American Journal of Multidisciplinary Research & Development (AJMRD)
Volume 03, Issue 07 (July- 2021), PP 23-26
ISSN: 2360-821X
www.ajmrd.com

Research Paper **Open Access**

Information systems security in the age of pandemics: COVID-19 and beyond

Dismas Kitaria[1], David Kibara[2]Stephen Mageto[3],Patrick Njuguna[4]
[1,2,3,4]Computer Science Department, Meru University of Science and Technology, Kenya
**Corresponding Author: DismasKitaria*

ABSTRACT: In the wake of the COVID-19, most organizations have had to invest in different information systems to facilitate virtual working and meetings between organizations to ensure adherence to the COVID-19 prevention guidelines. This presented a new challenge of information systems security, which most organizations may not have been ready to handle or manage. As a result, organizations have had to change how they view information systems security. This new unfolding of events has presented an opportunity for cybercriminals to exploit the crisis, which involves some laxity in security measures to accommodate the new working formula and focus shifting to the pandemic. Due to the increased risks and challenges to information systems, organizations have understood the need to invest in information systems security. To address human actions as a source of risk to information systems, organizations have and should develop appropriate interventions such as cybersecurity awareness campaigns, governance frameworks, and protocols. Even beyond the COVID-19 era, the policies, protocols, and guidelines that organizations have developed to prevent attacks on information systems will become operations guiding policies.

Keywords: *cyberattacks,cybercriminals*, COVID-19*, information system security*

I. Introduction

In the wake of the COVID-19, most organizations have had to invest in different information systems to facilitate virtual working and meetings between organizations. While this move has helped organizations remain operational in a manner that adheres to the COVID-19 prevention guidelines, it presents a new challenge of information systems security, which most organizations may not have been ready to handle or manage. There have been different technological innovations that have been developed, including information systems and technology geared towards making a positive contribution to the global pandemic [1]. As the COVID-19 pandemic continues to rage across the world, it affects all aspects of life as we previously understood but presents different perspectives where information systems can positively contribute [2]. Organizations have had to change how they view information systems security. Remote working during the COVID-19 pandemic has seen most people working from their homes, using their own computers, routers, and virus protection. There is a need to consider cybersecurity protection for people to invest in for protection against possible hacker attacks, which might expose an organization's highly sensitive information [3]. The purpose of this research review paper is to provide a comprehensive review of the literature on information systems security in the age of pandemic and even beyond the pandemic.

II. Definition

It is important to understand the meaning of information systems and information systems. Several definitions have been proposed to explain the term information system.In general terms, an information system refers to "a system of people, data records and activities that process the data and information in an organization, and it includes the organization’s manual and automated processes" [4].An information system may be considered as “computer-based systems, which are combinations of hardware, software, and telecommunications networks that people build and use to collect, create, and distribute useful information” [5]. One of the most relevant definitions of an information system is one that considers it as a working system. An information system is "a work system whose processes and activities are devoted to processing information, i.e., capturing, transmitting, storing, retrieving, manipulating, and displaying information" [6]. Information system as a working system involves human participants and machines working on processes and activities with information technology assistance. Information system security can be defined as the "application of any technical methods and managerial processes on the information resources (hardware, software and data) in order to keep organizational assets and personal privacy protected" [7]. Another closely related but different term is information system management, which refers to "a set of activities involved in configuring resources to meet an organization's information security needs" [8]. The purpose of information system security is to secure information in the systems to ensure that the information within the information systems is to retain its confidentiality, integrity, and availability [9]. This narrative review seeks to examine how in the current age of the COVID-19 pandemic, information systems security is facing various challenges and solutions implemented to protect the confidentially, integrity, and availability of the information in information systems and assess whether such solutions would last beyond the pandemic era.

