Print ISSN: 0976-2876 Online ISSN: 2250-0138

Available online at: http://www.ijsr.in

INDIAN JOURNAL OF SCIENTIFIC RESEARCH

DOI:10.32606/IJSR.V12.I2.00007

Received: 12-09-2021 Accepted: 14-12-2021 Publication: 31-01-2022

Indian J.Sci.Res. 12 (2): 45-49, 2022 Original Research Article

CYBERSECURITY RISKS IN THE HEALTHCARE INDUSTRY

RAVINDRA PATEL[1]

Department of Computer Science, 1 University Drive Campbellsville, KY, USA

ABSTRACT

Cybersecurity risks have been the recent challenge in most organizations transmitting their data into cloud computing. The challenges of cybersecurity may range from external sourcing to internal sourcing. This depends on the sector that has been undermined by the specific risk. This research paper has focused on the cybersecurity risks in the health docket. The paper has elaborated on the background of the primary cause of the risk in the health industry. Further, the primary challenges experienced by the hospitals and the health centers were elevated. The benefits of mitigating the cybersecurity issues in the health centers also elaborated in detail. Obstacles to achieving the benefits are well defined, focusing on a lack of resources and the organizations' management level. Several innovations made to curb the networking insecurity phenomenon are also profoundly elaborated. The paper researches the actual sources and the impact of the cybercrimes in health industries. Findings showed that most of the sources of risk got triggered internally.

KEYWORDS: Cybersecurity, Risk, Cloud Computing, Health Care, Research, Threat, Obstacles, Innovations, Methods, Organizations

With the continued support of the healthcare industry in providing life-critical services, through working to enhance patient care and efficient treatment using the new technologies, cyber threats and crimeless looks are focusing on exploiting the vulnerabilities in the system. The vulnerabilities may have resulted from the external or internal factors in the health care industry (Kim and Zakson, 2015). New technologies, however, optimally improve the health care system by enhancing effectiveness and efficiency. The health care system's significant challenges include imposing malware in the systems, compromising the systems' optimistic integrity, and leakages of the patient's data. Indeed, most health institutions have lost trust and reputations among public members due to the cybersecurity attack. Ideally, such health centers may have optimal services in the treatment and provision of the services, but with their virtual services affected, the quality is greatly affected. Considering the revolution in the advancement of technology, having a stable system is critical. Most of the services are operated and processed through the IT infrastructures, particulate in the health sector (Coventry & Branley, 2018).

CYBERSECURITY THREATS IN THE HEALTHCARE INDUSTRY

Ransomware

Ransomware is a software attack that affects the system and demands subscriptions or direct pays to recess the services. In the health care industry, the malicious attack targets assets such as the computer containing the patient's data (Kruse *et al.*, 2017). In such cases, the ransomware may not manipulate or affect the patients. However, data for the operations to processed health care staff requires regular patient data access to acquire the medical history and information. The prompt to pay to access the data is, therefore, not inevitable. Indeed attempts to reverse the attacking technique through security costing may be expensive and time-consuming. Attackers of ransomware use the method and request payments, which are reasonable compared to the time and resources the health care center may require to revert the process. The health care centers' management should install antiviruses and detect devices in their systems to prevent such attacks (Strielkina *et al.*, 2018).

Intentional Insider Threats

Intentional insider threats have been alarming in the health care industry. Detecting the insider threats as they may be part of the team managing the health care industry (Meng *et al.*, 2018). Insider threats are common in a big hospital where the organizations' data and sensitive information is compromised. Identifying the compromise sources is also a challenge in most cases, especially amongst those in the high management of health care industries. There is their reason which may result in the insiders' attack. Threats include having been bribed, recruited, or motives from the grades, particularly

[1]**Corresponding author**

in disgruntled employees. The intruder attacker employs using a formal process but later develops an unethical interest in conducting security activities in the system. In such cases, the challenge of identifying such people is high because of the trust and the goodwill they have developed amongst other members of the health care industries. Bribing is most common in the health sectors. Groups of individual cybercriminals can bribe health workers, especially those working in the data analysis departments. Such bribed members fetch information and data of the patient and the health departments using devices such as the flash disks and giving out the credentials to access individual accounts. In turn, it gets compensated through money or a secured job elsewhere. The information leaked is commonly used to spoil the institutions' health care sectors' reputations for competitive purposes or wrong motives, which, amongst the workers, can as well result in cybersecurity bin the organizations. They may have been due to the dissatisfaction of the workers of dictatorship from the top management. In such cases, the patients' data may become compromised, and the payment process may also be affected. This results in information leaks on the payments and the medical history of the different patients in a particular institution (Strielkina *et al.*, 2018).

