International Journal of Safety and Security Engineering
Vol. 11, No. 1, February, 2021, pp. 101-104
Journal homepage: http://iieta.org/journals/ijsse

Business Organization Security Strategies to Cyber Security Threats

Bandr Fakiha

Faculty of Health Sciences, Medical Health Services, Umm Al-Qura University, Al-Qunfudhah, 21912, K.S.A.

Corresponding Author Email: bsfakiha@uqu.edu.sa

https://doi.org/10.18280/ijsse.110111

Received: 22 October 2020
Accepted: 13 January 2021

Keywords:
SIEM framework, cyber-attacks, ICT, cyber-security, business organizations, cyber-security threats

ABSTRACT

It is argued that the advancement of Information, Communication and Technology went hand in hand with the emergence of certain threats and vulnerabilities to cybersecurity. In several cases, cyber attacks have targeted the information, communication and infrastructure networks of numerous organizations. Today, hackers and intruders have advanced technology within their scope that lets them access the organizational information system. The present study highlights numerous internet security related problems, it offers a broad-based overview of internet threats from the perspective of business enterprises, along with prevention measures and enhanced safety strategies. A systematic analysis of secondary literature was introduced by researchers, the study found that it is critical for organizations to choose an IT security management tool that can be categorized as best practices and standards. The Security Incident Event Management (SIEM) framework is one key instrument proposed here. SIEM instruments help security analysts gain insight into the security threats targeting the IT structures of a given organization.

1. INTRODUCTION

The use and advancement of information technology has enhanced flexibility and reliability in the provision of services for a long time, and a good number of organizations today rely on IT in an increasing number of ways [1]. For both commercial and non-commercial firms, the use of IT is gradually becoming more vital, this is because bulk of company activities are technology oriented [2]. Although the computerization process is taking place at a high pace, business entities have become increasingly concerned about the protection of essential IT devices. For instance, device hacking and intrusion incidents by cybercriminals are proving to be quite common, this issue affects organizations using IT systems; hacking or intrusion of organization's computer system can lead to; money theft, or stealing of confidential information of organizations, while many organizations move their operations into the cloud. Jing et al. [3] point out that new incidence of data breaches and vulnerabilities are likely to occur in cloud computing. Most organizations across the world lack coordinated activities on IT security related issues such as Cyber safety. This paper's research report will highlight some internet security concerns and include a broad-based overview of cybersecurity threats to business entities, together with mitigation and enhanced defense strategies.

2. LITERATURE REVIEW

This paper will look at the security issues that have emerged as a result of new technology in the business world. The SIEM framework is also discussed in the paper, which is an important tool for defending computer systems and networks from cyber-attacks by criminals. The research will continue in the following order: materials and methods used in the study; findings produced by the study; and finally, the results of the study's findings.

3. MATERIALS AND METHOD

The literature study was carried out to identify cyber security threats and ways to mitigate those threats. Journal papers, books, and periodicals on cyber security were sufficient secondary sources for analysis [4]. In order to find books and other scholarly articles, the university library database was used, as shown in Figure 1, each article was created by first entering relevant keywords into databases within computer systems. The researcher made a search of different peer-reviewed articles from different databases which included: Google Scholar, EBSCOhost, ERIC and Academic OneFile. Different keywords were used in the search, including 'Information Security Culture', 'Cyber Security Culture', 'Security Culture', 'Organization Culture' and 'Organizational Culture' as examples of these terms.

5000 documents, which also included conventional teaching studies as well as other organizational papers, represented the quest strategy implemented in a variety of organizational databases. Despite the accessibility of multiple data through the search strategy, the data cleaning process was heavily enforced, eliminating all duplicates. After eliminating all duplicates, the titles and abstracts of the remaining 2865 publications were reviewed. A further 2500 were disqualified as they did not comply with the requirements for inclusion. In addition, there was no research on "ongoing analysis" included. Based on architecture and general research methods, other studies were omitted.

