International Journal of Economics, Commerce and Management
United Kingdom ISSN 2348 0386 Vol. VIII, Issue 12, Dec 2020

http://ijecm.co.uk/

ASSESSING STRATEGIES TO CREATE CYBER SECURITY AWARENESS AMONG EMPLOYEES IN NATIONAL MICROFINANCE BANK IN TANZANIA

Sabrina Yussuf Shaaban
Institute Of Accountancy Arusha (IAA), P.O. BOX 69007, Dar es Salaam Campus, Tanzania
saysha.yussuf@gmail.com

Haruna Issa Athumani ✉
Institute Of Accountancy Arusha (IAA), P.O. BOX 69007, Dar es Salaam Campus, Tanzania
harunaathumani.ha@gmail.com

Abstract

The main objective of this study was to assess strategies adopted by banks in Tanzania to create awareness of their employees on cyber security. Specifically cyber security policies, training for their employees, as well as planning and outsourcing cyber security specialists. Both empirical and theoretical literature review were done relevant to the variables under study. The study adopted case study design and both quantitative and qualitative approaches were used. Data was analyzed using descriptive statistics and presented by tables and charts for quantitative data. For qualitative data counter analysis was used in analysis. Result showed that 90% of the respondents agreed that banks outsource cyber security specialists while 80% agreed that the bank has established cyber security policies. For the banks to provide training concerning cyber security to their employees the result revealed that 42% agreed, 30% were neutral and 28% disagreed. For bank to establish cyber security plan the result revealed that 66% agreed and 34% were neutral. The study finding conclude that; bank has established cyber security policies and bank provide training concerning cyber security to their employees regularly. This study recommends for security awareness and training to be provided regularly so that to influence employees and in this way bring about compliance with cyber security policies.

Keywords: Awareness, Bank, Cybersecurity, Employees, Outsource, Policies, Strategies, Training

INTRODUCTION

Banks and other financial institutions worldwide are increasingly concerned about cybersecurity awareness and their implementation (Babu, 2018; Mukhopadhya, 2018; Rajendra, 2018). The same trend is observed in Tanzania as well (SERIANU, 2017; SERIANU, 2016). The primary reason being the lack of awareness and their consequences (Boer and Vazquez, 2017). It has been observed that a lack of awareness of cyber threats and their serious implications by Bank`s staff is a major challenge for banks (Babu, 2018). It is posited that the impact cyber threats have on banking system should be well understood by the top management as well as at staff at lower levels and thus managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment (Babu, 2018). All employees have to take appropriate measures to reduce the risk of cyber threats (Finau et al., 2013; NCSC, 2014).

An important fact is that all employees within the bank must be aware of cybercrime dangers and to take appropriate measures to reduce the risk of cybercrime (Finau et al., 2013). Similarly, all employees should be aware of the security risks associated with their private online activities, such as indiscreet use of social media, use of public cloud. Cyber security policy should address mixing company data with private data on mobile devices (Kojo, 2015). This will require a high level of awareness among staff at all levels. Top Management and Board should also have a fair degree of awareness of the fine nuances of the threats and appropriate familiarization may be organized (Babu, 2018).

Taken together, the level of cyber security awareness among employees, customers and other key stakeholders of financial institutions is questionable given the persistent and increasing cybercrimes in the sector. Thus, having a deeper understanding of awareness among employees and customers in Banks regarding cyber security measures and implementation would help in devising strategies for improving the capacity of employees and customers to manage cybercrimes of different sorts (Hadlington, 2018).

Therefore, employees use their device to access the bank service or use the bank device to check their email. This may create an opportunity for security attacks sent to them disguised as a genuine offer or gift. Additional, bank employees who are unhappy about treatment by the institution steal sensitive bank information which they can decide to sell the information to cybercriminals. Thus, the current study is proposed to assess the cyber security awareness among employees from Bank Industry. A comprehensive understanding and assessment study was conducted to help the bank to offer them better strategies to address their employees in an efficient way. The goal of the study is to provide insights into what is required in the Tanzanian banks to create cyber security awareness among its employees.

Objective of Study

To assess strategies adopted by banks in Tanzania to create awareness of their employees on cyber security.

