International Journal of Computer Applications Technology and Research
Volume 13–Issue 07, 39 – 41, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1307.1006

Cybersecurity: A Case of Company and Organization Security

Asnath Nyachiro
Technical University of Mombasa
Mombasa, Kenya

Kennedy Hadullo
Technical University of Mombasa
Mombasa, Kenya

Kelvin Tole
Technical University of Mombasa
Mombasa, Kenya

Abstract: In the current digital landscape, organizations heavily rely on interconnected technologies to enhance operational efficiency, yet this dependency also exposes them to significant cybersecurity risks. Despite deploying advanced cybersecurity tools, employees remain a critical vulnerability due to their limited awareness of cybersecurity threats. Research highlights the pivotal role of employees in mitigating such risks, emphasizing the impact of human error and behavior on organizational security. This study aims to assess the level of cybersecurity awareness among employees and evaluate the effectiveness of training initiatives in enhancing organizational cybersecurity resilience. The methodology involved a comprehensive literature review, encompassing articles, journals, case studies, and books related to cybersecurity awareness, cyber threats, and employee training. Key search terms included "cybersecurity," "cyber threats," "cyberattacks," "user awareness," "cybersecurity training," and "knowledge of cybersecurity," using databases like Google Scholar, Science Direct, and Springer. The review highlighted various cybersecurity challenges faced by organizations, including internal threats from employees and external threats from hackers and malicious actors.

Keywords: cybersecurity, cyber threats, cyberattacks, user awareness, cybersecurity training and knowledge of cybersecurity.

1. INTRODUCTION

The growing reliance on digital technologies and information systems within organizations has brought about unprecedented levels of interconnectedness and efficiency. However, this technological advancement also introduces significant cybersecurity challenges, particularly related to the human element within organizations. Despite the implementation of sophisticated cybersecurity tools and protocols, employees remain a critical point of vulnerability due to their lack of awareness and understanding of cybersecurity risks. Research in the field of cybersecurity underscores the pivotal role of employees in mitigating cybersecurity threats, emphasizing that human error and behavior often pose the greatest risks to organizational security.

2. METHODOLOGY

The literature review included articles, journals, case studies, and books relating to content on user awareness of cybersecurity, cyberattacks. The terms and keywords used in the search process included cybersecurity, cyberthreats, cyberattacks, user awareness, cybersecurity training, and knowledge of cybersecurity. The databases used were Google Scholar, Science Direct, and Springer. These included conference reports, articles, and journals.

3. LITERATURE REVIEW

Data Safety According to earlier studies, information and information assets have historically been protected from potential cyberthreats and cyberattacks using a technological method (Carcary et al., 2016). It could be argued that the security of information and information assets requires the use of technical tools yet, organizations, including governments, have searched for proactive measures to safeguard data and information systems from human behaviors in response to Carcary et al. (2016)'s research. According to Antoniou (2018), merely employing technological tools to prevent human behaviors like password sharing among coworkers or viewing private information over an unsecured WiFi network is insufficient. Maynard et al. (2018) are among the other academics who have proposed that workers should also be considered a potential cybersecurity risk in addition to the technical concerns. They proposed that one of the primary contributing factors to cyberthreats that target data and information systems is an employee. According to McLane (2018), employees that are primarily regarded as the weakest link must have their information and information assets secured.

Knowledge is another element that affects information security. For instance, Kim et al. (2014) investigated the barriers to employee adherence to security protocols that may avert cyberattacks using a quantitative research methodology. They discovered that the application of preventive measures in the adoption of information security is hampered by ignorance. This is consistent with study by Alqahtani (2017), who discovered that employees think that the adoption of information security preventative measures is mostly influenced by their ability to recognize cyberthreats.

Information systems are facing more dangers and vulnerabilities as a result of the growing use of network solutions (Adebayo, 2012; Chul et al., 2016; Ferrillo & Singer, 2015). According to Ferrillo and Singer's (2015) conclusion, employees' risky activities may negatively impact information and data systems. Employee behavior decisions are strongly correlated with their perception of risk (Ahmad et al., 2019; Ferrillo & Singer, 2015). According to Dang-Pham et al. (2017), employee behavior decisions may have an impact on how information systems are managed. Hadlington (2017) provided evidence for this theory by examining the traits and attitudes of the public sector, including how these factors have affected the employees' intents toward information and cybersecurity. Furthermore, Gordon et al. (2015) and Hwang et al. (2017) looked at how employees behaved and thought about information system security challenges, and they found that workers can build moral convictions about cybersecurity.

