Robert Morris University

Security in Healthcare Information Systems

Midterm Paper

Danielle Wicklund

Dr. Wenil Wang

INFS6440-B

November 17th, 2019

Security in Healthcare Information Systems

Imagine exiting the hospital after a six hour visit to the emergency room. Imagine hearing that the hospital you visited just experienced a data breach. Imagine discovering that your social security number and other private data were retrieved during this attack. Cyberattacks can create negativity in a patient's quality of care, even after the fact. The overall objective of my paper is to assess security, particularly that pertaining to computers, in healthcare systems. In addition, I will explain why cybersecurity is paramount to the medical industry.

Cybersecurity is one of my interests, which influenced my decision to pursue my master's degree in it. In fact, several of my social media accounts were hacked years ago. These hacking left me livid and exposed. Personally, I empathize with the frustration and vulnerability that victims of cyber crime endure. As a result, this is one of the reasons why I chose this topic. I want to understand how to fight the cyber criminals and help to protect peoples' sensitive information.

Besides being relevant in my own life, this technological issue is applicable to the health care field. Obviously, data breaches could result in litigation and immense costs. Furthermore, privacy and confidentiality of patient data are attributed to computer security. Therefore, many federal policies center on the secure access and protection of health information (Hebda et al., 2019, p. 102). For instance, "The Health Insurance Portability and Accountability Act of 1996 required the Department of Health and Human Services to develop regulations protecting the privacy and security of designated health information" (Hebda et al., 2019, p. 102).

Before this paper dives into the nitty gritty of healthcare cyber security, I will delve into its history. The first purported case of cybercrime can be traced back to the 1970s. Since its inception, cybercriminals have greatly refined their technological and hacking tools. These tools

include spam, viruses, and malware. "The health industry is an attractive target for cybercriminals as health data contains sensitive personal and financial information" (Kruse et al., 2017, pg. 1). Thus, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to curtail data breaches. HIPPA mandates healthcare entities to have physical and technical safeguards (Kruse et al., 2017, pg. 1). Unfortunately, cybercriminals have circumvented these measures, and this needs to be addressed.

Due to cybersecurity's infancy, there is insufficient evidence of interviews, equipment requirements, time requirements, and organization of the facility. On the other hand, there are a plethora of ways to confront this problem. First and foremost, the medical field must improve its development of an electronic infrastructure. Organizations are spending money and time on getting their healthcare technology integrated. However, they are not exerting as much effort into software upgrades (Kruse et al., 2017, pg. 2). To correct this issue, healthcare professionals must be made aware of this dilemma. If the healthcare IT infrastructure is penetrated, protection and patient confidentiality are lost. So, they need to invest in the maintenance of their technology (Kruse et al., 2017, pg. 8).

As mentioned in the aforementioned paragraph, healthcare providers do not understand the pertinence of security in healthcare information systems. Therefore, its value to HCIS and identification of the problem must be discussed. Primarily, the dilemma is healthcare's gravely flawed cybersecurity (Kent State, 2018). Also, security is imperative because of patient trust, patient privacy, and compliance with HIPPA (Kent State, 2018).

The application of good cyber hygiene is a way to address this problem. Healthcare providers and organization benefit greatly from effective cybersecurity. They do not have to con-

tend with litigation or expenses resulting from data breaches. The government like the Department of Health & Human Services can issue fines worth thousands or even millions of dollars (Morse, 2019). In 2017, a data breach could cost approximately $3.62 million (Kent State, 2018). To break it down further, this is equivalent to $408 per patient record (Morse, 2019). In addition, patients can be reasonably assured that their sensitive data is safeguarded. Otherwise, they may not be willing to share their data (Martin et al., 2017, pg. 2). Most importantly, "If clinicians do not have access to the right data because of malware, or if data has been compromised, it can mean life or death for a patient" (Kent State, 2018).

