EJTAS
ISSN 2786-7447
EUROPEAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES
OPEN ACCESS
PEER REVIEWED

Assessing the Effectiveness of the Implementation of Cybercrimes Mitigation Strategies in Selected Commercial Banks in Tanzania

Patrice Samwel Mwita
Directorate of ICT, Tanzania Commercial Bank, Tanzania

Julius Raphael Athuman Mhina
Department of Computer Science, Faculty of Computing and Mathematics, Institute of Finance Management, Tanzania

Suggested Citation
Mwita, P.S. & Mhina, J.R.A. (2023). Assessing the Effectiveness of the Implementation of Cybercrimes Mitigation Strategies in Selected Commercial Banks in Tanzania. *European Journal of Theoretical and Applied Sciences, 1*(6), 571-583.
DOI: 10.59324/ejtas.2023.1(6).58

Abstract:

This study aimed to assess the effectiveness of implemented cybercrime mitigation strategies for commercial banks in Tanzania. Most financial sectors, like banks, are vulnerable to continuous attacks from external and internal cybercriminals such that the majority of banks spend their time updating and maintaining cybercrime mitigation strategies against cyber attacks. Despite the ongoing efforts to prevent cyber attacks the studies and experiences show that such attacks still occur regardless of the strong measures implemented against cyber attacks. It is articulated with different researchers that there is a gap to make a resilient and stronger systems against cybercrimes. This research assessed the effectiveness of cybercrime mitigation strategies by analyzing public awareness, budget allocation, support from management, and availability of skilled personnel. The study used a sample of 885 respondents from five biggest banks in Tanzania. The collected data were analyzed using descriptive statistical methods. The implications emanating from the study were discussed.

Keywords: *Cyber Crimes, Cyber Security, Mitigation, Challenges, Tanzania.*

Introduction

The rapid and tremendous growth in science and technology and its application in many ways have triggered the way institutions, especially commercial banks, operate by improving customer service delivery. According to Oluoch (2018), with the use of advanced technology, financial institutions strive to provide their services closer to the customers. The aim is to remove customer-direct contact, which wastes time and it is costly. Many African financial institutions, such as commercial banks, have positively responded to the rapid growth in the use of science and technology through service diversification, including establishing and promoting online services such as the use of mobile phone banking (checking account balance, withdrawing, depositing and requesting mini-bank statements (to mention a few). As expected, cybercriminals are not left behind. Ndulu (2012), the former governor of the central Bank of Tanzania (BOT), stated that the monthly services of sending and receiving money through mobile phones had increased up to Tsh 861.8 billion.

The increase in the volume of sending and receiving money undertaken by mobile phones should be taken into consideration by regulating the law and institutional framework to that effect to protect the banks, network operators, and customers against fraud and hackers. As argued by various authors, ICT experts are now worried about the increasing volume of money exchange through mobile transfer, and the platforms should be protected against cybercrimes.

On the other hand, the commercial banks have put mitigation strategies against cybercrimes. Some of these cybercrime mitigation strategies, according to Ubena (2010), included hiring a cybercrimes specialist to manage cyber issues integration of ant cyber security systems in banks' operation systems. Other strategies include the use of strong antivirus, strong passwords, and having in place risk-free information system management. Undertaking routine systems audits is seen as an important strategy in the management of cybercrimes in many financial institutions to date.

Despite all the cybercrime mitigation strategies in place, practical evidence indicates that cybercrimes are still one of the major threats in commercial banks' online operations today. According to Shulla (2013), commercial banks' online services are continuously hacked, resulting in many potential customers either churning from one bank to another or deregistering with online services in search of more secure financial services.

The sustenance of cybercrimes in many commercial banks in Africa, despite all the efforts in place promoted, prompted the researcher to focus the study on the assessment of the effectiveness of the implementation of cybercrimes mitigation strategies in some selected commercial banks in Tanzania.

Literature Review

This segment debates the review of literature focused on cybercrimes that occurred in financial institutions. The literature review provides an understanding of previous work done by other researchers published and reviewed in various journals, books, and reports. Cybercrime activities have been tremendously hindering online bank services with sophisticated attacks organized by professional hackers. Cyberwarfare has been causing huge chaos in the financial sector, such as data breaches, identity theft, and other white-collar crimes, resulting in huge losses to the banking industry. Due to the internet infrastructure growth, many companies and financial sectors prefer to use it for efficiency in providing services to their stakeholder, hence attracting cybercriminals to conduct illicit acts. Therefore, there must be cyber mitigation strategies be in place in case any attacks likely to happen.

Authentication Mechanism in Banking Environment

According to Council (2005), the Financial institution should use certain guidance when evaluating and implementing authentication systems. The single-factor authentication method has been considered a weak authentication, which results in account fraud and identity theft (e.g., ID/password) due to authentication exploitation. Therefore, any banking product and service required to use an authentication system should be assessed to identify the types and level of risk associated with their Internet banking application and should consider using multi-factor authentication in a situation where a high-risk transaction is involved. Another study conducted in UK banks suggested that two factors are the best mechanisms in combating password breaches and guessing attacks against remote access to financial services. In order for the factor mechanism to work the best, the researchers (Krol, 2015) suggested that to design the best multi-factor authentication system; one should reduce steps in authentications and remove unnecessary features that do not reflect security concerns.