LITERATURE REVIEW

General Deterrence Theory

This theory propositions that individuals can be discouraged from committing irregular selfish acts through the use of strategies which include strong deterrents and sanctions comparative to the act (Schuessler, 2009). Strategies such as employees' education, cybersecurity policies, cybersecurity plan and outsourcing cybersecurity specialists to create awareness of their employees on cybersecurity (Schuessler, 2009). The theory relates to this study as it informs systems administrators and managers on strategies that should be adopted by banks in Tanzania to create awareness of their employees concerning cybersecurity.

Security awareness training

Security awareness training is a formal process for educating employees about computer security.A good security awareness program should educate employees about corporate policies and procedures for working with information technology (IT). Employees should receive information about who to contact if they discover a security threat and be taught that data is a valuable corporate asset. (Proof point, 2020)

Kim (2013) argued that cyber security training is imperative for college students and that survey data can help determine whether problems with security are due to lack of concern or lack of skill (in navigating devices' security settings).

The importance of public security awareness has been studied by researchers a decade ago. CSI (2007) determined lack of security awareness of people as one of the most critical computer security issues in coming years.

Information security awareness is particularly important for banking information which must at all-time be protected from cyber-attacks that he/she may later use the data for personal advantage. Some of related research in cyber security, as well as information security awareness and training, within the banking industry and other sector (Kim, 2013).

Online cybersecurity training is to help employees to protect themselves and the company against cyber-attacks and threats. Training empowers employees with an up-to-date know-how on how to recognize and mitigate a cyber-threat. By making employees able to identify and eliminate cyber threats, you are strengthening the most vulnerable link in the chain. (Defendants, 2016)

Outsourcing Cybersecurity Specialists

Outsourcing cybersecurity isn’t just a great way to save a good amount of money and time, it also addresses another pressing concern, that of skill gap that you may face locally. There just aren’t enough cybersecurity experts to keep pace with the massive online businesses today is to outsource their cybersecurity functions to reputable cybersecurity provider. (Irfan, 2019)

Cybersecurity specialists can help with monitoring the tactics and behavior of cybercriminals, identifying network vulnerabilities, and, most of all: detect and respond swiftly to incidents. Being able to rectify issues quickly is what can prevent an attack from escalating, thus mitigating the knock-on effect to a company’s trust and reputation with clients. (Gary McCauley, 2020)

Cybersecurity strategy

Cybersecurity strategy is a plan of actions designed to improve the security and resilience of infrastructures and services. It is a high-level top-down approach to cybersecurity that establishes a range of objectives and priorities that should be achieved in a specific timeframe (Enisa, 2020)

An empirical study by Okuku et al. (2015) concludes that Kenya’s growth in Internet use has been facilitated by high proliferation and adoption of mobile communications and the role of governmental cyber security strategy is important for improving public awareness of Internet threats. The study by Okuku et al. (2015) proposed that future research in this area be carried out to specifically measure the effectiveness of cyber security awareness approaches in countries with vibrant mobile Internet societies that have implemented awareness drives. The study by Casey (2011) concludes that issues experience in the telecommunications industry include; breaches to data confidentiality, integrity and availability of computer data Crimes related to data include data infiltration, unauthorized encryption and lose, unwanted data infiltration, deletion, alterations.

Information security policy

An information security policy is a set of rules enacted by an organization to ensure that all users of networks or the IT structure within the organization's domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organization stretches its authority. Bakari (2017) presented issues around Information Security Management (ISM). It provides that ISM relates to the processes of ensuring availability, confidentiality and integrity for business productivity. The author argues that successful ISM is dependent on the availability and implementation of a credible Information Security Policy.

Cybersecurity policies are important because cyberattacks and data breaches are potentially costly. At the same time, employees are often the weak links in an organization's security. Employees share passwords, click on malicious URLs and attachments, use unapproved cloud applications, and neglect to encrypt sensitive files. A cybersecurity policy sets the standards of behavior for activities such as the encryption of email attachments and restrictions on the use of social media. (McAfee, 2020)

Conceptual Framework

General Deterrence theory which the study has used as a foundation was presented along with related concepts. The major parts of the theory compose of organization strategies on cyber security awareness on their employees, which include policies, plan, training and outsourcing of cyber security specialist. These parts construct the base, on which the conceptual model is presented below.