III. Risks and Challenges to Information Systems Security during the Pandemic Era

As a response to curb the spread of COVID-19, health guidelines on maintaining physical distance led to national lockdowns, which made people and organizations dependent on technologies to carry on their business. Therefore, it is apparent the pandemic has led to drastic changes to business models, contributing to the phenomena of "working from home," where employees are remotely connected to the organization's corporate information systems infrastructure [10]. This new unfolding of events has presented an opportunity for cybercriminals to exploit the crisis, which involves some laxity in security measures to accommodate the new working formula and focus shifting to the pandemic. This leads to a challenge where the global economy has to deal with both the COVID-19 pandemic and cybersecurity warfare, where there are increased risks for the occurrence of cybercrimes [10]. A notable challenge of the "working from home" phenomenon is that most personal information technology devices tend to be poorly configured relative to the work-based information systems, making the home devices more prone to cyberattacks [11]. A report by Delloite observed that even with the increase in technology need, most organizations filed to avail a cyber-safe remote-working environment, which has contributed to increased exposure to cyber risk. Cybersecurity experts have estimated that the incidents of cybercrimes and attacks have almost doubled in the wake of the COVID-19 pandemic [12]. The cybercriminals have exploited the opportunity presented by the unprecedented havoc due to the COVID-19 pandemic to carry out attacks on information systems and steal or distort sensitive information.

Different industries face different challenges and risks to information systems security. The health sector is one of the industries whose information cybercriminal attacks have often compromised systems security. It has been identified that COVID-19 has challenges in the health care information system [13]. It has been observed that cyber attackers have sought to exploit the crisis of the COVID-19 pandemic and carried out attacks against health care organization's information systems [14]. The World Health Organization has identified that during the COVID-19 pandemic period, the number of cyber-attacks has increased five-fold, with the increased cyber risks arising from the actions of people and systems and technology failures [15]. It has been observed that "the main changes to health services caused by the COVID-19 pandemic include decreased mobility, border closures, and the increasing reliance on remote work, often carried out with little previous experience and planning" [13]. Another sector affected by the COVID-19 pandemic is the e-Commerce sector. Most small and medium-sized commercial stores have shifted to the digital platform to sustain their business following the pandemic. It has been reported that the financial sector has been affected by hackers relatively more than other sectors during the COVID era but are also has a leading edge in their response to the cyber risk [16]. The extent of information systems security exposure to the risk of attacks is evident from the increased attacks on organizations. These attacks have affected even the large organization such as "World Health Organization (WHO), World Bank, US Centers for Disease Control and Prevention (CDC), the Gates Foundations, the US National Institutes of Health (NIH), the Wuhan Institute of Virology" [17]. Organizations from different sectors have been compelled to shift to holding online meetings using different platforms such as zoom during the pandemic. The online meeting platforms have presented a major weak point for attacks, which hackers have exploited to pose a threat referred to as "Zoom bombing" [17]. Therefore, it is apparent that different industries have been affected by the increased risks and challenges to information systems security.

IV. Solutions to Risks and Challenges to Information Systems Security during the Pandemic Era

Due to the increased risks and challenges to information systems, organizations have understood the need to invest in information systems security. Organizations have had to invest in their capacity to counteract cyberattacks in an effort to protect their information system. Among the notable solutions to prevent attacks on information systems is remote working security assurance. With remote working being an integral part of many business models, including the healthcare services delivery model, employees have been prompted to utilize enterprise remote desktop protocols and virtual private networks (VPN) to access corporate networks [13]. Other security features have been added to support the "working from home" phenomena, such as the use of a firewall, whitelist, and multifactor authentication. In addition, organizations offering video conferencing platforms have taken initiatives to improve the security of their platforms to improve the security of information systems. For example, Zoom has been forced to evaluate and improve its security measures, such as improvement in end-to-end encryption. It is noted that Zoom Video Communications initiated end-to-end encryption with the aim of protecting conversation during the meeting even from insiders in Zoom company itself [18].

Among the factors contributing to increased risks to information systems security is human factors. To address human actions as a source of risk to information systems, organizations have and should develop appropriate interventions such as cybersecurity awareness campaigns, governance frameworks, and protocols. Cybersecurity awareness campaigns and educational programs would be an essential intervention to address threats to information system security. Such training and awareness campaigns would equip the employees with skills to identify possible threats and urge them to be vigilant and collaborate to combat cybercrime, especially in the COVID-19 era [10]. In addition, organizations have been urged to implement a cybersecurity governance framework addressing issues such as good cyber hygiene, verify sources, and get official updates [19]. Information system security protocols provide guidelines to employees engaged in remote working, which is a norm during this COVID era.

Among the solution proposed to improve information systems, security is the use of artificial intelligence. This intervention involves using artificial intelligence to identify and prevent threats before there is an establishment in the information system [17]. An artificial intelligence solution would involve a collective of data for service and analyzing it to establish patterns or common attacks. Such a solution is expected to be effective during the COVID-19 pandemic era, characterized by more frequent attacks, whereby speeding up the machine learning process and preventing information system cyberattacks would be more effective [17].