Mobile Malware

The mobile device is used frequently in surfing the internet, doing shopping online, and conducting transactions online; however, the smartphone has become an easy link to cybercriminals by trying to deceive users into subscribing, registering, or installing fake mobile applications. As stated by Qamar et al. (2019), the popularity of Android OS is not only attracting users but also becoming a vital target for malware coders (Leopando & Zeus, 2010) because the security structure of Android is weak and many malware threats can be installed such as worm, backdoor, viruses, and Trojan. Many banks have been a victim of mobile malware attacks, especially banks that use Android OS to deploy applications; hence, the researcher suggested specific tools to detect malware, analyze applications at runtime, and apply hybrid analysis tools. Other authors, such as Shahriar (2015), discuss various phishing attacks using mobile devices and propose countermeasures such as content-based filtering, which is based on a set of rules for identifying benign and suspected phishing contents, black-listing, and white-listing. The authors still focus on user awareness of cyberattacks as a big problem, overwhelmingly among many financial institutions. Furthermore, another article by Wazid (2019) proposed mitigation for mobile banking threats by developing an awareness program that will educate banking clients and employees about various threats, installation of antivirus software, and use of strong authentication schemes, but the researcher shows the limitation of those solution like awareness program has to based not only on online/banking user but also for online/offline mode, still need strong mechanism in authenticating services and last is bank infrastructure should not be much affected by unknown anomalies such as zero-day attack. Most researchers argue that the most effective way to mitigate such attacks from ransomware or malware depends on user awareness (Nadir et al., 2018) and finance institutions to have a response unit dealing with cyber threats when they arise, and law enforcement agencies should make a platform to aid users in strength their knowledge about ransomware.

Social Engineering

This is the most dangerous attack up to date; it involves psychological manipulation of the banking customer and employee since the attacker uses human behavior to collect vital information like the security policies of a bank. Research by Airehrour (2018) conducted in the New Zealand bank sector found that 64% needed to learn, and 40% knew and expressed the issue due to a lack of good secure cyber policies. The study proposes a few solutions, such as limiting the information made available to the public, for instance, in social media, improving banking policies and practices, conducting awareness among customers against social engineering attacks, implementing a tool to detect phishing attacks, and last to improve network security, for instance, use of antivirus, data protection software, content filtering, and network monitoring tools. However, the study presented that limitations are hindering the success of preventing cyber-attacks. For example, public awareness, technical policies, and authors' suggestions are still based on education and training concerning cybercrime threats.

Information Sharing in Cyber Attack Mitigation

The investigation by Johnson (2016) reported that the best way to combat cyber-attacks is through collaboration between government organs and financial institutions on sharing information of cyber threat intelligence data better to comprehend the developing nature of complex security risk. By doing so, cyber intelligence analytics could aid both parties in detecting, mitigating, and responding to any threat. The authors suggested that in this modern cyberwarfare, the finance institution should focus more on the data and less on network security, and sharing of information is essential for both private and public sectors so as to analyze threat trends and data in a comprehensive cyber threat information database. Also, another researcher (He, 2018) reported the same thing about the importance of information sharing on cybersecurity issues among organizations, which can help to monitor and improve understanding of security problems. Even in another survey paper (Pala, 2019) explained the importance of coordination and support to help reinforce cyberattack mitigation.

Cybercrime Awareness

A study by Catota (2018) exposed the challenges that existed in dealing with cyber-attacks In the financial sector in the Ecuador zone, where it shows most banks need more user awareness, scarcity of financial and technical resources to combat the threats, and the weakness of legal frameworks. Therefore, in their study, authors suggested strong implementations of incident response strategies and established information sharing of cyber incidents. A study conducted by Malik et al. (2019) that was based on a Pakistan bank indicated that lack of security awareness imposes a great hindrance toward mitigating cybercrime threats in banks. The study made suggestions to train employees about threats on cybercrimes and educate customers concerning cyber threats in their services via real examples and real case studies. Also, a study by Tariq et al. (2013) showed that a lack of strong cyber laws and a central body to generate a response to cyber threats imposed challenges to mitigate cybercrime; therefore, most suggestions due to government inadequate and limited scope and resources they should form a framework which will aid them to strengthen law and incident response in cybercrime space. A study conducted in Vietnam by Tam et al. (2020) also shows that more than 50% of bank customers need a clearer understanding of knowledge or measures on how to prevent cybercrime. Commercial banks faced cybercrimes due to poor management, human capacity, support environment, and legal framework. In their suggestions to overcome, they proposed that banks secure their software, frequently check technical gaps and cybercrime activities, policymakers should adjust more rules and regulations in handling cybercrimes in banking sectors, and for banking technology ecosystem infrastructure should conduct training, share information and use high-quality technologies and for customers, banks should improve the knowledge and skills for their stakeholders to understand the services and use of a strong password. Moreover, another investigation by Alghazo et al. (2017) analyzed the use of Internet Banking services and investigated the perception of users and banks. The preliminary investigation was to find out the user knowledge of cyber security and common awareness of threats in Internet banks.

