Chapter 14
Exploring Healthcare Cybersecurity Systems in the Age of COVID-19

Kevin Richardson
https://orcid.org/0009-0002-3212-8669
Edward Waters University, USA

Darrell Norman Burrell
https://orcid.org/0000-0002-4675-9544
Marymount University, USA

Horace C. Mingo
https://orcid.org/0000-0002-2395-2990
Marymount University, USA

Jennifer Ferreras-Perez
Marymount University, USA

Philip Shen
Marymount University, USA

S. Raschid Muller
https://orcid.org/0000-0002-1742-7575
Capitol Technology University, USA

Dustin Bessette
https://orcid.org/0000-0002-5482-6241
Mt. Hood Community College, USA

Katrina Khanta
Marymount University, USA

ABSTRACT

Unauthorized access to protected information in the healthcare industry is what constitutes a cyber breach. The repercussions of a data breach in cyberspace might be quite severe. Legal fees and settlements can result in a significant amount of additional expenses for leaders of organizations. When managing a data breach requires advance planning, it is possible to build a proactive and aggressive strategy to secure the data. It is essential to incorporate cybersecurity safeguards into information technology (IT) systems throughout the development stage in order to reduce the risk of being attacked by cybercriminals. Administrators of healthcare facilities now have the responsibility of managing both technological systems and clinical systems, which is especially important in the high-risk and high-vulnerability cybersecurity environment that has emerged in the wake of COVID-19. A systems dynamics method is taken in this chapter to investigate potential cybersecurity threats in the healthcare industry.

DOI: 10.4018/978-1-6684-7207-1.ch014

INTRODUCTION

As the importance of information technology to the healthcare industry continues to expand, the cybersecurity of the healthcare industry's information technology infrastructure is becoming increasingly significant (Burrell, 2022; Burrell et al., 2021). The pandemic produced by the novel coronavirus (COVID-19) has significant and long-lasting effects on the world's social and economic systems. In addition to other possible issues across various areas, it has brought many cybersecurity challenges that must be addressed promptly to protect victims and critical infrastructure (Burrell, 2022; Burrell et al., 2021).

The importance of supply chains has never been more in the spotlight than it is now. Once the domain of experts and academics, supply chain management has been at the forefront of media coverage throughout the COVID-19 epidemic. This sudden fame has arisen because of the frustratingly low availability of many goods and services. These shortages have forced everyone to face the fact that the items we usually take for granted are transported via intricate global supply systems vulnerable to disruption (National Academies of Sciences, 2022).

Healthcare organizations face the same cybersecurity issues as any modern organization in the digital age. However, there are some unique or more frequent issues specific to healthcare cybersecurity. Healthcare organizations are a prime target for attack because they store financial and patient information. Patient information sells for more than the average on the dark web (Stack, 2017).

The Ponemon Institute issues periodic reports on cybersecurity and healthcare. According to their most recent report, 56% of the respondents reported that their healthcare organization had a cyberattack (Cynerio and Ponemon Institute, 2022). Cyberattacks impact patient care, and this includes an increase in patient mortality. According to this report, the Internet of Things (IoT) and devices are involved in 88% of data breaches. Someone must be responsible for IoT devices. In most healthcare organizations, many people have cybersecurity responsibilities, but due to the lack of overall accountability, there may be gaps or delays in implementing security measures (Cynerio and Ponemon Institute, 2022). The risk of IoT is acknowledged to be high by the survey respondents but security is not up to par given this high risk (Cynerio and Ponemon Institute, 2022).

The types of attacks in healthcare vary widely. Ransomware is a way for cybercriminals to monetize their efforts since healthcare organizations have a time-critical mission and frequently have deep pockets (Ponemon Institute, 2021). Ransomware attacks against healthcare organizations have been increasing significantly in frequency since the beginning of the Covid-19 pandemic in 2020 (Alawida et al., 2022). Phishing is a well-established attack method that takes advantage of the human element of cyber vulnerability (Al-Qahtani & Cresci, 2022). Covid 19 changed the way many people worked. Many people had to pivot to working remotely. Many organizations did not anticipate the need to secure this extended environment. People were looking for information about the pandemic. There was a sharp increase in demand for personal protective equipment. In March 2020, phishing attacks increased by 600% compared to the prior month (Al-Qahtani & Cresci, 2022).

Cynerio/Ponemon surveyed individuals involved in U.S. healthcare cybersecurity. According to the report, 17% of $145 million goes to I.T. security for a typical institution (Cynerio and Ponemon Institute, 2022). According to the HIMSS survey, 40% of respondents stated that 6% or less of the I.T. budget was allocated to cybersecurity (*HIMSS Healthcare Cybersecurity Survey*, 2021). The situation is very different, according to Gioulekas et al., who reported on cybersecurity in low to middle-income E.U. countries (Gioulekas et al., 2022). The typical security budget is <5% of the total I.T. budget. Some hospitals even lacked a dedicated cybersecurity team.