats.

4.5 Software and Technologies for Security

This code is based on field interviews. Firewalls, antivirus software, and intrusion detection systems are some of the specific cybersecurity solutions that have been put in place. One of the interviewees said, *'we rely on firewalls, antivirus software, and intrusion detection systems because each of these tools plays a role in protecting digital assets, detecting threats, and ensuring that networks remain safe.'* Another participant explained that outdated systems pose a challenge, noting, *'sometimes we still have old operating systems or unsupported hardware; and without security upgrades these become easy entry points for attackers.'* These insights show that while security technologies are central to cybersecurity readiness, obsolete systems can undermine overall effectiveness.

Field interviews show that data backup and recovery solutions are a code. This has to do with cybersecurity; organizations need data backup and recovery systems to be able to deal with and respond to cyber threats. These systems improve overall cybersecurity readiness by lowering the risks of data loss, speeding up recovery, and helping with incident response operations. Another interviewee said, *'Our backup and recovery systems have saved us during attacks; without them, we would have lost critical data and struggled to resume operations.'* This highlights how practical backup measures strengthen resilience and enable faster organizational recovery when incidents occur. A cloud storage misconfiguration that accidentally makes private client financial information available to the public internet is an example.

4.6 Influence of Cybersecurity Implementation Effectiveness (CIE)

The analysis revealed that the presence of strong policies, rigorous risk management, capable human resource, and modern infrastructure alone do not ensure readiness. Their implementation effectiveness—measured by the extent of enforcement, monitoring, timely updates, and incident-response drills—proved decisive. LGAs that demonstrated systematic audits, continuous training, and

prompt corrective actions reported significantly higher readiness. One interviewee stated, "*having policies and tools is not enough; what matters is how consistently we implement and monitor them.*" Another interviewee added, "*we improved our readiness only after introducing regular audits and drills, because that forced us to put policies into practice rather than leaving them on paper*." This confirms that Cybersecurity Implementation Effectiveness (CIE) mediates the relationship between the four independent variables and overall cybersecurity readiness.

5.0 Discussion

The results underscore the mediating role of Cybersecurity Implementation Effectiveness, showing that factors such as policies or technology improve readiness only when effectively implemented. The study findings indicate that cybersecurity policies significantly impact cybersecurity readiness among Local Government Authorities. Similar findings are reported by Pereia and Bobbert (2019) who revealed that good cybersecurity policies are based on a few essential ideas: risk management, compliance, user behaviour and training, incident response and recovery, and continuous improvement. These findings imply that businesses can build a complete security system that protects them from the existing dangers and can also adapt to meet new ones. As the digital world keeps changing, it will be important to keep these themes in mind to protect sensitive data and make sure that organizations can handle cyber threats.

Managing risk is a key idea in cybersecurity policies. Cybersecurity risk management entails the identification, evaluation, and prioritization of risks, followed by the synchronized deployment of resources to mitigate or regulate the probability and consequences of detrimental occurrences. A full risk assessment is the first step in good risk management. This looks at possible threats, weaknesses, and the effects of possible security breaches. Similar observations are made by Shaaban and Athumani (2020) that policies should say how to frequently update risk assessments and change security measures as needed. This proactive approach helps businesses see and deal with any risks before they are exploited by enemies. Risk management also means using the best ways to protect data, systems, and networks, making sure that any possible weak spots are taken care of.

Radanliev and Burnap (2021) also observe that the human component is a big problem because it has a big effect on how ready people are for cybersecurity. They show the kinds of potential cyber risks , how hackers work, and how to stay safe online. Organizations may greatly lower the risks of successful assaults and ensure that occurrences are dealt with quickly and effectively by encouraging a culture of alertness and responsibility. As reported by Borgman and Choo (2019) a Verizon investigation found that 81per cent of hacking-related incidents used stolen or weak passwords. This number shows how important it is to follow best practices for password management and other things users do to keep their computers safe.

Ma (2020) also says that technology and infrastructure affect cybersecurity readiness mostly by providing cybersecurity solutions such as firewalls, antivirus software, intrusion detection and prevention systems, endpoint protection platforms, and security information and event management (SIEM). These are all necessary for building a strong and effective cybersecurity posture. A similar view is provided by Versify (2019) who argues that the best ways to back up and restore data it not only protecting them but also making a company more resistant to new cyber-attacks. As cyber threats keep getting worse, data backup and recovery systems will become even more important for maintaining cybersecurity readiness. This shows how important it is to be vigilant and keep changing these important habits.

6.0 Conclusion and Recommendations

6.1 Conclusion

The evaluation of cybersecurity readiness among Local Government Authorities (LGAs) in Tanzania provides significant insights into the existing level of preparedness and obstacles encountered in the implementation of shared government ICT infrastructures. First, the report shows how important it is for governments to be ready for cyberattacks as more of their services are shifted to online platforms.

As Tanzania's LGAs move toward using common ICT infrastructures, strong cybersecurity measures are more important than ever before. The fact that these infrastructures are shared creates both chances for efficiency and risks of possible weaknesses that need to be fixed. Crucially, the study demonstrates that Cybersecurity Implementation Effectiveness (CIE) is the linchpin through which policies, risk management, human factors, and technology and infrastructure translate into actual readiness.

The study shows that different LGAs are ready for cybersecurity at different levels. Some authorities take a proactive approach to cybersecurity by putting in place thorough plans and injecting money into the resources they need. However, others are still lagging behind and are having trouble with things such as awareness, expertise, and how to use their resources. This difference shows how important it is for all LGAs to have a common way of managing cybersecurity to secure government data and systems uniformly. A major result is that training and education for personnel are very important for improving cybersecurity readiness. LGAs that put a lot of effort into ongoing training for their workers are better prepared to deal with cyber risks. This highlights the human aspect of cybersecurity and the necessity of fostering a culture of security awareness within enterprises.