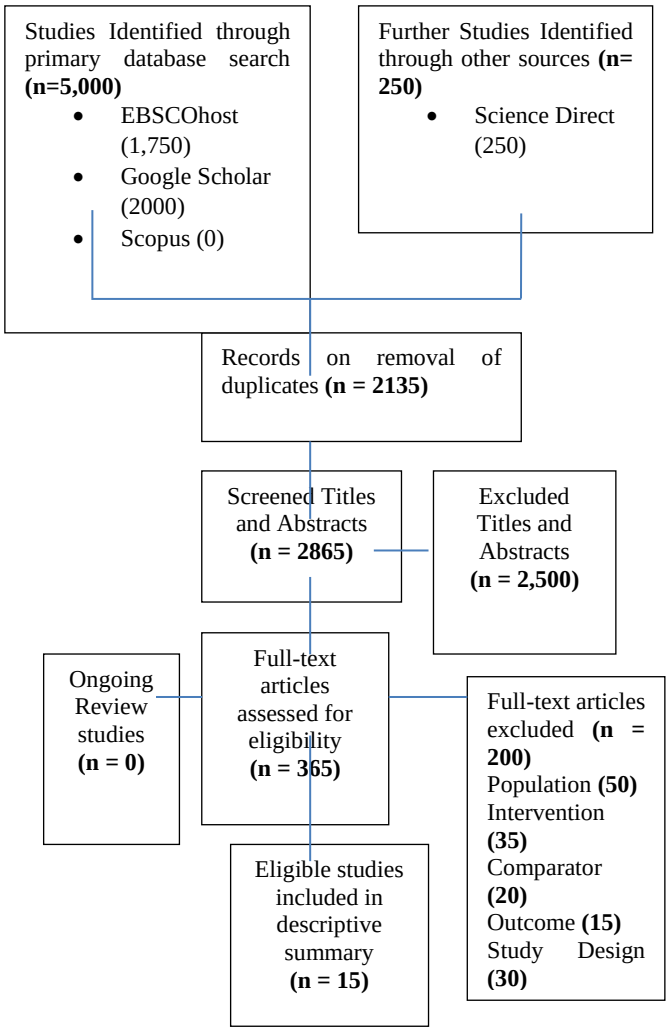

Figure 1. PRISMA study flowchart of search results

4. FINDINGS

4.1 Cyber security threats

From Figure 2, cyber-security risks have continued to develop and, as a result, have taken on a new shape, according to the literature. According to Wanyoike et al. [5], 430 million new malware pieces were found in 2015, a 36 percent rise over 2014. With the increasing rate of technology adoption by small businesses, these statistics leave them highly vulnerable.

Figure 2. Cyber security threats

According to Flores et al., cyber-attacks have the potential to influence both large and small business organizations, resulting in a range of financial consequences such as data theft, manipulation, and corruption. These risks ultimately interfere with the organization's brand, leading to a poor reputation and decreased competition in the financial markets.

In several cases, cyber-attacks have been aimed at various organizations' ICT systems. Hackers and intruders today have access to cutting-edge technology that enables them to gain access to an organization's information system, which can have a huge negative effect on the whole system [6], which has been a great challenge experienced by different business organizations. Hence, they need a complex security infrastructure that can protect the current computer networks from dangerous threats [7]. The protection system can consist of firewalls, intrusion detection and prevention systems, and path management solutions, along with some strong anti-viruses.

4.2 Prevention strategies

Despite the threats of cyber-attacks, non-profit organizations are undergoing a drastic transition in order to adopt modern information technology. Defending against the possibility of cyber-attack is one of the most critical aspects that today's business organizations must strengthen. While many organizations are going ahead with E-services and making their information more digital, easy, and available, according to Singh et al. [8], there is a possibility of a significant cyber threat. Users and organizations are requesting granular systems that can provide the data stored online with vital protection [9]. In modern times, cyber-attacks have become quite complex, and more sophisticated tools are required to provide the entire computer system with security.

In their report [10] recommended that the current information and technology climate requires a comprehensive protection framework that can secure existing computer networks from hazardous external and internal threats, Firewalls, intrusion detection and prevention systems, and, finally, path management solutions, along with reliable anti-virus [11], can be part of this form of protection framework. Each of these solutions completes the task at hand and then produces a large amount of log data that can be conveniently processed within the system. Both log files of the individual device are evaluated and compared appropriately for the system to identify potential security threats at the earliest possible period. Owing to the level of difficulty involved, this has proved to be exceedingly difficult for small companies to achieve, Selecting IT security management software of a high quality is important for the security management approaches for the information technology of a given enterprise. The Security Incident Event Management (SIEM) framework is an effective tool here, according to Pham [12]. SIEM software allows security analysts gain insight into the security threats targeting the IT processes of a given company [13]. This can be achieved by searching at the logs generated by network devices and looking for signs of an ongoing attack. Figure 3 showed the components of SIEM system. The SIEM system must be capable of correlating a large number of logs from different sources and detecting an attack with a high detection rate and low false-positive rate [14].