Cyberattack in Africa Atmosphere

As African countries are in a rush to the digital era of technology, it is a good idea to catch up and use sophisticated technology in diversity operations; however, on the other hand, it leads to exposure to cyber-attacks, which brings damage to social and politics (Yusuf, 2020). Reports (Chapman, 2018) have been published and exposed damages and concerns about Africa toward cybercrime mitigations. Kshetri and Nir (2019) listed the impact of cybercrimes, such as in bank sectors that lost huge amounts of money in cybercrimes. The causes are the usage of pirated software, poor allocation of cybersecurity budgets, the majority of users needing to be more experienced with usage of the internet services, and the language barrier because most of cybersecurity products guidance is in the English language. Finally, weak legislation and law enforcement in the bank sector need to be laxer of proper cybersecurity practices, which impose high risk from threats like hacking, insider attackers, and employees with poor intellect of security. The security measures for business and clients was to create a cyber awareness program, train employee, hire professionals, and, as an organization, invest much in cybersecurity technologies for policymakers to focus on increasing awareness of cybersecurity practices and strengthen capabilities in this area. In the study done by (Mbelli et al.,2016) concerning cyber security in South African banks, they discovered that most attacks are phishing attacks, which are identified as phishing scams and malware. The measurement proposed was to strengthen legislation and standards in cybercrime, and special organs in government should invest in this sector. They should increase awareness and education in financial institutions as well as hire experts in cybersecurity with well-structured incident response management in the organization. In another investigation by Sutherland (2017), cybersecurity was focused on government delays due to the national cybersecurity policy framework being complex, hence causing delays in implementations. A lack of priority given to cybersecurity caused even other private financial sectors to not comply with the framework. Another investigation done in a Nigeria bank by Wang et al. (2020) showed the existence of cyberattacks such as viruses, worms and phishing attacks. The researchers commented on the insignificance of investing in advanced technologies in the banks, which caused frequent attacks due to hackers using sophisticated hacking tools to conduct big attacks and needing a strong incident response team in cyber breaches after the incident has been detected.

Moreover, insufficient management support and training, as well as the presence of ineffective and compliance structure of legislation against cybercrime, are the reasons cyberattacks remain dominant. Furthermore, in another survey done in Zimbabwe, 22 selected banks concerning cyber fraud issues found that it is indeed a phenomenon. Challenges were spotted, such as inadequate advanced technology that can be used to detect cyber threats, poor cyber law, and lack of knowledge, awareness, and education regarding cyber cyberattacks. Therefore, the solution was to involve all stakeholders in discussing and implementing the measures against the cyber-attacks reported by Dzomira, and Shewangu (2014). with the increase of interconnected devices and many companies using technology for their services, they are exposed to cyber threats. Therefore, Africa should come up with a cybersecurity resilience plan by Tambo et al. (2017) there should be strong decision-making platforms and frameworks in which all stakeholders will participate and build a reliable cyber security environment for allowing them to share cyber-attack data, research, and agenda in promoting the effectiveness solution, monitoring and best practices regarding cyberattacks likewise another researcher proposed the same idea of having cybersecurity resilience program since of disbelief that cyber threat only happened to the developed world. Africa must form this program with an effective response to cyberattacks, aiming to address high-priority vulnerabilities while establishing implementations and education. In achieving this, private and public partnerships are vital for this program to be effective through sharing expertise and information (Dalton et al., 2017)

Cybercrime Ambience in Tanzania

One of the cybercrime reports published in 2010 by Ulanga (2010) showed how the legal framework of Tanzania fails to address certain issues concerning cybercrime warfare, such as the correct use and protection of users for cybercrime activities, for example, lack of suitable legislation for electronic transactions. Therefore, Tanzania has to strengthen the cyber law acts for the benefit of the country and its people. Another cybercrime analysis done by Serianu (2016) illustrated the cyber intelligence report of Tanzania that the majority of malicious activity observed came from spam email, dictionary attacks (attacks focus on password guess), Port 80, routers (MikroTik, Dlink) and web server attack especially Microsoft IIS and they went further and elaborated risk faced in finance sector such as E-commerce fraud, social engineering fraud, ATM card skimming, and spam mails all targeted in finance sectors. The survey proved to be the gap in the legal framework, lack of collaboration between the private and government sectors, Education awareness, certificated security personnel, and lack of a central organ of cybersecurity intelligence database that will act as a meeting up point of all organization to share their tactics, stay up to date with trend cybersecurity threats and technology. Even another research done by (Initiatives(IFM)) raised the same issues concerning security threats in ATM and mobile banking, mobile applications, legal framework, and cybersecurity incidence response teams and proposed solutions towards combating the threats in cyberspace, such as promoting research in cybersecurity areas.

The Conceptual framework

The theoretical reviews done above have provided an understanding of the effectiveness of cybercrime mitigation strategies done by other researchers published and reviewed in various journals, books, and reports. It is articulated by different researchers that there is a gap in achieving effective mitigation of cybercrime due to improper strategies in preventive techniques, capacity building, collaborations, and failure to recognize internal cybercrime response units in the organization structure. Furthermore, the researchers assessed the effectiveness of cybercrime mitigation strategies by analyzing language barriers, public awareness, budget allocation, support from management and the public sector (law enforcement), and availability of resources (skilled personnel).

