Bima Journal of Science and Technology, Vol. 8(4B) Jan, 2025 ISSN: 2536-6041

DOI: 10.56892/bima.v8i4B.1191

Impact of Teaching Cybersecurity Professional Courses for Students of Higher Learning Institutions: What Should the Society Expect?

Anold S. Nkata*

Department of Information and Communication, Arusha Technical College, P.O. Box 296, Arusha -Tanzania

Corresponding Author: anold.it2008@gmail.com or ankata@atc.ac.tz

ABSTRACT

The evolution of science, technology, and innovation (STI) characterized by digital transformation has significantly increased cybersecurity threats in socio-economic activities across the globe. The cybersecurity index of the global year 2024 outlines that the economy of developing countries will be affected by cyber criminals who are rapidly increasing worldwide. Globally, cybercriminals are constantly innovating their skills of attacking and hacking information systems. This study examined the problem in Tanzania by assessing the impact of teaching professional cybersecurity courses for students pursuing higher education who later graduate and live without employment. Findings reveal that the nation produces cybersecurity professionals who graduate yearly with sophisticated cybersecurity skills. The study recommends that the government should take precautions to protect itself economically and set a professional cybersecurity policy of identifying and registering students graduating in the field of cybersecurity. Moreover, public training and awareness of cybercrime Acts, and infringements are highly needed for the citizens. This study serves as a knowledge gap for education policymakers, education institutions, and the government to take measures to safeguard the nation's future digital economy by enhancing cybersecurity awareness among the citizens through the provision of education using mass media and training via various education platforms.

Keywords: Cybersecurity Awareness, Cybersecurity Threats, Cybercriminals, Cybersecurity Professionals Courses.

INTRODUCTION

Globally, the practice of teaching cybersecurity courses and programs has gained popularity in this era of cyberspace due to the tremendous change in digital transformation (Chongrui et al. 2019). In the context of business, cyberspace has fundamentally transformed the technology of socio-economic activities in terms of the way people interact, communicate, trade, and deliver customer value.

Trading of e-commerce and mobile commerce technology has resulted in cybercriminals bringing cybersecurity threats to the socio-economic activities of the citizens (Gilliard et al. 2024). The term cybercrime does not contain a universal definition; however, the term can be well described as a criminal activity performed by cybercriminals using any information technology-related tools and systems(Chipwaza and Semlambo 2024). Worldwide, higher learning institutions,

DOI: 10.56892/bima.v8i4B.1190

education scholars, and information system professionals have immersed themselves in the field of cyberspace by conducting training in cyber security courses. Most of these training courses are based on how to protect the organizational IT system from cyber-attacks, based on three tenets of information systems such as confidentiality, availability, and integrity.

However, a few of the learning contents emphasize how to protect themselves from cybercrimes, protect others' privacy, and the basics of social and ethical issues in computing which are based on intellectual property rights and copyrights (URT-Cyber Security Strategies, 2022). Well, due to the transformation of socio-economic activities which are mostly done online, and the lack of employment facing a high number of graduates, some of them have been misusing their professional skills by doing unethical issues related to cybercriminals (Mwananchicommunication 2023).

In Tanzania, most universities and colleges have been admitting students to pursue diploma and bachelor degrees in cybersecurity. Students have been taught and imparted sophisticated knowledge, IT security skills, and various mechanisms used by cybercriminals in exploiting the security of Automated Teller Machines (ATM) of bank systems, and other IT systems. The training programs impart sophisticated skills to students in attacking information systems using web injection tools such as SQL injection Cross-*Site Scripting* (*XSS*) and other modern network tools. Students graduating in the field of cyber security are proficient experts in creating malicious software that can steal sensitive information and cause backdoor attacks, phishing, and zero-day attacks. This situation has brought security fear to users of Automated Teller Machine (ATM) of Banks and mobile money services (Mbogoro and Masele 2020). In May 2023, the University of Iringa decided to expel more than fifty students from their studies after two hundred and fifty-six students who were studying IT courses attempted to hack the University students' management systems used to keep records of students' fee payments and examinations results (Tanzaniaweb.Live 2023).