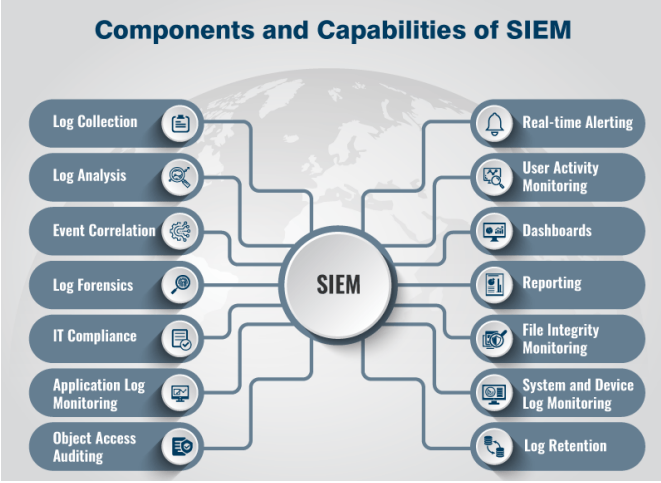

Figure 3. The components of SIEM system

In addition, Pham [14] suggests that security analysts need to find a way to identify the various components of the different departments in order to prioritize threats and respond first to the most important threats. As the amount of cybercrime grows worldwide, it is important to have a consistent legal structure to deal with it. The SIEM method provides mechanisms for the aggregation, interpretation and association of events from different sources [15]. The primary capabilities of today's SIEM solutions are threat detection, incident response, and log management.

In addition, Singh et al. [8] pointed out that Intrusion Detection Systems (IDS) is another type of security tool that can be used to improve the security of communication and information systems in the same way as firewalls, antivirus software and access control systems are often used. IDS is a type of computer or application program that monitors system or network operation for policy violations or malicious activities and sends a report to the management station [16]. Even though this intrusion detection technology is still in its infancy, it should be treated as a reliable protection. Azodolmolky et al. [17] argue that IDS plays some important role within the information security architecture.

5. DISCUSSION

The advancement of information, communication, and technology has coincided with the advent of a slew of cyber security threats and flaws. Data protection is an issue that requires a type of intentional act that can impact the three fundamental properties of a given information system. The first property is confidentiality, which is the right of a network or computer system to safely store relevant information that is deemed important to the organization and to protect those elements of exclusive access only to relevant users configured for that function [18]. The second property is integrity, the guarantee that all available programs and data or information are properly planned and adjusted only in the manner allowed or appropriate by the authorities of the organization. Reliability/availability is the last property of a protected information system, ensuring that the computer network and the whole system are available to all relevant company stakeholders without any sort of delays or blackouts [19].

The cyber security risk has the potential to affect individual users, both large and small business organizations, resulting in a variety of financial effects, such as money theft, digital assets and confidential information.

Despite the complexities of cyber security, small companies are continually undergoing radical changes in order to embrace the new information age, as a result, they've always had to rely on information technology to manage some crucial part of their key service deliveries, and as a result, it's become a valuable tool for the organization's information.

It is essential for an organization's information technology security management to select IT security management resources that can be identified as best practices and standards. The Security Incident Event Management (SIEM) framework is an effective tool in this scenario. SIEM tools help security analysts gain insight into the security threats that target a given business organization's IT systems [20]. This is achieved by analysing network device-generated logs and looking for signs of an ongoing attack. The SIEM device must be able to compare a large number of logs from different sources and detect an attack with a high detection rate and a low false positive rate. This must be achieved when prioritizing warnings so that security analysts can concentrate on the system's high-threat alerts.

6. CONCLUSION

In several cases, cyber-attacks have been aimed at various organizations' information, communication, and technology networks. Hackers and intruders today have access to cutting-edge technology that enables them to gain access to an organization's information system. For any business enterprise to be protected from cyber threats, they need a comprehensive protection framework such as antiviruses, firewalls, and the SIEM tool that can secure current computer networks from dangerous threats.