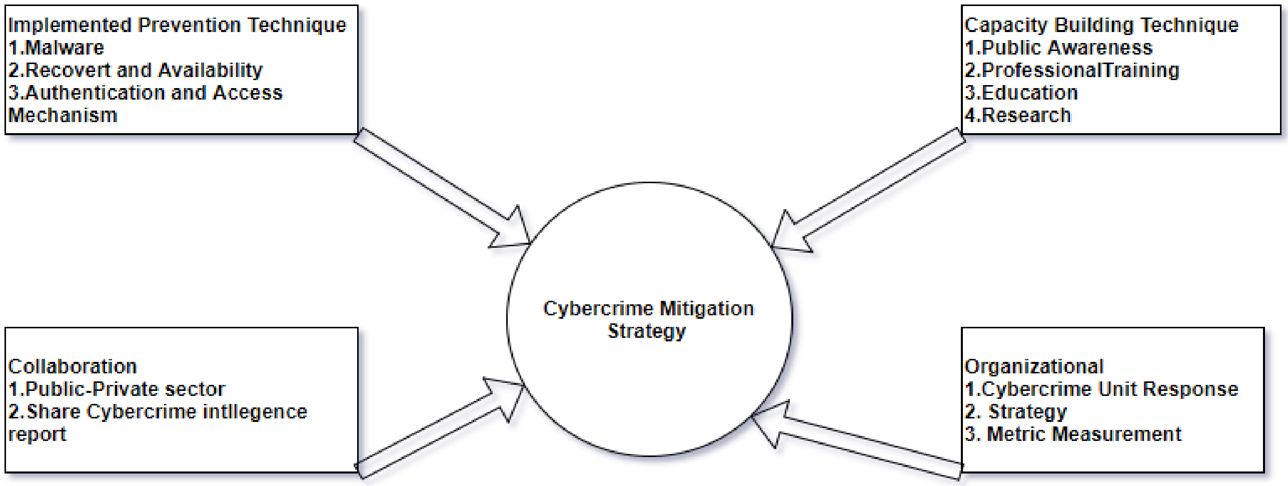
Implemented Prevention Technique
1.Malware
2.Recovert and Availability
3.Authentication and Access Mechanism
Capacity Building Technique
1.Public Awareness
2.ProfessionalTraining
3.Education
4.Research
Cybercrime Mitigation Strategy
Collaboration
1.Public-Private sector
2.Share Cybercrime intllegence report
Organizational
1.Cybercrime Unit Response
2. Strategy
3. Metric Measurement

Figure 1. Conceptualized Cybercrime Mitigation Strategies
Source: Research Data, 2023

Materials and Methods

Research Design and Approach

A research design is a framework of research methods and techniques showing how the problem under investigation will be solved. In this case, the cross-sectional research design was adopted in the study since it uses survey techniques to gather data, which is costless and time-manageable. This study adopted a cross-sectional survey across the Tanzania commercial banks, and the data collected will be used for further investigation to align with the objective of the study. In the study, the researcher will obtain data from 5 banks, and the questionnaire will be distributed to the bank's IT, legal, and HR departments and to customers and bank branch managers.

The Study Area

The study targeted five (5) commercial banks in Tanzania as its main case study.

Target Population

The population of the study is the entire group of individual subjects with a common characteristic that is the interest of a researcher. The study targeted the five commercial banks in Tanzania as its main case study. This purposive population selection technique was selected since the study was more interested in extreme cases of banks that are prone to cybercrimes and have many customers subscribed to online bank services. The 5 banks were CRDB, NMB, SCB, NBC and Stanbic bank. The respondents of this study were bank employees and customers.

Sampling Procedures and Sample Size

A sample is a sub-group deducted from the population. This sub-group will represent the whole population with the relevant characteristics. Each member in the sample is referred to as a respondent or subject. Therefore, in this study, 885 participants were selected randomly to respond to the questionnaire. The study used a purposive sampling method in selecting the respondents in each participant's banks. The respondents were bank IT specialists, HR, Bank branch managers, Legal officers, and customers. The study focused on five commercial banks in Tanzania.

A total of 195 sample sizes of bank staff will be examined in the study. Moreover, the sample size was calculated using the Raosoft Sample Size calculator (calculator, n.d.) using a 90% confidence level.

About 690 customers will be investigated in the study. The sample size was calculated using the Raosoft Sample size calculator using a 90% confidence level.

Data Sources and Collection Instruments

The study employed primary and secondary data. The primary data collection used in this study was the questionnaire. This was used for the intention of collecting primary quantitative data. The questionnaire comprised a structured questionnaire molded from the research questions and was distributed to the respondents via email and social media. The sections were organized according to the research objectives. The secondary data was obtained through magazines, newspapers, articles, books, and high-ranked journals.

Data Analysis

The finalized questionnaire was edited to check the completeness and consistency, then followed the data coding, which allowed the responses to be classified into various meaningful categories. The data collected was quantitative, and it was evaluated by using descriptive analysis methods. Moreover, with that data, further analysis was completed using MS Excel to generate reports. The researcher then presented the analyzed data in tables and figures.

Validity and Reliability

The study of this research has been subjected to validity and reliability by conducting in-depth meetings and mock sessions with professionals who are currently working in a Tanzania bank and researchers who possess in-depth experience and knowledge of the cyber city domain. The responses and contributions have helped to refine the questionnaires and structure in order to meet the research objectives. Hence, this research proved to be valid and reliable. The validity was measured based on opinions from the experts (researchers and lecturers).

Results

In this study, a total of 821 responses were received from the five commercial banks that were under investigation, with a response rate of 92.8%. According to Mugenda & Mugenda (2000), a response rate above 50% is a good fit for the study. Therefore, with confidence, this study achieved the validity and reliability of the data collected.

Response Rate

This study aimed to get 885 participants; however, 821 participants responded. 61% came from customers (504 customers), 5% from IT security (41 ICT staff), 5% from Legal Officers (37), followed by 26% from branch managers (214) and 3% from Human resources (25). The distribution of respondents per type is shown in Figure 2.