Application of cybersecurity tools like Metasploit, Nmap, and Wireshark is now common to students pursuing cybersecurity programs (TCRA 2024).In Tanzania, most of the socio-economic activities are done online (Tan 2014). Payments for various services and goods are also done through mobile banking application systems and mobile phones. Moreover, the government effectively generates public revenues through an electronic tax collection system done through control numbers. Due to the lack of employment opportunities and financial support for cybersecurity graduates, society has to expect an increased number of new kinds of cyberattacks who are knowledgeable about keyloggers.

Social engineering cyberattacks are the most dominant types of cyberattacks affecting the socio-economic activities of Tanzanian citizens compared to the other types of cyberattacks (Mhina and Nsombo 2023).

A social engineering attack is a type of cyberattack that manipulates the psychological minds of users of a system to trick them into making security mistakes or giving them sensitive information such as passwords (Manske 2000). Due to an increasing number of mobile device users who are doing mobile money transactions, e-banking, and online trading, the number of social engineering attackers is also increasing.

DOI: 10.56892/bima.v8i4B.1190

Without effective measures accompanied by training and cybersecurity awareness among Tanzanian citizens, social engineering attacks characterized by spear phishing are going to affect the socio-economic activities and the national economy in the future (Pallangyo 2022).

LITERATURE REVIEW

This section investigates research reports of an increased number of cybercrimes in the globe. The study critically examines the rapidly emerging trends of cybercriminals in Tanzania specifically for the users of mobile phones, mobile money services, mobile application bank systems, and ATMs. Also, the study examined reports and cyber cases of cyberattacks in the sectors of education specifically in higher learning education institutions. Moreover, it evaluates the modern technology used by cybercriminals to hack information systems and its impact on socio-economic activities in developing countries.

Various research studies show that the statistical rate of cybercriminal cases has been increasing day after day across the globe (Luis et al. 2024; Mabrouk 2020). A study by (Ntembo and Casimir 2023), shows that digital transformation has resulted in an increasing number of cybercrimes in Tanzania. This situation has a direct impact on socio-economic activities especially in this era of blockchain technology whereby most people are training online (Msengi 2024). With the growth of digital technology, cybercriminals are constantly innovating their skills in attacking information systems (Burov 2020). In the year 2020, a young male student of seventeen years old from the UK implemented a fake website that sold a fake gift of vouchers by impersonating love2shop and he eventually generated six thousand pounds of shillings within a short period (Collier 2022). To attract more customers, the guy purchases a Google advert to allow his website to appear at the top of search pages on top of the genuine sites. After the police investigation, the cybercriminal acknowledged that the sophisticated skills he applied to commit offenses were acquired from school when he was studying IT security (Collier 2022).

On April 18, 2024, the UK Metropolitan Police Service, in cooperation with the European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT) managed to shut down the website called LabHost created by university students to genera funds for boosting their income (Peters & Jordan 2020). This website implemented the LabRat tool to offer two-factor authentication (2FA) services to cybercriminals. The website existed for three years from 2021 to 2024 whereby and it operated as a ''Phishing-as-a-Service (PhaaS) provider''. It mainly targeted organizations of high profiles, service providers, and big financial institutions around the world to generate income. However, up to April 10th, 2024, the UK was at number eight for the leading country of cybercrime cases in the world (CybercrimeIndex 2024). Russia, Ukraine, China, the USA, Nigeria, and Romania were the world's leading countries in cybersecurity threats (CybercrimeIndex 2024).

The police task force in Tanzania has reported several cases of cybercriminals (Oreku, 2021). Most of the reported cybercriminals of bank institutions seem to be ICT professionals (Mwananchi 2024). A study conducted (Kayumbe and Michael 2021) shows that small and medium Business enterprises (SMEs), financial institutions, and telecommunication companies offering

DOI: 10.56892/bima.v8i4B.1190

mobile bank services are mainly targeted by cyberattacks and are at risk (Kayumbe and Michael 2021).