Intrusion Detection Systems (IDS) is another type of security tool that can be used in the same way that firewalls, antivirus software and access control systems are often used to improve the security of communication and information systems.

ACKNOWLEDGMENT

Special thanks for Umm Al-Qura University for their support and assistance.

REFERENCES

[1] Borrett, M., Carter, R., Wespi, A. (2014). How is cyber threat evolving and what do organizations need to consider? Journal of business continuity & emergency planning, 7(2): 163-171.

[2] Fischer, E.A. (2014). Cybersecurity issues and challenges: In brief. Library of Congress. Congressional Research Service, Washington D.C.

[3] Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. Wireless Networks, 20: 2481-2501. https://doi.org/10.1007/s11276-014-0761-7

[4] Onimisi, A.C., Nonyelum, O.F. (2018). Evaluation and analysis of cyber attacks in Nigeria. IUP Journal of Information Technology, 14(1): 16-29.

[5] Wanyoike, D.M., Mukulu, E., Waititu, A.G. (2012). ICT attributes as determinants of internet social network adoption by formal small enterprises in urban Kenya. International Journal of Arts and Commerce, 1(7): 48-60.

[6] Weru, T., Sevilla, J., Olukuru, J., Mutegi, L., Mberi, T. (2017). Cyber-smart children, cyber-safe teenagers: Enhancing internet safety for children. 2017 IST-Africa Week Conference (IST-Africa), Windhoek, Namibia, pp. 1-8. https://doi.org/10.23919/ISTAFRICA.2017.8102292

[7] Sim, J., Saunders, B., Waterfield, J., Kingstone, T. (2018). Can sample size in qualitative research be determined a priori? International Journal of Social Research Methodology, 21(5): 619-634. https://doi.org/10.1080/13645579.2018.1454643

[8] Singh, J., Pasquier, T., Bacon, J., Ko, H., Eyers, D. (2016). Twenty security considerations for cloud-supported Internet of Things. IEEE Internet of things Journal, 3(3): 269-284. https://doi.org/10.1109/JIOT.2015.2460333

[9] Internet security threat report (2016). Symantec Product Inc; Virginia. USA.

[10] Tounsi, W., Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber-attacks. Computers & Security, 72: 212-233. https://doi.org/10.1016/j.cose.2017.09.001

[11] Patel, M., Patel, N. (2019). Exploring research methodology: Review article. International Journal of Research and Review, 6(3).

[12] Pham, L.T. (2018). A Review of key paradigms: Positivism, interpretivism and critical inquiry. Doctoral dissertation, University of Adelaide.

[13] Rahman, M.S. (2016). The advantages and disadvantages of using qualitative and quantitative approaches and methods in language "Testing and assessment" research: A literature review. Journal of Education and Learning, 6(1): 102. http://dx.doi.org/10.5539/jel.v6n1p102

[14] Regnault, A., Willgoss, T., Barbic, S. (2018). Towards the use of mixed methods inquiry as best practice in health outcomes research. Journal of Patient-reported Outcomes, 2(1): 19. https://doi.org/10.1186/s41687-018-0043-8

[15] De Vaus, D. (2012). Surveys in Social Research. London: Taylor and Francis. https://doi.org/10.4324/9780203519196

[16] Yin, R.K. (2016). Mixed methods research are the methods genuinely integrated or merely parallel. Research in the Schools, 13(1): 41-4 https://doi.org/10.7176/JLLL.350401

[17] Azodolmolky, S., Wieder, P., Yahyapour, R. (2017). Cloud computing networking: Challenges and opportunities for innovations. IEEE Communications Magazine, 51(7): 54-62. https://doi.org/10.1109/MCOM.2013.6553678

[18] Carlin, J.P. (2016). Detect, disrupt, deter: A whole-of-government approach to national security cyber threats. Harvard National Security Journal, 7: 391-577.

[19] Datta, R. (2018). Traditional storytelling: An effective Indigenous research methodology and its implications for environmental research. AlterNative: An International Journal of Indigenous Peoples, 14(1): 35-44. https://doi.org/10.1177/1177180117741351

[20] Flores, D.A., Qazi, F., Jhumka, A. (2016). Bring your disclosure: Analysing BYOD threats to corporate information. Paper presented at 2016 IEEE International Conference on Turst, Security and Privacy in Computing and Communications, Tianjin, China.