Implemented Cybercrime Mitigation Strategies

According to the study findings as shown in Figure 3, the study showed that majority of the IT Practitioners i.e. (39%) deployed malware prevention strategies, followed by 34% who used recovery and system availability, and finally by 27% who adopted access restriction strategies. The researcher attempted to highlight the mitigation strategies used by IT security experts to prevent cyberattacks, and by knowing the strategies used, it is easy to derive what types of attacks occurred. These study findings that the common mitigation strategy used was malware since commercial banks are being affected with different advanced malware with the aim to gain access to the bank's IT infrastructure followed by recovery and system availability.

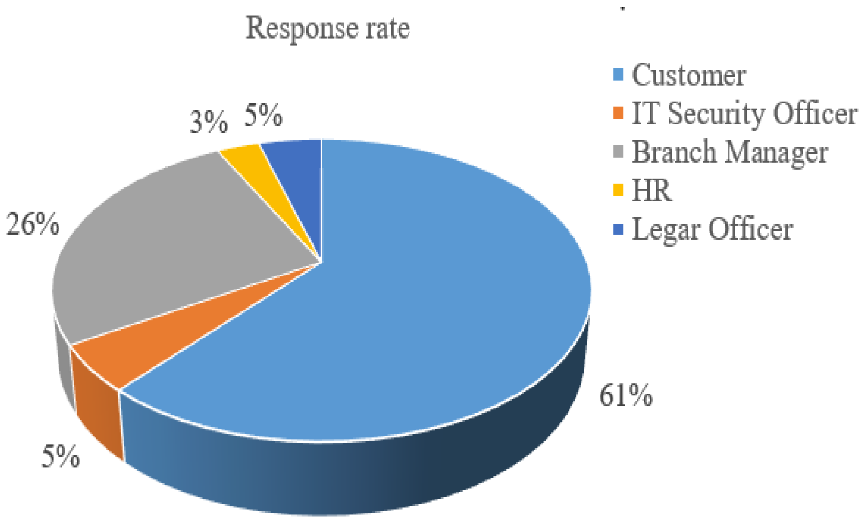

Figure 2. Response Rate
Source: Research Data, 2023

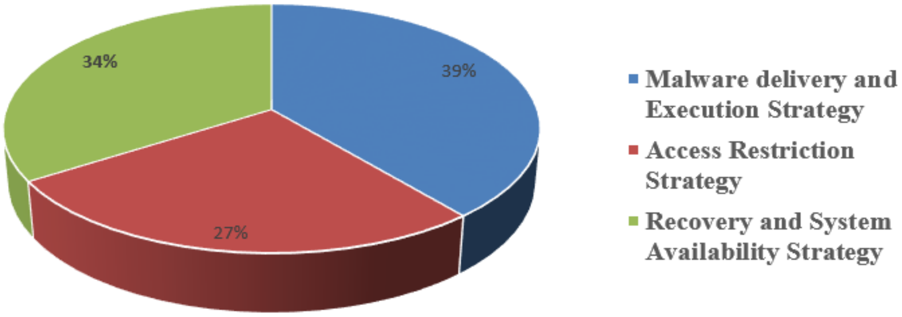

Figure 3. Implemented Mitigation Strategies
Source: Research Data, 2023

Participated Banks

From this study, the targeted banks were five, which are NMB, CRDB, NBC, STANBIC, and Standard Chartered Bank. The reasons for selecting these banks were the number of customers, popularity, and the online bank they offered, which attracted black hackers to attempt to do malicious activity. The distribution of the respondents per bank is as shown in Figure 6.

Cyber Crime Familiarity

According to study findings in Figure 8, the majority, 38%, lack knowledge about cybercrime, and very minor, about 33%, claimed to know much about cybercrime. The researcher tried to highlight that public knowledge of cybercrime can impact the effectiveness of cybercrime mitigation strategies simply if the mass does not know about cyberwarfare; hence, any strategies implemented would not yield positive results. Therefore, this study wanted to know how familiar they are concerned with the matter of cybercrime.