Information security is the overarching theme and fundamental building block for the creation of any cybersecurity awareness campaign, according to Fietkiewicz et al. (2017). It is therefore the duty of all government personnel, not only managers and supervisors, to protect confidential information (Gordon et al., 2015). According to

Dykstra and Spafford (2018), research on how people affect information security is essential for developing cybersecurity solutions and equipping staff members with cybersecurity awareness training to fend off potential threats.

Information system access and identification can now be stolen or surmised thanks to the globalization of communication across information systems networks (Gabriel & Mohamed, 2011; Solari, 2012). Additionally, as the majority of cyberthreats and cyberattacks do not originate from the actual location of the attack, it has become more difficult to identify their origins due to the globalization of information systems networks (Gabriel & Mohamed, 2011). But in order to stop hackers and lessen cyberattacks, Bland et al. (2020) created an algorithm to recognize trojan methods and script comments. On the other hand, Solari (2012) supported the initial perspective by examining the elements that preceded cyberattacks and concluded that information security and information threat mitigation needed to be concentrated on identifying elements that can encourage employee behaviors that will increase cybersecurity awareness.

3.1. INTERNAL THREATS

Employees, contractors, and supervisors who have been granted access to confidential information and information systems are examples of internal dangers. Certain researchers (Ahmad et al., 2014; Glasser & Taneja, 2017) have concentrated on internal threats in which the goal was premeditated and hostile. Internal threats that fall under the heading of malicious internal threats that were planned include information theft for monetary gain and retaliation. Internal threats were recognized by Ahmad et al. (2015), along with the reasons why they are detrimental to information security. Scholars such as Harnett (2016) and Kshetri (2013) have concentrated on personnel that pose a threat internally but lack malicious intent. The organization's personnel are merely unable to oversee information security. Internal risks are those that come from within the company, according to Harnett (2016). After reviewing the literature on internal threats, Ahmad et al. 2015 came to the conclusion that the two main contributors to internal security events and significant risks to information security were employees' inappropriate behavior and a lack of cybersecurity awareness. Gabriel and Mohamed (2011) claim that by comprehending what influences employee behavior, internal dangers can be lessened or managed.

3.2 EXTERNAL THREATS

Hackers, former employees, natural calamities, and other governmental organizations are some of these threats. Threats from the outside lack access to the information systems and rights (Harnett, 2016). Stephen (2011) noted in his study on cybercrimes that the 2007 Denial of Service (DoS) assaults against Estonia were a significant example of an external cyberattack. Because it impacted every digital service in the nation over the course of 22 days. This attack was noteworthy and a milestone since every harmful traffic came from somewhere other than Estonia.

Comprehending the factors that impact users' awareness of cybersecurity is a pertinent issue for multiple reasons. First, scholarly research suggests that user knowledge of cybersecurity has a role in the overall decline in cyberattacks on information systems (Asllani et al., 2013; Ki-Aries & Faily, 2017; Knapp & Ferrante, 2012). A company misses out on a chance to avoid cyberattacks and putting information security policies and procedures in place by failing to adopt a cybersecurity awareness posture (Ki-Aries & Faily, 2017). For example, Hajli and Lin (2016) discovered that after creating information security policies, staff members were able to incorporate the policies into their regular tasks, such as sharing their computer's password with coworkers or refraining from utilizing an open WiFi network to access the organization's files.

De Bruijn and Janssen's (2017) case study was one of the research contributions that highlighted the organization's inadequate information management as a contributing element in cyberattacks, as opposed to the employees. This study also highlighted the organization's responsibility in preventing cyberattacks. They insinuated that focusing on information security management and implementing effective governance are necessary to prevent cyberattacks and breaches of data security. A thorough analysis of the literature on cybersecurity trends and potential defenses against cyberattacks was carried out by Steinbart et al. (2016). They found out that a large number of businesses had not taken the necessary precautions to protect their information systems from cyberthreats and cyberattacks, leaving gaps and backdoors open to hackers and other unauthorized users. Furthermore, Steinbart et al. recommended that companies spend money and effort training end users and developing security policies and procedures. According to Creasey (2013), this is important yet frequently disregarded due to a lack of knowledge or resources within the company.

4. ACKNOWLEDGMENTS

Our thanks to the Technical University of Mombasa.