6.2 Recommendations

Based on what the study found, here are some suggestions for policymakers. People who determine policies should create a National Cybersecurity Framework for LGAs by making a complete, standardized framework that lists the best practices, protocols, and regulations for LGAs when it comes to cybersecurity. This framework should follow national and international cybersecurity standards and be updated often to deal with new threats.

Also, policymakers can push for more money to be spent on cybersecurity by asking for more money to be spent on cybersecurity measures. This should include expenditures in technology, hiring and training staff, and regular security checks.

Finally, the paper says that policymakers should set up regular, thorough, and required cybersecurity training for all LGA employees. These should include basic security awareness, how to spot threats, how to respond to incidents, and security duties that are specific to each function. Strengthen Cybersecurity Implementation Effectiveness (CIE) by institutionalizing regular security audits, automated compliance checks, and clear performance indicators to ensure that policies and technological safeguards are not only adopted but fully operationalized.

Reference

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Lei, L., & Boiten, E. (2020). A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. *Applied Sciences*, 10(10), 3660. https://doi.org/10.3390/app10103660

Borgman, B., & Choo, K. (2019). Cybersecurity readiness in the South Australian government. Computer Standards and Interfaces, 1-8. Retrieved May 9, 2024, from https://doi.org/10.1016/j.csi.2014.06.002

Dube, D., & Mohanty, R. (2020). Towards development of cybersecurity maturity model. *International Journal of Business Information Systems,* 3(1), 23-25. https://doi.org/10.1504/IJBIS.2020.10014790

Ganin, A., Quach, P., Panwar, M., Collier, Z., Keisler, J., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. Risk Analysis, 183-199. https://doi.org/10.1111/risa.12891

Global Militarization Indices. (2020).

Gorwa, R., & Smeets, M. (2019). Cyber Conflict in Political Science. A Review of Methods and Literature. 19-20.

Kitena, A., & Mshana, J. (2022). Factors Influencing Implementation Of Information Security System In Public Organizations: A Case Of Dar Es Salaam City Council.

Kothari, A. N., Arffa, M. L., Chang, V., Blackwell, R. H., Syn, W. K., Zhang, J., ... & Kuo, P. C. (2016). Osteopontin—a master regulator of epithelial-mesenchymal transition. *Journal of Clinical Medicine*, 5(4), 39.

Cite paper: *Kwesigabo, E.M. & Gidion, M. (2025). Cybersecurity Readiness in Local Government Authorities: A Case Study of Municipal Councils in Tanzania's Dar es Salaam Region. Business Education Journal, vol(11), Issue 2; 10 pages.*

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527.

Kweka, J., & Sooi, F. (2022). The Role of Innovation and Technology Upgrading on Industrial and Export Competitiveness in Tanzania. REPOA, Dar es Salaam. Retrieved from https://www.repoa.or.tz/wp-content/uploads/2023/06/The-Role-of-Innovation-and-Technology-Upgrading-on-Industrial-and-Export-Competitiveness-in-Tanzania-Report-Web-Ready-.pdf

Ma, R. (2020). The effectiveness of Britain's Cybersecurity. San Francisco: San Francisco State University.

Maimon, D. (2020). Maimon, D. (2020). Deterrence in cyberspace: An interdisciplinary review of the empirical literature. *The Palgrave handbook of international cybercrime and cyberdeviance*, 1-19.

Paganini, P. (2021). Reading INTERPOL, The African Cyberthreat Assessment Report 2021. Lyon: World Press. Retrieved from https://cybersecurityworldconference.com

Manda, P. A., & Mkhai, E. (2016). ICT access and use in local governance in Babati town council, Tanzania. *University of Dar es Salaam Library Journal*, *11*(2), 93-103.

Pereia, A., & Bobbert, Y. (2019). Cybersecurity Readiness: An Empirical Study of Effective Cybersecurity Practices for Industrial Control Systems. *Scientific Journal of Research and Research Reviews*. https://doi.org/10.33552/SJRR.2019.02.000536

Radanliev, P., & Burnap, P. (2021). Epistemological equation for analysing uncontrollable states in complex systems: quantifying cyber risks from the internet of things. *Review of Social network Strategies*, 381-411. https://doi.org /10.1007/s12626-021-00086-5

Shaaban, S., & Athumani, H. (2020). Assessing Strategies to Create Cyber Security Awareness among Employees of National Microfinance Bank in Tanzania. *International Journal of Economics, Commerce and Management*, VIII (12), 250-259. Retrieved April 17, 2024 from https://ijecm.co.uk/wp-content/uploads/2020/12/81214.pdf

Tanzania Communications Regulatory Authority (TCRA). (2022). Annual Report on Cyber Security. Retrieved from TCRA website.

Tanzania Cyber Security Task Force. (2023). Cyber Security Assessment of Local Government Authorities in Tanzania. Dar es Salaam: Tanzania Cyber Security Task Force

URT. (2022). President's Office Public Service Management and Good Governance: Government Cyber Security Strategy. Dodoma.

Versify. (2019). How to identify a cyber-security asset. Retrieved April 19, 2024, from http://www.versify.com/how-do-i-define-a-cyber-security-asset/

Cite paper: *Kwesigabo, E.M. & Gidion, M. (2025). Cybersecurity Readiness in Local Government Authorities: A Case Study of Municipal Councils in Tanzania's Dar es Salaam Region. Business Education Journal, vol(11), Issue 2; 10 pages.*