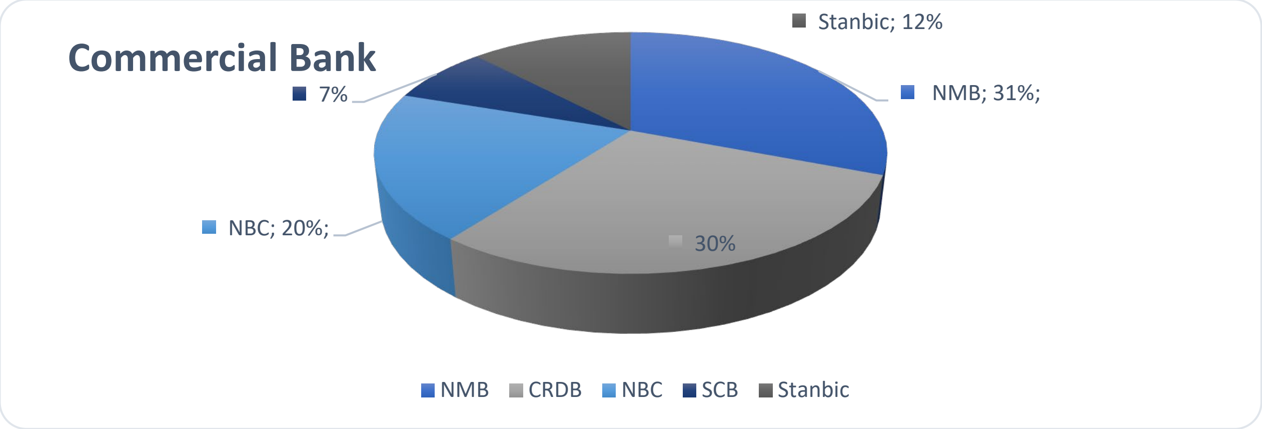

Figure 4. Response Rate
Source: Research Data, 2023

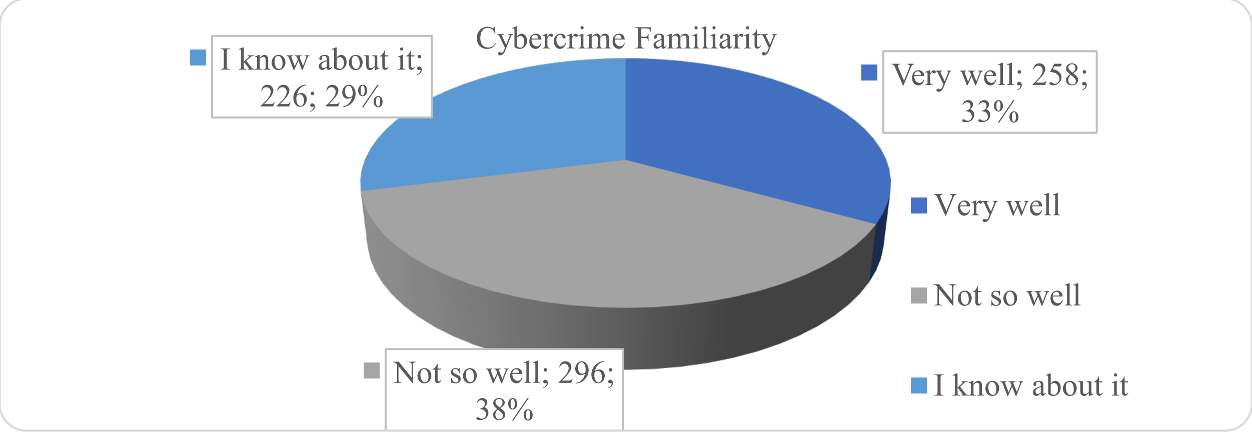

Figure 5. Cyber Crime Familiarity
Source: Research Data, 2023

Response to Effectiveness of Cybercrime Mitigation Strategies

According to study findings in the below figure, 47% of participants responded that the strength of cybercrime mitigation strategies was good, and the remaining 30% claimed to be excellent and 23% bad. The researcher focused on bank employees' and customers' views on how cybercrime mitigation techniques are performed toward mitigating cyberattacks. As the figure shows, there is a gap in achieving excellent mitigation strategies.

Other Opinions Limiting the Effectiveness of Cybercrime Mitigation Strategies

Furthermore, the study was carried out to collect opinions on how to make sure the implementation of cybercrime mitigation strategies is effectively performed and maintained. The findings were that 36% of respondents' opinion was to emphasize training and to provide awareness programs that focused on cyberspace, and 26% insisted on cultivating skilled professional employees who are well-specialized in the cybersecurity world.

15% of respondents suggested there should be management that supports and is willing to invest time and cost in cybercrime warfare—followed by 15% and 9%, whose opinions were based on increased budget and receiving support from law enforcement organs. The study validated that there is room to achieve effectiveness in implementing cybercrime mitigation strategies.

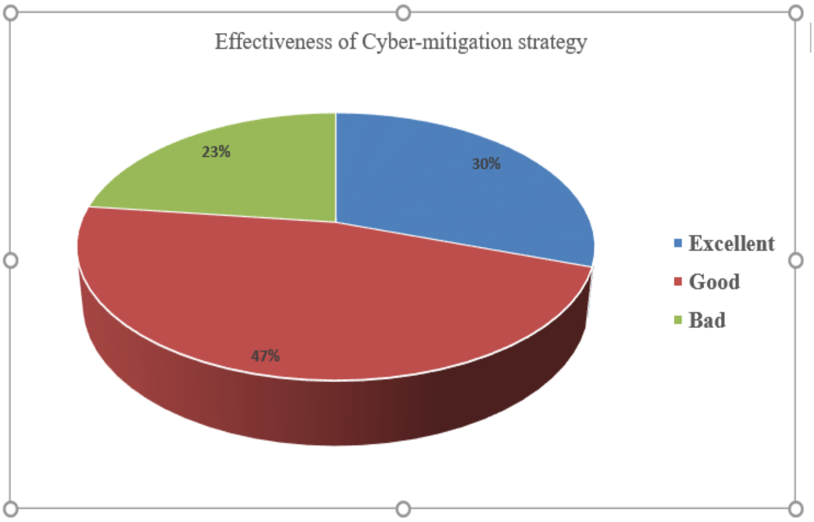

Figure 6. Effectiveness of Cyber Crime Mitigation Strategies
Source: Research Data, 2023

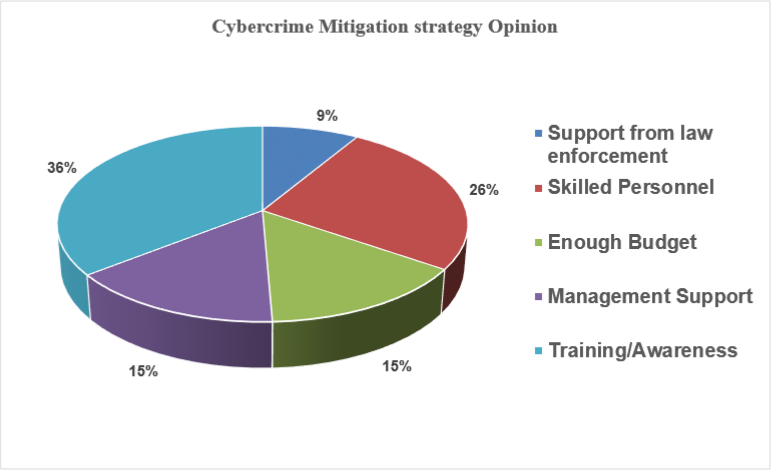

Figure 7. Recommended Cybercrimes Mitigation Strategies
Source: Research Data, 2023