Subsequently, the technological aspect must be brought to attention. Healthcare's IT infrastructure is vulnerable because it is running on outdated operating systems. To demonstrate, hospitals in the United Kingdom are still using Microsoft Windows XP, which was phased out in 2014 (Martin et al., 2017, pg. 2). Next, cybercriminals have a wide variety of resources to attack medical organizations. For example, Hollywood Presbyterian Medical Center was infiltrated by phishing and ransomware (Cabrera, 2016, pg. 28). Furthermore, wearable devices like pacemakers can be hacked and used to gain access to networks (Cabrera, 2016, pg. 28). Therefore, personnel should be trained in cybersecurity protocols and respond swiftly to threats (Cabrera, 2016, pg. 28).

Afterwards, the benefits and drawbacks need to be discussed. To start with, "Cybersecurity is not just about protecting; it is fundamental for maintaining the safety, privacy, and trust of patients" (Martin et al., 2017, pg. 4). Likewise, health care providers would comply with regulations and improve the quality of health care (Cabrera, 2016, pg. 30). Nevertheless, such preventive measures are costly. These systems require purchasing cyber insurance and software with a

price tag of $1 million or more. Vendors will have to install and continuously monitor this software (Morse, 2019). Also, it is arduous to pinpoint threats that could hinder the hospital internally and externally (Kruse et al., 2017, pg. 7).

In conclusion, my analysis and summary highlight the importance of security in healthcare information systems. Not only does it ensure high quality care for patients, but it also helps the medical industry. Cybercrime is on the rise due to rapid innovation of technology and hacking tools (Cabrera, 2016, pg. 27). Case in point, there are myriad of ways to infiltrate these organizations. Most notably, wearable devices are emerging technologies subject to hacking. Unfortunately, we did not know that healthcare cybersecurity is plagued by underinvestment and inherent weaknesses (Martin et al., 2017, pg. 1). To illustrate, "The healthcare industry is lagging behind other leading industries in securing vital data" (Kruse et al., 2017, pg. 8). This is an ongoing issue that hospitals must correct immediately.

Thus, cybersecurity experts and medical personnel must be educated on threat prevention and strengthen the resilience of their technological infrastructures. Likewise, software upgrades and risk assessments must be continuously conducted (Morse, 2019). For your reference, a graphic is attached on the next page that suggests recommendations on how to enhance and maintain healthcare security (Kent State University, 2018). If hospitals have any doubt about practicing good cyber hygiene, they should ponder Florence Nightingale's quote, "The very first requirement in a hospital is that it should do the sick no harm."

6 Imperatives for HEALTHCARE CYBERSECURITY[1]

1. Define and streamline leadership, governance and expectations for healthcare cybersecurity

2. Improve medical device and health IT security and resilience

3. Develop the necessary healthcare workforce capacity to prioritize and ensure cybersecurity awareness and technical capabilities

4. Increase industry readiness with better cybersecurity awareness and education

5. Identify mechanisms to protect research and development efforts and intellectual property from attacks and exposures

6. Improve data sharing of industry threats, risks and mitigation

KENT STATE UNIVERSITY

1. Retrieved on February 28, 2018, from phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

References

Cabrera, E. (2016). Health care: Cyberattacks and how to fight back. *Journal of Health Care Compliance, 18*(5), 27-30. Retrieved from http://reddog.rmu.edu:2060/login.aspx?direct=true&db=buh&AN119552415&site=ehost-live&scope=site

Hebda, T., Hunter, K. & Czar, P. (2019). *Handbook of Informatics for Nurses & Healthcare Professionals* (6th edition). Upper Saddle River, NJ: Pearson Education.

Kent State University. (2018, February 28). *Security in healthcare information systems*. Retrieved from https://onlinedegrees.kent.edu/ischool/health-informatics/community/health-care-data-security

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology & Health Care, 25*(1), 1–10. https://reddog.rmu.edu:3345/10.3233/THC-161263

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ : British Medical Journal (Online), 358* doi:http://reddog.rmu.edu:2081/10.1136/bmj.j3179

Morse, S. (2019, July 30). Healthcare's number one financial issue is cybersecurity. *Healthcare Finance News*. Retrieved from https://www.healthcarefinancenews.com/node/139027