Distributed Denial of Services (DDoS)

The DDoS attack is a widespread technique, tactic, and a procedure used by cybercriminal attacks to affect the network to the point of inoperability (Elam, 2020). The attack can pose a major challenge in the health sector, which requires constant access to the network. Without access to the system, health workers may not receive the records and prescriptions and provide proper treatment to them. Indeed most of the health care center has evaluated all of their activities in the cloud computing services. An issue related to accessing o the information from the services provider can affect all the health center departments. Today with the advancement in technology, hackers and cybercrimes are using the DDoS attack on the health care industry, upholding the negative impact they cause to the whole sector. The DDoS attack is employed with political motives. Through this, healthcare in a particular region can cause a high community inference that translated to political aspects (Hoffman, 2020).

Data Breaches in the Health Sector

Every day hospitals are reporting new cases of data breached. This phenomenon has been gradually rising with the current advancement in technology. Data breaching is fatal to the health state of any organization. Data breaches may be external intruders in the health care industries, loss of a device with the patient, and the hospital data from the insiders. The data breaches' primary motives are the legal requirements in insurance services and the accountability Acts programs. Through the insurance services, cybercrimes use the data to claim payments from the insurance companies; research shows that most insurance companies' claims experience high interferences when dealing with the health sector than other sectors like vehicle claims and compensations. The breached data used to make payment to an individual who claims to the insured patients. In the accountability Act, the data's breaching is conducted to hand certain unaccountable activities. Managers and directors in the health actors use the method to boost their performance measurements (Muthuppalaniappan and Stevenson, 2021).

Email Compromise

The email compromise of the information is sensitive to the organization. Hacking health care emails results in sidestepping on email activities such as filtering (Snellings, 2020). This results in the email displaying messages in the networking systems without requesting the encryption procedures. Most of the communication in the health care services are transacted through email platforms. Email platform is preferred due to its ability to retrieve and the formality in displaying the data and the information. However, having the system hacked, information such as the confidential emails amongst managing the directors and the patient's records are easily compromised (Muthuppalaniappan and Stevenson, 2021).

Additionally, the mail system is electronic; therefore, the attack may result in malware installations to the devices holding the accounts. Other email attacks will cause misbehaving, where the platform creates emails and automatically sends it to various individuals or organizations. Messages may also have created, which are codded in unethical language or ethically, to request individual favors from other organizations. Such communications are fatal in the health care industry as they can result in conflicts amongst management or the significantly affected hospitals stakeholders (Muthuppalaniappan and Stevenson, 2021).

BENEFITS OF CURBING CYBERSECURITY RISKS IN THE HEALTH SECTOR

Financial Security is Assured

Ideally, the health care organization's primary purposes are to offer quality medical services and

maximize their profits. Without a systematic financial system, the health sector may face management challenges and the operations of their services (Ervural, 2018). Hackers aim to affect the health institutions' financial assistance to make fetching the finds and distort the systems to curb the health sector from overrating efficiently. As addressed above, Ransomware malware focuses on fetching the health sector funds. The demand to pay the amounts So that the hospital can progress with their services is fatal and can vastly affect its financial status. Therefore, to have a stable financial position in the health sector requires setting in the security of the system to avoid the high risk that may be more expensive. Having a secured system also helps in avoiding operations such as disaster recovery activities. These activities are expensive and may cost organizations high costs (Razaque *et al.*, 2019).

Keeping the Information of the Patients Confidential

Confidentiality in the health sector is crucial, as the organizations' principles cover most of the documents. It is offensive to disclose the patient medical records ton authorized people, especially those not family members. Through unethical activities such as cyber-criminal activities, information, and essential ant details are compromised (Jalali and Kaiser, 2018). This data may manipulate the system and confuse the services' offering through the IT infrastructures. Compromising may also lead to fatalities as different patient records get manipulated, resulting in wrong medications. Therefore, having a curbing strategy is crucial to patient privacy and the confidential health care center documents (Thames and Schaefer, 2017).