Challenges Limiting the Effectiveness of Cybercrime Mitigation Strategies

The study was carried out to evaluate the challenges that hindered the effectiveness of the implemented cybercrime mitigation strategies. The findings were 36% of respondents their opinion weight on cost, 28% of respondents claimed that it be the lack of internal support (management support), and 27% of respondents agreed to the medium extent that unavailable resources such as advanced technology and skilled personnel caused mitigation strategies not to be effective. Finally, the remaining percent of respondents agreed on the lack of strong law enforcement.

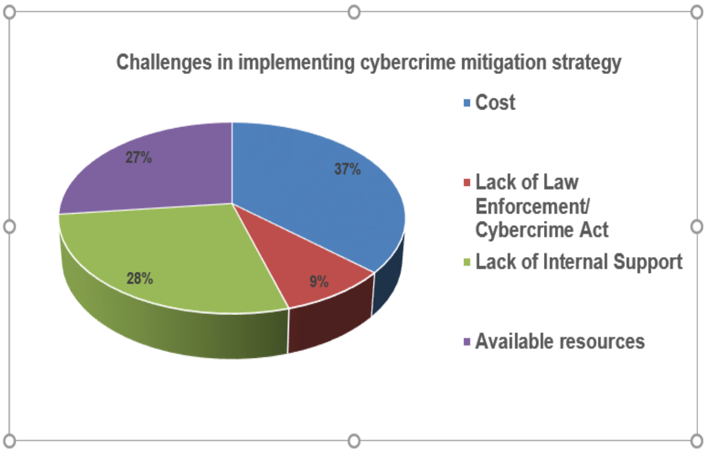

Figure 8. Challenges Facing Cybercrimes Mitigation Strategies
Source: Research Data, 2023

Discussion

The study established that public awareness of cybercrime proved to be the major issue when it comes to cybercrime mitigation strategies' effectiveness. To have a well-planned awareness program for the masses is very important; if any mitigation strategies are implemented, and the majority are well informed about them, then those strategies produce the best result. As observed in the findings, the majority of the respondents have little knowledge about cybercrime, and this implies that some banks under study need to use a different method to spread awareness about cybercrime while others do well.

As shown in the findings, there is a big gap between banks when it comes to knowing, measuring, and applying the right mitigation strategies in order to produce good results.

Furthermore, the most common opinions deducted from the study, the most three common, were training and awareness, strong support from management, and skilled personnel. Moreover, the least ones were support from law enforcement organs and enough allocated budget.

The study established that public awareness of cybercrime proved to be the major issue when it comes to cybercrime mitigation strategies' effectiveness. To have a well-planned awareness program for the masses is very important; if any mitigation strategies are implemented, and the majority are well informed about them, then those strategies produce the best result. As observed in the findings, the majority of the respondents have little knowledge about cybercrime, and this implies that some banks under study need to use a different method to spread awareness about cybercrime while others do well.

As shown in the findings, there is a big gap between banks when it comes to knowing, measuring, and applying the right mitigation strategies in order to produce good results.

Furthermore, the most common opinions deducted from the study, the most three common, were training and awareness, strong support from management, and skilled personnel. Moreover, the least ones were support from law enforcement organs and enough allocated budget.

Conclusion

The study revealed that capacity-building techniques (public awareness), support from management, law enforcement, budget and resources (technology, skilled personnel) can have an impact on cybercrime mitigation strategies to be effective. Applying the above variables could have a great positive effect on any implementation of cybercrime mitigation strategies to be effective in banks. On the other hand, if not applied, it can cause a negative impact that can make any implemented cybercrime mitigation strategies not perform at their best. Therefore, this study sought to assess the effectiveness of implemented cybercrime mitigation strategies(s) in Tanzania commercial banks. The study analyzed and observed that the variables mentioned above, such as public awareness, budget, resources, management, and law enforcement support, influence improving the performance of implemented cybercrime mitigation strategies and increasing satisfaction toward the shareholders of the banks.

Conflict of Interests

No conflict of interest.

References

Airehrour, D.A. (2018). Social engineering attacks and countermeasures in the New Zealand banking system: Advancing a user-reflective mitigation model. *Information, 9*, 110. https://doi.org/10.3390/info9050110

Alghazo, J.M., Kazmi, Z. & Latif, G. (2017). Cyber security analysis of Internet banking in emerging countries: User and bank perspectives. *2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS)* (pp. 1 -- 6). IEEE.

Anderson, R.D. (2007). Teaching the theory of evolution in a social, intellectual and pedagogical context. *Science Education*, *91*(4), 664–677. https://doi.org/10.1002/sce.20204

Raosoft. (n.d.). *Sample size calculator*. Retrieved from http://www.raosoft.com/samplesize.html

Catota, F.E., Morgan, M.G. & Sicker, D.C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. *Journal of Cybersecurity,* *4*(1), tyy002. https://doi.org/10.1093/cybsec/tyy002

Chapman, C. (2018). *How Africa is tackling its cybersecurity skills gap.* Retrieved from https://portswigger.net/daily-swig/how-africa-is-tackling-its-cybersecurity-skills-gap

Council, F.F. (2005). Authentication in an Internet banking environment. *FFIEC agencies.*

Dalton, W., van Vuuren, J.J. & Westcott, J. (2017). Building cybersecurity resilience in Africa. *12th International Conference on Cyber Warfare and Security*, (pp. 112 --120).