In developing countries like Tanzania, cybercrime cases are increasing rapidly due to unemployment and low income (Moses, Aloyce Semlambo, and Paulo Sabaya 2023). Users of mobile phones are pre-cautioned to be careful and stay away from socio-engineering activities (Pallangyo 2022). Social engineering attacks are the leading attacks targeting users of mobile phones (Muzigura and Casimir 2023). Social engineering attacks are the kinds of attacks whereby cybercriminals use a psychological mind to trick users into making security mistakes and providing sensitive data such as access credentials such as passwords or PINs for mobile services (Naz et al. 2024).

MATERIALS AND METHODS

This study reviewed various cybercrime cases that happened around the globe and in Tanzania by evaluating the factors or motives that drive them into cybercriminal activities. The study systematically reviewed cybercrime reports and scholarly works in Tanzania by assessing the professionalism of cyber attackers by reversing the technology used by cyber attackers to compromise the security of information systems. To ensure the reliability and validity of the findings, the study reviewed cybercrime reports and scholarly works that happened in Tanzania within five years, from 2019 to 2024.

In this case, the study had two research questions. The first research question was to examine on; what are the motives and driving forces that lead to an increase of cyber criminal' cases across the globe. The second research question is on which kind of technology cybercriminals most use to compromise the security of an information system.

Sampling Techniques

To answer the first research question, the study purposely investigated the reported cases of cybercriminals of financial interest compared to other cybercriminal cases. Moreover, to answer the second research question, the study used purposely sampling techniques to review the technology used by cyber criminals to compromise the security systems of information systems to examine the professionalism used by cyber attackers whether is due to the application of IT security tools and computing technology or not.

Ethical Consideration

The study considered all ethical issues and demographic information while carrying out this study. All related works of scholarly used in this study were cited and acknowledged. The reported cybercrime cases were taken under study considerations use and not otherwise.

RESULTS

This part of the research article presents the interpretation of the findings. To address the objective of the study to draw conclusions and recommendations for the future sustainable development of Tanzania and the world in general, the study systematically discussed the findings of each cybercrime case reviewed and contributed a knowledge gap to the education policymakers to implement the strategic solution of dealing cybersecurity challenges in socio-economic activities.

DOI: 10.56892/bima.v8i4B.1190

Assessment of Cybercrime Cases Across the Globe from the Year 2018-2024.

The incidents of cybercrime in both developed and developing countries have been increasing due to the rapid advancement of science, technology, and innovation which has transformed people in the way they communicate, conduct transaction business, and how people socialize (ITU 2024). The acceleration of cybercriminal incidents increased more during the global lockdown when people opted to use the internet to work and trade online to avoid social contact (Wolff,2023).

During COVID-19, cybercrimes severely brought organizations into financial stress (Schotte and Abdallaert 2023). Distributed denial of services (DDoS) attacks, ransomware, backdoors, and social engineering were the most dominant types of cyber attackers during the period of the pandemic (Nallainathan 2021). In Tanzania, social engineering attacks incidents of cybercrimes increased during the pandemic due to remote working facilitated by mobile phones exchange of information and business transactions (Chipwaza and Semlambo 2024). This shows that changes in the socio-economic activities of citizens done online rapidly motivate cybercrime.

Assessment of Cybercrime Trends in Tanzania

In Tanzania, cybercrime cases are increasing daily due to an increase in users of online services and mobile banking services (Massawe and Mshana 2023). Mwananchi Communication Ltd reported that a total of Tsh 5.067 billion was stolen by cybercriminals in 2023 from the users of mobile money services, and ATM bank services (Cummunication 2024). The status of cybercrimes in Tanzania has been a threat to socio-economic activities where financial transactions of goods and services are done through mobile bank systems and mobile money services (Chipwaza and Semlambo 2024).