5. REFERENCES

[1] Adebayo, A. O. (2012). A foundation for breach data analysis. Journal of Information Engineering and Applications, 2, 17-21

[2] Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing, 25, 357-370. https://doi.org/10.1007/s10845-012-0683-0

[3] Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. International Journal of Information Management, 35, 717-723. https://doi.org/10.1016/j.ijinfomgt.2015.08.001

[4] Ahmad, Z., Ong, T. S., Liew, T. H., & Norhashim, M. (2019). Security monitoring and information security assurance behaviour among employees: An empirical analysis. Information and Computer Security. https://doi.org/10.1108/ICS-10- 2017-0073

[5] Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. Procedia Computer Science, 124, 691-697. https://doi.org/10.1016/j.procs.2017.12.206

[6] Antoniou, G. S. (2018). A framework for the governance of information security: Can it be used in an organization. SoutheastCon, 1-30. https://doi.org/10.1109/secon.2018.8479032

[7] Asllani, A., White, C. S., and Ettkin, L. (2013). Viewing cybersecurity as a public good: The role of governments, businesses, and individuals. Journal of Legal, Ethical and Regulatory Issues, 16(1),17-14

[8] Bland, J. A., Petty, M. D., Whitaker, T. S., Maxwell, K. P., & Cantrell, W. A. (2020). Machine learning cyberattack and defense strategies. Computers & Security, 92. https://doi.org/10.1016/j.cose.2020.101738

[9] Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A framework for information security governance and management. IT Professional, 18(2), 22–30. https://doi.org/10.1109/mitp.2016.27

[10] Chul H, L., Xianjun, G., & Raghunathan, S. (2016). Mandatory standards and organizational information security. Information Systems Research, 27(1), 70-86. https://doi.org/10.1287/isre.2015.0607

[11] Creasey, J. (2013). Cybersecurity incident response guide. https://www.crestapproved.org/wpcontent/uploads/2014/11/CSIRProcurementGui de.pdf

[12] Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Investigation into the formation of information security influence: Network analysis of an emerging organization. Computers & Security, 70, 111-123. https://doi.org/10.1016/j.cose.2017.05.010

De Bruijn, H. & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34 (1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

[13] Dykstra, J., & Spafford, E. H. (2018). The case for disappearing cybersecurity. Communications of the ACM, 61(7), 40– 42. https://doi.org/10.1145/3213764

[14] Ferrillo, P., & Singer, R. (2015). Is employee awareness and training the holy grail of cybersecurity? Corporate Governance Advisor, 23(3), 10-13.

[15] Fietkiewicz, K. J., Mainka, A., & Stock, W. G. (2017). eGovernment in cities of the knowledge society. An empirical investigation of smart cities' governmental websites. Government Information Quarterly, 34(1), 75–83. https://doi.org/10.1016/j.giq.2016.08.003

[16] Gabriel, B. A., & Mohamed, A. (2011). Impact of globalization. European Business Review, 23(1), 120-132. https://doi.org/10.1108/09555341111098026

[17] Glasser, D. & Taneja, A. (2017). A routine activity theory-based framework for combating cybercrime. In Identity theft: Breakthroughs in research and practice, (pp. 69-78).

[18] Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. Journal of Cybersecurity, 1, 3-17. https://doi.org/10.1093/cybsec/tyv011

[19] Hadlington, L. (2017). Human factors in cybersecurity; Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), 1-18. https://doi.org/10.1016/j.heliyon.2017.e00346

[20] Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. Journal of Business Ethics, 133(1), 111. https://doi.org/10.1007/s10551-014-2346-x

[21] Harnett, T. (2016). Protecting your most valuable assets crafting a cybersecurity strategy to guard against internal and external threats. Chief Learning Officer, 15(8), 26.

[22] Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. Online Information Review, 41(1), 2-18. https://doi.org/10.1108/oir-11-2015-0358

[23] Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. Computers & Security, 70, 663-674. https://doi.org/10.1016/j.cose.2017.08.001

[24] Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. The Scientific World Journal, 2014,1-12. https://doi.org/10.1155/2014/463870

[25] Knapp, K. J., & Ferrante, C. J. (2012). Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. Journal of Management Policy and Practice, 13(5), 66–80

[26] Kshetri, N. (2013). Privacy and security issues in cloud security: The role of institutions and institutional evolution. Telecommunications Policy, 37(4-5), 372-386. https://doi.org/10.1016/j.telpol.2012.04.011

[27] Maynard, S. B., Tan, T., Ahmad, A., & Ruighaver, T. (2018). Towards a framework for strategic security context in information security governance. Pacific Asia Journal of the Association for Information Systems, 10(4), 65. https://doi.org/10.17705/1pais.10403

[28] McLane, P. (2018). Cyberattacks put every enterprise at risk: Techniques diversify as corporate adversaries get smarter. Multichannel News (15), 8

[29] Solari, L. (2012). Globalization will make us all more different. People and Strategy, 35(2), 30-35

[30] Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs. Journal of Information Systems, 30(1), 71-92. https://doi.org/10.2308/isys-51257

[31] Stephen, H. (2011). Revisiting the Estonian cyberattacks: Digital threats and multinational responses. Journal of Strategic Security, 4(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[32] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[33] Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.

[34] Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender