Advances in Informatics, Management and Technology in Healthcare
J. Mantas et al. (Eds.)

doi:10.3233/SHTI220739

Classification of Challenges and Threats in Healthcare Cybersecurity: A Systematic Review

Roaa ALJURAID[a,1] and Taghreed JUSTINIA[b]
[a] *College Health Sciences, Saudi Electronic University, Jeddah, Saudi Arabia*
[b] *College of Public Health and Health Informatics, King Saud bin Abdulaziz University for Health Sciences, Riyadh, Saudi Arabia*

Abstract. The rapid development of electronic health has highlighted the essential position information security holds today in the healthcare industry. Indeed, healthcare organisations have increasingly become targets for cyberattacks. The authors investigated cybersecurity challenges through identifying cases within the academic literature related to cybersecurity threats and vulnerabilities present within healthcare settings. The fast adoption of healthcare information systems has exposed the healthcare industry to numerous kinds of cyberattacks, thereby prompting the international academic community to investigate these threats. There are various cybersecurity challenges and vulnerabilities within healthcare that could later be exploited and lead to cybercrimes. As security systems continue to develop, the interest in cybersecurity as a form of defense and protection is expected to grow.

Keywords. Cybersecurity, health, healthcare, threats, ransomware, cybercrime, barriers, information security

1. Introduction

Cybercrime is a universal challenge that first appeared as the use of information technology (IT) stabilised internationally in the late 1970s [1]. The healthcare sector experiences far more dangers than others due to the inherent vulnerability of its systems. Healthcare systems contain certain weakness which can be exploited, resulting in damage to its functions, such as hardware, software, networks, operating system, medical devices, processes, and even people. Any possible vulnerability that can be exploited is considered a threat and must be eliminated accordingly [2]. The purpose of this research is to examine the existing literature so as to investigate cybersecurity's challenges and threats within healthcare, and how these vulnerabilities could most effectively be handled by the health information security theories.

[1] Corresponding Author, Roaa Aljuraid, Saudi Electronic University, Saudi Arabia; E-mail: roaljuraid@gmail.com.

2. Methodology

The structure of this review was based on the preferred reporting items for systematic reviews and meta-analyses (PRISMA). The systematic search started in August 2019. The following different online databases were queried: NCBI/PubMed, PMC, ACM Digital Library, Science Direct, IEEE Xplore, Google Scholar (GS), Saudi Digital Library, Springer, BASE (Grey Literature), and dblp (Grey Literature). The querying used a combination of the following keywords: cybersecurity, health, healthcare, threats, ransomware, cybercrime, and information security.

The literature was restricted to studies published in the English language and the publication between 2009–2019 were included. Moreover, the search included papers with keywords mentioned in the title/abstract, meaning that those without full text availability were included in the review. Grey literature was searched for so as to avoid publication bias and additional studies were manually identified from searching reference lists. A combination of several search queries was formed according to each database or search engine, followed by specifying the database filters according to the inclusion criteria. Once done, the studies were chosen by hand screening, for example, the following key terms with Boolean operators was used in PubMed: ((ransomware) OR (information security) OR (cyber security)) AND ((challenges) OR (threats)) AND ((healthcare) OR (health)). The papers included in this systematic review had to have discussed cybersecurity challenges in healthcare and the related security threats. And all the duplicated studies from the literature searches were excluded.

3. Results

The search revealed 234 potential records through the selected online databases, 11 studies were manually picked. The abstracts were read, and finally 62 articles were selected according to relevance to the topic. The studies distributed into 3 themes, which included 18 articles regarding the context of cybersecurity, 27 papers on cyber threats, and 17 relating to barriers to cybersecurity.

Further analyses were conducted, and the healthcare cyber threat's theme were divided into three main categories: cybersquatting threats, which includes hackers, spyware and malware attacks, viruses, and data breaches; insider threats, such as incompetent human behaviour resulting from recklessness, ignorance, curiosity (e.g., using another employee's password, etc.); and technological failures of hardware, software, infrastructure, and power. In this study, each category is further characterised as either deliberate or accidental threats that could potentially lead to vulnerabilities. The threat level was determined according to potential motives and harmful consequences, hence cybercrime (and intentional threat) and (unintentional) power failure that resulted in very severe results to health data are both considered as having high threat levels. Unintentional insider threats, such as human usability errors, were considered low threats. Table 1 displays the categories of cybersecurity threats.

This study also sought to investigate which threats and vulnerabilities violate the three core principles of information security (i.e., confidentiality, integrity and availability). In order to achieve this, the relevant academic literature have been examined. Moreover, the cascading consequences of these cyber threats have been explored. Table 2 determines the cybersecurity barriers or vulnerabilities that violate the three goals of the health information security theory.

Table 1. Famous threats in healthcare organisations.