Most Tanzanian citizens are not trading online due to the high fear of cybersecurity threats (Oreku 2021). An increase in cybersecurity threats in Tanzania has not only affected the socio-economic activities but also the national income that is generated from the tourism sectors (Pallangyo 2022). Despite the efforts of government, agencies, and individual efforts of users of digital systems, cybersecurity awareness, and training are highly needed for Tanzanian citizens to match with the technological trends of the modern emerging cybercriminals.

Assessments of the Technology Used by Cybercrimers to Breach the Security of Information Systems

Change in science, engineering, technology, and innovation (SETI) has resulted in innovations of sophisticated skills used by cybercriminals in breaching security systems for the users of mobile money, the internet, and the mobile application of bank services. In Tanzania, cybercriminals are daily innovating their skills by breaching the security systems for users of mobile money and bank services. Phishing kind of cyber-attacks and other social engineering attacks such as spear phishing, baiting, ransomware malware, pretexting, quid pro quo, vishing and water-holing, and tailgating are the common cyber-attacks for mobile money transactions in Tanzania (Muzigura and Casimir 2023). Various measures have been taken by Tanzania telecommunication companies in cooperation with the cybercrime

DOI: 10.56892/bima.v8i4B.1190

investigation unit of Tanzania police to combat this kind of cyberattack (Massawe and Mshana 2023).

Despite these efforts, this shows that most people in Tanzania still don't have education regarding the ethical use of cyber technology.

Assessment of the Motives and Driving Forces of Cybercrime in Tanzania

The lack of employment opportunities for cybersecurity graduates and the desire to be rich without proper strategic efforts to work is the driving force behind an increase in cybercrime cases in Tanzania (Ntembo & Casimir, 2023). In Tanzania, employment opportunities have been a big challenge to the young citizens graduating from higher learning education.

The number of students graduating with different professional skills in the field of computing technology and information system security is increasing yearly (Mwananchimagazine 2024). Students graduating in the field of computing have the potential opportunity to apply their acquired skills in fighting against cybercrimes. However, due to the lack of employment opportunities, there is a high possibility of turning their potentially acquired educational skills into bad use in cyberspace.

DISCUSSION

Based on the above review of cybercrime cases, it is clear that most cybercrime cases are due to professional cybersecurity experts. Due to digital transformation, and the lack of employment opportunities for cybersecurity professionals graduating yearly in computing, cybercriminals are expected to increase. However, some people have engaged in cyber criminal activities without proper knowledge and education about the ethical use of the internet, and mobile phones, and the consequences of cyber infringements.

CONCLUSION

Despite the current efforts and measures undertaken by the government in fighting against cybercrimes, cybercrime cases will keep increasing in Tanzania and across the globe. In this respect, this study concluded by recommending that, the government has to effectively use the mass media communication systems to provide public training about the impact of cybercrime on socio-economic activities for sustainable development of the nation. Education about the ethical use of the Internet should be provided to the students in primary and secondary schools. Graduates of professional cybersecurity courses should be registered and monitored by regulatory bodies of communication authorities in the country. Moreover, the nation's cyber acts stipulate the rules and guidance about the improper use of the internet and other digital tools should be educated to society.

REFERENCES

Chipwaza, C. S., & Semlambo, A. A. (2024). Impact of Remote Work Technology on Employee Performance: A Case of Dodoma University, Tanzania. *Educational Research (IJMCER),* 6(2), 143–150. *https://www.academia.edu/download/*112793206/IJMCER_l0620143150.pdf

Chongrui, L., Zhiqiang, W., Cong, W., Das, R., & Sandhane, R. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity

Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *Journal of Physics: Conference Series*. https://doi.org/10.1088/1742-6596/1339/1/012098

Burov, Oleksandr. 2020. "Cybersecurity and Innovative Digital Educational Environment." *Information Technologies and Learning Tools* 80(6):414–30. doi: 10.33407/itlt.v80i6.4159.