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. *Risk Governance and Control: Financial Markets and Institutions*, p. 16 -- 26.

Force., T. P. (2018). *Crimes and Traffic Incidents Report.* Dar Es Salaam, Tanzania.

He, M., Devine, L., & Zhuang, J. (2018). Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach. *Risk analysis : an official publication of the Society for Risk Analysis*, *38*(2), 215–225. https://doi.org/10.1111/risa.12878

Zeus. J.L. (2010). Now bypasses two-factor authentication. Retrieved from: https://blog.trendmicro.com/trendlabs-security- intelligence/

Johnson, A.L. (2016). Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation. *North Carolina Banking Institute, 20*, 277.

Krol, K. Philippou, E., De Cristofaro, E., & Sasse, A. (2015). "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. https://doi.org/10.14722/usec.2015.23001

Kshetri, N. (2019). *Cybercrime and cybersecurity in Africa.* Taylor & Francis.

Lubua, E.W. (2014). Cyber Crimes Incidents in Financial Institutions of Tanzania.

Shoukat, M.M. & Islam, U. (2019). Cybercrime: an emerging threat to the banking sector of Pakistan. *Journal of Financial Crime, 26.* http://dx.doi.org/10.1108/JFC-11-2017-0118

Mbelli, T.M. & Dwolatzky, B. (2016). Cyber security, a threat to cyberbanking in South Africa: An approach to network and application security. *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)*, (pp. 1 -- 6).

Mugenda, A & Mugenda, O. (2003). *Research Methods: Quantitative and Qualitative approaches.* NAIROBI: African Center for Technology Studies (ACTS).

Nadir, I. & Bakhshi, T. (2018). Contemporary cybercrime: A taxonomy of ransomware threats \& mitigation techniques. *International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)* (pp. 1 -- 7). IEEE.

Oluoch, O.M. (2018). *Effect of Cybercrime Securities Strategies of Online Banking: A Survey of Commercial Banks in Kenya.* A research project report submitted in partial fulfillment of the requirement for the award of dgree of Master of Business Advinistration, School of Businnes, University of Nairobi.

Pala, A.A. (2019). Information sharing in cybersecurity: A review. *Decision Analysis, 16*(3), 172-196. http://dx.doi.org/10.1287/deca.2018.0387

Qamar, A., Karim, A. & Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems*, *97*, p. 887–909. https://doi.org/10.1016/j.future.2019.03.007

Serianu. (2016). *Tanzania Cybersecurity report.* Retrieved from https://www.serianu.com/downloads/TanzaniaCyberSecurityReport2016.pdf

Shahriar, H., Klintic, T. and Clincy, V. (2015) Mobile Phishing Attacks and Mitigation Techniques. *Journal of Information Security, 6,* 206-212. http://dx.doi.org/10.4236/jis.2015.63021

Shulla, G. (2013). *An Overview of Legal and Institutional Response To Cybercrimes in Tanzania: Legal and Institutional Challenges on Combating Cybercrimes on Mobile Money Transfer And Payments.* Case Study Dar-Es-Salaam City.

Sutherland, E. (2017). Governance of cybersecurity case of South Africa. *African Journal of Information and Communication, 20*(20), 83–112. http://dx.doi.org/10.23962/10539/23574

Tam, L. T., Chau, N. M., Mai, P. N., Phuong, N. H., & Tran, V. K. H. (2020). Cyber crimes in the banking sector: Case study of Vietnam. *International Journal of Social Science and Economics Invention, 6*(05), 272-277. https://doi.org/10.23958/ijssei/vol06-i05/207

Tambo, E., & Adama, K. (2017). Promoting cybersecurity awareness and resilience approaches, capabilities, and action plans against cybercrimes and frauds in Africa. *International Journal of Cyber-Security and Digital Forensics, 6*(3), 126-138. http://dx.doi.org/10.17781/P002278

Tanzania, T. U. (2015). *The Cybercrimes Act.* Dar es Salaam.

Tariq, M., Aslam, B., Rashid, I., & Waqar, A. (2013). Cyber threats and incident response capability - a case study of Pakistan. *2013 2nd National Conference on Information Assurance (NCIA)*, 15-20. https://doi.org/10.1109/NCIA.2013.6725319

Tariq, N. (2018). Impact of cyberattacks on financial institutions. *The Journal of Internet Banking and Commerce, 23*, 1-11.

Ubena, J. (2010). Why Tanzania Still Needs Broad Electronic Communications Legislations. *Law Reform Journal, Vol. 2.*

Wang, V., Nnaji, H. & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice, 62*, 100415. https://doi.org/10.1016/j.ijlcj.2020.100415

Wazid, M. A. (2019). Mobile banking: evolution and threats: malware threats and security solutions. *IEEE Consumer Electronics Magazine, 8*, 56–60. https://doi.org/10.1109/MCE.2018.2881291

Yusuf, K. (2020). *Africa is leaving itself dangerously exposed to cyber-attacks.* Retrieved from https://www.accaglobal.com/my/en/member/member/accounting-business/2019/02/insights/cyber-attacks.html