V. Implications Beyond COVID-19 Era

While the COVID-19 has opened a window of opportunity to organizations to shift into the digital platform, it has also exposed a laxity in their information systems security. The pandemic has made it clear that my organizations should invest in information system security and have plans to minimize possible cyberattacks. Even beyond the COVID-19 era, the policies, protocols, and guidelines that organizations have developed in response to preventing attacks on information systems will become operations guiding policies. Organizations will continue taking proactive measures to improve information system security. Industries will develop sector-wide guidelines to govern information system security. Organizations offer remote work platforms has been made to realize vulnerabilities in their systems, which will become keener addressing such threats even beyond the COVID-era.

VI. Conclusion

The ongoing COVID-19 has exposed the vulnerabilities of information system security. The COVID-19 has changed the business model in most industries, with the most notable change being the increased adoption of the "working from home" arrangement. Another notable observation has been that there is an increase in attacks on information systems. A key advantage of this research paper review is that it has reviewed different sources and thereby provided a broader perspective on information systems security during COVID and beyond. However, one of the limitations of this study is that since it uses secondary data, the research had no control over the quality of the evidence. Nevertheless, the study findings can be applied by the management of any organization seeking to improve its information systems security.

References

[1] He, W., Zhang, Z. J., & Li, W. (2021). Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. *International journal of information management*, *57*, 102287. https://doi.org/10.1016/j.ijinfomgt.2020.102287

[2] Ågerfalk, P. J., Conboy, K., & Myers, M. D. (2020). Information systems in the age of pandemics: COVID-19 and beyond.

[3] Wang, L., & Alexander, C. A. (2021). Cybersecurity during the COVID-19 pandemic. *AIMS Electronics and Electrical Engineering*, *5*(2), 146-157.

[4] Paul, R. J. (2010). What an information system is, and why is it important to know this. *Journal of computing and information technology*, *18*(2), 95-99.

[5] Jessup, L. M., & Valacich, J. S. (2008). *Information systems today: managing in the digital world* (Vol. 3). Upper Saddle River, NJ: Pearson Prentice Hall.

[6] Alter, S. (2008). Defining information systems as work systems: implications for the IS field. *European Journal of Information Systems*, *17*(5), 448-469.

[7] Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*.

[8] Singh, A. N., & Gupta, M. P. (2019). Information security management practices: Case studies from India. *Global Business Review*, *20*(1), 253-271.

[9] Lundgren, B., & Möller, N. (2019). Defining information security. *Science and engineering ethics*, *25*(2), 419-441.

[10] Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1), 1-11.

[11] BA, O., OM, O., Sobowale, A. A., Nnamdi, O., Adebimpe, E., & OO, A. (2020). Cyber Security Threats in the Era of COVID-19 Pandemic: A Case Study of Nigeria System. *International Journal of Advanced Research in Engineering and Technology*, *11*(9).

[12] Omodunbi B. A., Odiase P. O., Olaniyan O. M., Esan A. O (2016):; Cybercrime in Nigeria: Analysis, Detection and Prevention. InFUOYE Journal of Engineering and Technology Vol 1 Issue 1, Pp 37-42

[13] He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *Journal of medical Internet research*, *23*(4), e21747.

[14] Stein S, Jacobs J. Cyber-attack hits U.S. health agency amid Covid-19 Outbreak. Bloomberg. 2020 Mar 16. URL: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response

[15] Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber Risk in Health Facilities: A Systematic Literature Review. *Sustainability*, *12*(17), 7002.

[16] Aldasoro, I., Frost, J., Gambacorta, L., & Whyte, D. (2021). *Covid-19 and cyber risk in the financial sector* (No. 37). Bank for International Settlements.

[17] Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H., & Fatima, Z. (2020). Cyber Attacks in the Era of COVID-19 and Possible Solution Domains.

[18] Isobe, T., & Ito, R. (2021). Security Analysis of End-to-End Encryption for Zoom Meetings. *IACR Cryptol. ePrint Arch.*, *2021*, 486.

[19] Abukari, A. M., & Bankas, E. K. (2020). Some cybersecurity hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. *International Journal of Scientific & Engineering Research*, *11*(4), 1401-1407.