Obstacles Faced When Curbing The Cyber Security Risks In The Health Care Industries

Here are two common obstacles experienced when eliminating the risk related to cybersecurity. The obstacles include Failure of the corporation and lack of enough resources. The corporation is crucial in any organizational setups; indeed, if there is no systematic corporation between the employees, management, and stakeholders, they are motives for breaching data. Employees managing the system's security system should be well managed with refreshment training to improve the skills and know-how of dealing with the emerging insecurities. If there is a disconnect between the stakeholders, the management, and the security system experts, the networking system is left vulnerable in the managing team's hands. External intruders also take advantage of the health center with no substantial cooperation by invading their systems and breaching their data (Thames and Schaefer, 2017).

Lack of resources is also a significant obstacle facing the health sectors. Most cybersecurity threats get identified in the health sectors; however, having the solutions implemented may be expensive (Berger and Jones, 2016). The cost of having the implementation of the antivirus and then security site detectors is very high. Most of the small health institutions may have the challenge of implementing such devices. This has resulted in more challenges of the system and management challenges. Regular losing of the information and the data breaches has also raised conflicts. Although the source of these conflicts is taken from the inability to secure them due to scarcity of resources, organizations should plan to mitigate the risk to avoid the vast losses experienced.

Innovations in Health Care Services Cyber Security

Innovations in cybersecurity services include new development of the antiviruses and detection devices and installing the Artificial Intelligent (AI) technology in the systems. Compared to traditional networking systems, having AI devices can detect and eliminate the networking systems' risks. For instance, installing the AI software in the data warehouse of the health services industries would help unusual links and traffics directed to the data. Through this, the AI devices may alert the security team or automatically barrier the traffic from accessing the data. This has periodically helped in major hospitals where the sensitive and the patient data is prone to risk. New antiviruses have also been developed with algorithms to solve networking issues (Ahmed and Ullah, 2018). The computing services in the health sector are mostly used for communication among medical practitioners. Additionally, communication between external organizations is also conducted using networked computers. With the advanced antivirus, it is difficult for links sent to the computers to affect the information and data storage (McFarland and Olatunbosun, 2019).

METHODOLOGY

Summary and the Key Ideas of the Methodology

During the research to assess the cybersecurity risk in the health care centers, we adopted the qualitative research method, which included conducting interviews with the medical practitioners and the security team manning the medical institutions' systems. Throughout the research, the primary purpose was to know the sources of the risks and how frequent the system's risk

has been recurring. The effect, especially to the data and the health sector's sensitive information, impacts the overall health institutions and the possible solutions different hospitals have adopted to reduce the impacts. Different hospitals had different responses depending on the IT infrastructures' investment level and the preparedness towards the cybersecurity risks. Those with much connectivity of the networking infrastructures were more prone to the threat, while those with few IT infrastructures become less exposed to the risks (Le *et al.,* 2019).

Measurements

Despite concentrating on the qualitative research method, the research also involved some measurements that compare the risk in different hospitals, which, calculated as Risk=Likelihood × Impact. The like hood of the insecurity occurrence was different in the four hospitals which participated in the research. Those who had been affected before portrayed a high likely hood of the risk reoccurring again. Those that never got attacked by a cybercriminal activities showed a low likelihood of the risk occurrence. The medical practitioners in the less likely medical center responded that they feel they cannot be a target since they have never experienced the attack. However, after analyzing their systems' condition, it portrayed a need to have the software installed in their systems. Simultaneously, the impact on the affected hospitals was high despite having made efforts to prepare against the occurrence of such risks (Le *et al.,* 2019).

Analytical Discussions

After assessing the results from the hospitals and the impact of cybersecurity, it is clear that having networking security is critical. It is evident from the hospitals which had not to experience the cyber insecurity before. This hospital was more prone to the risks. If an attack has to be conducted at that particular time, the hospital could lose more than the hospitals which had implemented antiviruses and security detections devices in their systems. Additionally, the analysis of the impact is solely dependable on the size of the organizations. Ideally, having vast data and information, the networking systems, and the infrastructure is more riskers during the attack. There is a high possibility of losing much data and information as compared to those with fewer data. However, this should not become a reason or storing data and information in the systems. Indeed researches show that having data in the systems is faster inaccessibility, thus saving time and resources. Specifically, the health sector is much efficient when the data is uploaded in the systems. Medical records are easily retrieved, and referrals, comparisons, and contrasting can be conducted quickly. The analysis reflects that to have this applied efficiently, we will require to have secured systems and all the organization's IT infrastructures (Le *et al.,* 2019).