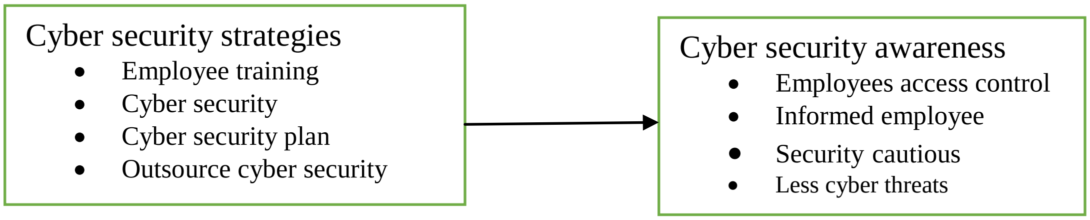

Figure 1: Conceptual Model

METHODOLOGY

The study adopted a case study design. Study was conducted at National Microfinance Bank, Magomeni Branch Tanzania. The particular branch was chosen as a case study because its employees were trained in cyber security before other branches and outsourced specialists were deployed there before any other branches. Therefore, the researcher it was expected that the researcher could get more information when assessing cybersecurity adoption by banks to create awareness among their employees.

This study employed both quantitative and qualitative approaches. The use of both of these approaches helped the researcher to complement the weakness of each, therefore provide an extended room for triangulation of both instruments for data collection and approaches. This study primary data was collected by using a questionnaire and structured interviews. The quantitative data were analyzed using descriptive statistic with the aid of Statistical Package for Social Sciences (SPSS V.23) and Microsoft excel. Qualitative data were analyzed by using content analysis.

The target population was all employees who involved in core bank activities from NMB because the researcher believed that those people pose important information to solve the problem under study. The purposive sampling design was used in the selected sample and the sample size is 50 staff. Respondents of this study received 50 questionnaires and interview guide and all 50 questionnaires and interview guides were returned and used for analysis.

FINDINGS

The study sought to assess strategies created by NMB bank in Tanzania on cybersecurity awareness of their employees. The following are findings presented in the table below:

Table 1: Cybersecurity Strategies

Statement		**SD**	**D**	**N**	**A**	**SA**
Bank has established cybersecurity policies	**F**	0	2	8	30	10
	(%)	0	4	16	60	20
Bank provide education concerning cybersecurity to all employees regularly	**F**	9	5	15	21	0
	(%)	18	10	30	42	0
Bank has established cyber security plan	**F**	0	0	17	33	0
	(%)	0	0	34	66	0
Bank outsource cybersecurity specialists	**F**	0	0	5	45	0
	(%)	0	0	10	90	0
Note SD=strongly disagree D= Disagree N=Neutral A=Agree SA=Strongly Agree						

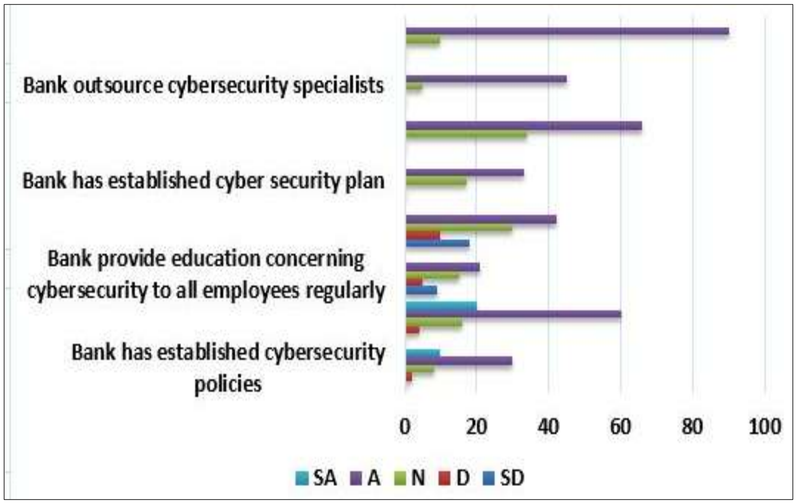

Figure 1: Cybersecurity Strategies

From the table above, majority of the respondents (80%) agreed that bank has established cyber security policies while 4% disagreed and 16% were neutral. During the interview, one of interviewees indicated that;