Chipwaza, C. S., and A. A. Semlambo. 2024. "Impact of Remote Work Technology on Employee Performance: A Case of Dodoma University, Tanzania." *Educational Research (IJMCER)* 6(2):143–50.

Chongrui, L., Zhiqiang, W., Cong, W., Das, R., & Sandhane, R. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *Journal of Physics: Conference Series*. https://doi.org/10.1088/1742-6596/1339/1/012098

Collier, Ben. 2022. "A 'Sophisticated Attack'? Innovation, Technical Sophistication, and Creativity in the Cybercrime Ecosystem." *Workshop on the Economics of Information Security* (June 2022).

Communication, Mwanachi. 2024. "Police-Tanzanians-Lost-Sh5-Billion-to-Cyber-Fraud-in-2023-4703676 @ Www.Thecitizen.Co.Tz."

CybercrimeIndex. 2024. "World-First-Cybercrime-Index-Ranks-Countries-by-Cybercrime-Threat-Level @ Www.Unsw.Edu.Au."

Gilliard, Ezekia, Abdul Maziko, Gideon Rwechungura, Ahmed Abubakar Aliyu, and Erasto Kayumbe. 2024. "Protecting Africa's Future: Cybersecurity Strategies for Child Safety, Learning, and Skill Acquisition in Tanzania."

ITU. 2024. "The Latest 2024 Cyber Crime Statistics (Updated July 2024)."

Kayumbe, Erasto, and Lucy Michael. 2021. "Cyberthreats : Can Small Businesses in Tanzania Outsmart Cybercriminals ?" *International Research Journal of Advanced Engineering and Science* 6(1):141–44.

Luis, Mgs, Antonio Villalta, Mgs Leonardo, Orleans Labre, Mgs Adriana, Mercedes Villalta Gavilanes, Dra Cecilia, Teresita De Jesús, and Carbajal Llauce. 2024. "Computer Crime in the Digital Age Literature Review of Scientific Articles From 2019 to 2024." *Journal of Ecohumanism* 6798:6439–48.

Mabrouk, Fatma. 2020. "Statistics of Cybercrime from 2016 to the First Half of 2020." *International Journal of Computer Science and Network* 9(5):252–59.

Manske, Kurt. 2000. "An Introduction to Social Engineering." Pp. 1–7 in *Information Systems Security*. Vol. 9.

Massawe, Edgar Rogart, and Juma Ally Mshana. 2023. "Preventing and Combating Cybercrimes: Case of Cybercrimes Investigation Unit of Tanzania Police." *European Journal of Theoretical and Applied Sciences* 1(5):1179–90. doi: 10.59324/ejtas.2023.1(5).102.

Mbogoro, F. .., and J. J. Masele. 2020. "Adoption of Cash Deposits through Automated Teller Machines (ATMs) by Banks in Tanzania: A Case of Selected Commercial Banks in Dar Es Salaam." *Business Management Review* 24(1):71–86.

Mhina, Julius Raphael Athuman, and Andrew

Justo Nsombo. 2023. "Assessment of the Effects of Access Control on Reducing Cybercrimes in the Selected Telecommunication Companies in Tanzania." *The Journal of Informatics* 3(1):34–50. doi: 10.59645/tji.v3i1.134.

Moses, Nkinde, Adam Aloyce Semlambo, and Dinael Paulo Sabaya. 2023. "The Impacts of Cybercrime on the Growth of Mobile Money Services in Tanzania; A Case of Kongwa District." |*International Journal of Business Management* 06(11):42–63.

Msengi, Ismail Emmanuel. 2024. "East African Journal of Law and Ethics The Role of Law Enforcement in Combating Financial Cybercrime in Tanzania : Examining the Laws and Practice." *East African Journal of Law and Ethics* 7(1):202–13. doi: 10.37284/eajle.7.1.2497.