Additionally, the level of the impacts can be reduced by having a well-managed health care setup. Management sometimes affects risk occurrence. Disadvantageously, the effect is commonly negative, where management fails to assign enough resources to mitigate the organization's possible risks (Sardi *et al.,* 2020). Management may also affect the security team by not providing them with the required tools to mitigate the risks, mostly due to un-cooperation between the organizations and the team managing the security system. Analytically, a hospital with ineffectively managed is prone to cybersecurity threats as compared to those with good management. Once the impact of cybersecurity has been experienced, Failure to cooperate and solve the issue may also create room for other risks. For instance, if the data gets breached, the management should engage all the members to recover or backup the data to avoid further breaching before tacking on other precautions (Elam, 2020).

CONCLUSION

Addressed Cybersecurity risks have been a manger Challenge in the health sectors. Factors such as mismanagement, loss of data and information, breaching, and the credential invading are common challenges. Due to the cyber insecurity, most health institutions have lost the grip move offering quality services, thus losing reputation and the competitive advantage in the industry. Internal intruders are defined as the major sources of insecurity in the health setups. The notation of trusting the n employees has undermined most hospitals, resulting in high costs of recovery and time consumptions. It is advisable to have the employees conduct their activities with the ethics and the organizations' principle. Without adhering to this, it is resulting in employees participating in cyber insecurity activities. Therefore, health sector management should be observant of employee's activities and implement the necessary instruments to curb the system's insecurity.

RECOMMENDATIONS

It is recommendable for the health care sector to install antiviruses and have coherent management of the networking system. This is important because, without coherence, the installed insecurity detectors and antivirus software may be compromised. The fact that email compromising has also been a challenge in most hospitals

and health departments, having only authorized individuals accessing the mail, could help curb this conduct. Most of the information was leaking and breached because of a lack of confidentiality mongers the workers. Therefore, apart from installing the software in the systems, it's crucial to have the management adhering to the precautions to curb cybersecurity risks in the organizations.

REFERENCES

Ahmed M. and Ullah A.S.S.M.B., 2018. Health Care Security Analytics. CRC Press, ISBN-13: 9780429446177 pp, 427-440.

Berger H. and Jones A., 2016. Cybersecurity & ethical hacking for SMEs. In Proceedings of the 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society (pp. 1-6).

Bhuyan S.S. Kabir U.Y., Escareno J.M., Ector K., Palakodeti S., Wyant D. and Dobalian A., 2020. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. Journal of medical systems, **44**(5): 1-9.

Coventry L. and Branley D., 2018. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas, **113**: 48-52.

Elam A.G., 2020. The Obstacles that Smaller Healthcare Facilities Face from Subpar Cybersecurity (Doctoral dissertation, Utica College).

Ervural B.C. and Ervural B., 2018. Overview of cyber security in the industry 4.0 era. In Industry 4.0: managing the digital transformation (pp. 267-284). Springer, Cham.

Hoffman S.A.E., 2020. Cybersecurity threats in healthcare organizations. World Libraries, **24**(1).

Jalali M.S. and Kaiser J.P., 2018. Cybersecurity in hospitals: a systematic, organizational perspective. Journal of medical Internet research, **20**(5): e10059.

Kim J. and Zakson D., 2015. Health Information and Data Security Safeguards. J. Marshall J. Info. Tech. & Privacy L., **32**: 133.

Kruse C.S., Frederick B., Jacobson T. and Monticone D.K., 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care.

Le D.N., Kumar R., Mishra B.K., Chatterjee J.M. and Khari M., 2019. Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies. John Wiley & Sons.

McFarland R.J. and Olatunbosun S.B., 2019. An exploratory study on the use of Internet_of_medical_things (IoMT) in the healthcare industry and their associated cybersecurity risks. In Proceedings on the International Conference on Internet Computing (ICOMP) (pp. 115-121). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Meng W., Choo K.K.R., Furnell S., Vasilakos A.V. and Probst C.W., 2018. Towards Bayesian-based trust management for insider attacks in healthcare software-defined networks. IEEE Transactions on Network and Service Management.

Muthuppalaniappan M. and Stevenson K., 2021. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. International Journal for Quality in Health Care, **33**(1): mzaa117.

Razaque A., Amsaad F., Khan M.J., Hariri S., Chen S., Siting C. and Ji X., 2019. Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain. IEEE Access, 7, 168774-168797.

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

Snellings E., 2020. Cyber Threats on the Electronic Healthcare Record System (Doctoral dissertation, Utica College).

Strielkina A., Illiashenko O., Zhydenko M. and Uzun D., 2018. Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment. In 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 67-73). IEEE.

Thames L. and Schaefer D., 2017. Cybersecurity for industry 4.0. Heidelberg: Springer.