> *"… We do have policies which govern our employees as well as operation on cyber security issues. We are regularly updating these policies as the technological environment changes"*

42% of the respondents agreed that bank provide education concerning cyber security to all employees regularly though 30% of the respondents were neutral, 18% strongly disagreed and 10% disagreed. One of the interviewees stated that;

> *"…Yes of course, our bank has special training programs meant to rise up cyber security awareness. Whenever we adopt and implement new systems, we must provide education on such systems as well as its repercussion on cyber space"*

In this study (66%) of the respondents agreed that bank has established cyber security plan while 34% of the respondents were neutral. On the issue of cyber security plan, one of the HoDs stated that;

> *"We have a cyber-security plan which was purposely established for protecting our customers, employees and bank in general".*

Also,

> *"Our cyber security plan enables IT team to communicate effectively about how cyber security capability is positioned within the bank".*

90% of the respondents agreed that bank outsource cyber security specialists though 10% were neutral. On the interview, respondents indicated that;

"Cyberspace is too broad; we do outsource competent cyber security specialists to assist us in some of our technological operations".

One of the IT specialists added that;

> *"External cyber security specialists have different and interesting exposure, we do outsource them not only for rising awareness but to learn something new from their competence and experience"*

DISCUSSION OF FINDINGS

Results of this study indicated that bank has complicated regulation in creating cyber security awareness among their employees. Findings unveiled that majority of the respondents agreed that bank had enough people to raise awareness though user risks and behavior modification pose a challenge to the bank in creating cyber security awareness among their employees. Chen-Li (2020) postulated that one of the toughest challenges of cyber security is to raise awareness among users. Technology solutions are instrumental in achieving a solid security posture, but they only get you so far. There's always the risk a user will make a split-second bad decision and open the door to attack. Awareness is important because attackers frequently take advantage of people's natural tendency to be helpful and forthcoming in order to get into a system (Muji et al 2019). Thus, if an NMB Bank does not manage security effectively, the impact to an organization could be very significant.

Findings unveiled that employee readiness, trust and continuously adoption of advanced technologies pose a challenge to the bank in creating cyber security awareness among their employees. Cyber security depends on people. It is people's intentional and unintentional actions that cause adverse consequences that security wants to prevent. Technologies meant to provide security ultimately depend on the effective implementation and operation of these technologies by people. This means that bank should depend on human resource to achieve a cyber-secured environment. Since humans resource are seen as the "weakest link" in the cyberspace, there is a clear requirement to ensure employees are trained correctly in terms of cyber security policies and principles. The goal is to ensure that employees are adhered to the cyber security policies and principles and they are not utilized by cybercriminals.

Findings indicated bank has established cyber security policies, bank provides education concerning cyber security to all employees regularly, bank has established cyber security plan. Results depicted that bank outsource cyber security specialists, carry out cyber risk assessment on its critical assets and carry out cyber security or information security audits. These findings are consistent with James et al (2019) findings who identifies keys strategies that impact on cyber security in organization as top management support, staff and management security awareness, strong information system security infrastructure, security culture, management style, management change and security and privacy regulations as well as frequently information security audits. Also these findings are in line with Keplain (2020) who indicated that to keep organization safe and secure the following thing should be adhered; create a security system, increase your employee skill set, backup your data, put the cloud to work, invest in your IT infrastructure and carry out cyber risk assessment regularly.

CONCLUSIVE REMARKS

Conclusions

From the findings, this study concluded that cyber security policies and education provision at NMB Bank must, of course, explore the latest and greatest technologies to rise cyber security awareness, but it is also critical that bank establish and maintain good security protocols and practices to supplement emerging technologies. Also the bank must make sure that it adopts technologies which it can fully utilize them. Because if the bank adopts technologies which cannot fully utilizes them it they end up creating significant inefficiencies within the cybersecurity team, thereby compromising the cyber security program.