Type of Threat	The Threat	Threat's Level	The Potential Motives
	Malware: Contagious Masked, Others (e.g., Ransomware)	Medium	Disrupt the system, preparing to break through the system.
		Medium	Disrupt the system, stealing sensitive information (e.g., login credentials).
		High	Obtaining money by demanding ransom, data breach is unlikely
	Denial of service attacks	High	Disrupt the system, preparing to break through the system, and demanding payment, data breach is unlikely
Cybersquatting	Phishing	Medium	Lead to data breach, obtaining sensitive information to sell on the dark web. May lead to other types of attack, such as ransomware and other misuses of data for financial gain
	Masquerade attacks	High	Obtain sensitive information and delete or modify health related information that could lead to harming the patients
	Data injection attack	High	Incorrect diagnosis, illegal insurance claim, and mission critical factors
	Hardware/software errors or failures	Medium	Usually unintentional, though could lead to unreliable services
Technological threats	Obsolete technology/out of date HIS	Medium	Usually unintentional, often resulting in untrustworthy and unreliable systems
	Critical infrastructure or power failure	High	Usually unintentional, but sever consequences could occur, such as data loss
Insider threats	Human usability error	Low	Usually from unintended negligence of the employees, hence, represents a serious risk to confidentiality and privacy
	Management weakness	Medium	Often unintentional due to staff and budget limitations, or overall lack of experience

Table 2. Cybersecurity barriers or vulnerabilities that violate the three goals of the health information theory.

Health information theory	Vulnerabilities	Threat	Cascading Consequence
Confidentiality	Password sharing	An authenticated access, phishing attacks, eavesdropping	Malicious use, such as harming the patients or selling data on the black market
Integrity	Typographical errors, data modification	False data injection attacks	Invalid data could severely harm the patient as the patient could receive incorrect treatment or medications
Availability	Timely availability of data, lack of data storage, or poor data maintenance	Denial of services attacks or technological threats, such as technological obsolescence	Delay of sensitive procedures, loss of data, loss of time and money

4. Discussion and Conclusion

There was an escalation in the rate of publication of related studies following 2012, with an exponential increase after 2016. This rate increase could be connected to the 2016 ransomware attack of the Hollywood Presbyterian Medical Center, which was the first highly publicised cyberattack against a hospital [1]. Numerous cybercrime incidents have since occurred, and the significance of cybersecurity has enormously grown in importance due to the WannaCry ransomware attack in May 2017, which affected many healthcare organisations throughout the world [3]. There are several studies have paid attention to the state of data breaches in the healthcare industry [4]. The studies concerning the theme of cyber threats have introduced and explored the concept of cybercrime and cyberterrorism threats [6][7]. Furthermore, as hacking continues to become a more destructive global phenomenon many have discuss the various cases of data breaches in the healthcare industry [5].

The core principles of information security include confidentiality, data integrity, and data availability [2]. Some of the unfortunate consequences of breaches to confidentiality are the malicious use of health records and their being sold on the dark web, and the use of data to harm patients [9]. Typographical errors are vulnerabilities that violate integrity, the term refers to incorrect data entry due to the clinical staff's lack of technical skill and is a common threat to the correctness and accuracy of electronic health records (EHRs) [8]. The unavailability of accessing data when needed is a potential concern for healthcare systems as they cannot afford any unavailability whatsoever [9]. The research themes and categories could be refined and further developed for future research. An overall lack of population amount was apparent. Nevertheless, interest in this topic continues to grow in line with cyber threats, thus highlighting the significance of comprehensive guidelines and standardised preventive measures. Future research could focus on defence mechanisms to cybersecurity threats in EHRs, or providing guidelines or standards for best practice measures.

References

[1] Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Vol. 25, Technology and Health Care. IOS Press; 2017. p. 1–10.

[2] Williams P and Woodward AJ. Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. Medical Devices: Evidence and Research 2015; 8: 305–321.

[3] Argaw ST, Bempong NE, Eshaya-Chauvin B, Flahault A. The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review. Vol. 19, BMC Medical Informatics and Decision Making. BioMed Central Ltd.; 2019.

[4] News From The Nation's Health. Vol. 107, No. 8, American Journal of Public Health [Internet]; 2017. p. 1195–1195. Available from: http://ajph.aphapublications.org/doi/10.2105/AJPH.2017.303913

[5] Gordon WJ, Fairhall A, Landman A. Threats to information security – Public health implications. Vol. 377, New England Journal of Medicine. Massachusetts Medical Society; 2017. p. 707–9.

[6] Frumento E. Cybersecurity and the Evolutions of Healthcare: Challenges and Threats Behind Its Evolution. In 2019. p. 35–69.

[7] Langer SG. Cyber-Security Issues in Healthcare Information Technology. Vol. 30, No. 1, Journal of Digital Imaging; 2017. p. 117–25.

[8] Bhartiya S, Mehrotra D. Threats and Challenges to Security of Electronic Health Records. Vol. 115, LNICST; 2013.

[9] Vinatzer BA, Heath LS, Almohri HMJ, Stulberg MJ, Lowe C, Li S. Cyberbiosecurity Challenges of Pathogen Genome Databases. Vol. 7, Frontiers in Bioengineering and Biotechnology [Internet]; 2019. Available from: https://www.frontiersin.org/article/10.3389/fbioe.2019.00106/full