Muzigura, Goodluck, and Respickius Casimir. 2023. "Evaluation of Measures Taken by Telecommunication Companies in Preventing Social Engineering Attacks in Tanzania." *European Journal of Theoretical and Applied Sciences* 1(4):1248–59. doi: 10.59324/ejtas.2023.1(4).114.

Mwananchi. 2024. "Wizi-Wa-Mtandao-Unavyozigharimu-Benki-Duniani-2776748 @ Www.Mwananchi.Co.Tz."

Mwananchicommunication. 2023. "Sintofahamu-Wanafunzi-Kuingilia-Mfumo-Uoi-Kujilipia-Ada-Kinyemela-4248024 @ Www.Mwananchi.Co.Tz."

Mwananchimagazine. 2024. "Tatizo-La-Ajira-Kwa-Vijana-Latakiwa-Kupewa-Kipaumbele-Kuepuka-Yasiyofaa-4687134 @ Www.Mwananchi.Co.Tz."

Nallainathan, Senthuran. 2021. "Analysis of the Evolving Cyber-Attack Trends during COVID-19 Pandemic." *International Journal of Science and Research (IJSR)* 10(4):139–44. doi: 10.21275/sr21403140109.

Naz, Anam, Madiha Sarwar, Muhammad Kaleem, Muhammad Azhar Mushtaq, and Salman Rashid. 2024. "A Comprehensive Survey on Social Engineering-Based Attacks on Social Networks." *International Journal of Advanced and Applied Sciences* 11(4):139–54. doi: 10.21833/ijaas.2024.04.016.

Ntembo, Faraj Nyuda, and Respickius Casimir. 2023. "The Driving Forces for the Involvement of Higher Learning Institution's Students in Cybercrime Acts. A Case of Selected Higher Learning Institutions in Tanzania." *European Journal of Theoretical and Applied Sciences* 1(4):911–22. doi: 10.59324/ejtas.2023.1(4).86.

Oreku, George S. 2021. "A Rule-Based Approach for Resolving Cybercrime in Financial Institutions: The Tanzania Case." *Journal of The Open University of Tanzania* 27(1):130–42. doi: 10.4324/9780203018569-18.

Pallangyo, Hakeem J. 2022. "CyberSecurity Challenges, Its Emerging Trends on Latest Information and Communication Technology and Cyber Crime in Mobile Money Transaction Services." *Tanzania Journal of Engineering and Technology* 41(2):189–204. doi: 10.52339/tjet.v41i2.792.

Peters, Allison, and Amy Jordan. 2020. "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime." *Journal of National Security Law and Policy* 10(3):487–524.

Schotte, Tamara, and Mercedes Abdallaert.

DOI: 10.56892/bima.v8i4B.1190

2023. “The Impact of the COVID-19 Pandemic on the Serious and Organised Crime Landscape: The Impact of the COVID-19 Pandemic on the Serious and Organised Crime Landscape: Assessing the Evolution of Serious and Organised Crime during COVID-19 through the Enterprise.” *An Introduction to European Law* 113–14. doi: 10.1017/cbo9781316278314.008.

Tanzaniaweb.Live. 2023. “Wanafunzi-Wa-IT-Wadukua-Mfumo-Wa-Ada-Iringa-729575 @ Www.Tanzaniaweb.Live.”

TCRA. 2024. “TZ-CERT HONEYPOTS WEEKLY REPORT Period : 23.” 23(October 2024):9–11.

URT-Cybersecurity Strategies. 2022. `` *Government Cybersecurity Strategy 2022 – 2027 Microsoft Account @ Copyright 2022 Po-Psmgg. All Rights Reserved. Government Cyber Security Strategy 2022 – 2027*.

Wolff, Josephine. 2023. “Trends in Cybercrime During the COVID-19 Pandemic.” Pp. 215–27 in *Beyond the Pandemic? Exploring the Impact of COVID-19 on Telecommunications and the Internet*, edited by J. Whalley, V. Stocker, and W. Lehr. Emerald Publishing Limited.