Implications of the Study

The implications for practitioners are potentially significant. In order for a bank to implement effective information security it is essential to gain the understanding of all the employees within the bank. In addition, compliance with security policies is necessary and, in some cases, this compliance needs to be demonstrated by either the information security function or the risk management function within an organization in order to justify their activities. At face value the outcome of this research points to the fact that security awareness training, while important, is not sufficient to prevent non-compliant behavior and to ensure compliant behavior.

Recommendations

Various recommendations were made based on the findings of this study;

i. Security awareness training should influence all employees not only IT staffs within an organization to ensure the appropriate behavior is enacted by all and, in this way, bring about compliance with cyber security policies.

ii. Commercial banks in Tanzania are recommended to create a set of initiatives to address the high priority risks and control gaps in cyber space.

iii. Despite active efforts to raise awareness in cyber security, the field continues to experience a shortage of individuals interested in the career, which is a significant concern for educators, policymakers, and researchers. To close these cyber security workforce gaps, Higher Learning Institutions in Tanzania are recommended to initiate courses special for cyber security.

Areas for further Research

Though this study has fulfilled its aim and objectives, there are a number of areas for additional studies and empirical research, given the limitations of the research;

i. On a geographical dimension, this study was restricted mainly to National Microfinance Bank - Tanzania. Therefore, it may not be suitable to generalize in this nation or any other nation to the entire population of banks. Further empirical studies are therefore required in distinct areas as well as in other East African nations.

ii. On methodology, the research approach selected for achieving the study goals was restricted to mixed research approach. As such, future research could build on this study by looking quantitatively approach at the cyber security awareness among employees in distinct sectors and industries. Future studies could use the same survey tool and technique to generalize research more globally.

REFERENCES

Dlamini, I; Taute, B. and Radebe, J. (2011)“Framework for an African policy towards creating cyber security awareness”, The Southern African Cyber Security Awareness Workshop (SACSAW) 2011, pp. 15-31.

Enisa.europa.eu. 2020. [Online] Available at:<https://www.enisa.europa.eu/topics/national-cyber-security-strategies [Accessed 24 November 2020].

Herath, T., Rao, H.R. .: Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems 18(2), 106-125(2009)

Kortjan, N and von Solms, R. (2014), “A conceptual framework for cyber-security awareness and education in SA”, Research Article- SACJ No. 52, July 2014, pp. 29-41.

Manque (2019) A framework for evaluating ICT security awareness. Volume 22, Issue 8, Pages 675-684.

Mcafee.com. 2020. How Cybersecurity Policies And Procedures Protect Against Cyber attacks | Mcafee. [Online] Available at:<https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/cybersecurity-policies.html> [Accessed 16 November 2020].

Mujl, F. Kruger HA, Kearney WD. (2019) Information Security Management (3): The Code of Practice for Information Security Management (BS7799). Information Management & Computer Security, Vol. 6, No. 5, pp. 224–225.

Proofpoint. 2020. What Is Security Awareness Training? | Proof point. [Online] Available at: <https://www.proofpoint.com/us/security-awareness/post/what-security-awareness-training [Accessed 24 November 2020].

Serianu (2016) “Africa cyber security report”. http://www.serianu.com/downloads/AfricaCyberSecurity Report2016.pdf, 2016. (Retrieved: August 2020).

Siponen, M., Mahmood, M. A., Pahnila, S. .: Technical opinion Are employees putting your company at risk by not following information security policies? Communications of the ACM, 52(12), 145-147(2009)

Tanzania Police Force (2012). Annual Crime report. Laboratory. Dar es Salaam.

Virtualemployee.com. 2020. How Has Outsourcing Become An Unlikely Cyber Security Savior For Businesses Globally? [Online] Available at: <https://www.virtualemployee.com/blog/how-has-outsourcing-become-an-unlikely-cyber-security-savior-for-businesses-globally[Accessed 18 November 2020].

Windsor, J. and Schuessler, J., 2020. General Deterrence Theory: Assessing Information Systems Security Effectiveness In Large Versus Small Businesses.

Wombat Security Technologies (Wombat) and the Aberdeen Group: “African union cybersecurity profile: Seeking a common continental policy”. https://jsis.washington.edu/news/africanunion-cybersecurity-profile-seeking common-continental-policy/, 2016. (retrieved: August 2020).