Chapter 4
Significance of Cyber Security in Healthcare Systems

Anuj Singh
https://orcid.org/0000-0001-8880-780X
Graphic Era University (Deemed), India

Somjit Mandal
National Chiao Tung University, Hsinchu, Taiwan

Kamlesh Chandra Purohit
Graphic Era University (Deemed), India

ABSTRACT

The healthcare sector is one of the industries most vulnerable to cyberattacks. healthcare cybercrime is significantly expanding as it relates to healthcare services that are digitally enabled, and it aims to exploit security flaws and vulnerabilities. Technology improvements have exposed the healthcare sector to a wide range of extremely dangerous threats, such as ransomware. Ransomware, a sort of hack that targets both organisations and individual people, has become more prevalent recently as a result of its effective results. There has been a significant improvement in its disputes over the previous several years. The study includes answers as well as a complete overview of ransomware attacks. The main goal of this study is to classify the cyberattack defences employed by healthcare programmes to stop ransomware, such as blockchain and machine learning. Studies investigating information security, medical organisations, and security firms will all benefit scientifically from the study.

INTRODUCTION

Healthcare is an extremely specialised profession that handles a lot of sensitive personal data. In our internet-driven age where everything is handled over the internet,

DOI: 10.4018/978-1-6684-6646-9.ch004

this information is even more crucial (Thamer & Alubady, 2021). Healthcare firms confront issues dealing with very sensitive information. They continually fight rising cyber hazards and adjust to the digital transition while adhering to tighter laws. The healthcare industry is currently quite dynamic. hospitals are joining networks, forming alliances, and undergoing an extraordinary degree of merger acquisition consolidation. This is an exciting time in healthcare because healthcare is changing new technologies are being developed daily that allow patients to track their own health patients are demanding more individualised care, and health information exchanges are being implemented. It's really not a question of if a breach occurs but rather where now that we all know that health care institutions are very vulnerable. Now that healthcare is complicated, personal health records are being prescribed online health communities, and it's getting worse, sensitive and personal information is being shared with a variety of technologies, and every time it's shared, there's a cyber risk involved, so healthcare organisations need to have measures in place to stop hackers from gaining access to that sensitive information (Maurya et al., 2018). Hospitals are targets of cyberattacks, which are on the rise. The abundance of sensitive data makes it a gold mine for cybercriminals. First off, the health care sector is ripe for hacking since patient records can be purchased on the dark web for up to $1,000 Medical records contain a range of A patient's medical data being stolen or compromised might have long-lasting effects. birth dates, credit card information, social security numbers, residences, and email addresses. Malicious software, sometimes known as malware, is merely software designed with the goal to harm systems, steal data, or generally cause chaos. Malware has infected more than 88% of the healthcare industries as a whole. 88%, now that's a lot. 96% of ransomware attacks on healthcare organisations target medical treatment centres because they are easy targets (Thamer et al., 2021). Healthcare had the fifth-highest number of ransomware assaults out of the 18 industries surveyed, and it completely destroys the healthcare institution.

The healthcare institution where it occurs presently according to article more than half of the healthcare industry and has a network security grade of less than a C-GRADE (Venter et al., 2019). This indicates that when they were evaluated, the security scores they received reflected whether or not the company could protect its data from data breaches, and obviously healthcare has not made that a priority. The healthcare industry ranks 15th and is vulnerable to social engineering techniques. Healthcare workers tend to be very trusting, but social engineering is really the ability to persuade someone to give you their personal or private information by using dishonest tactics (Zakus et al., 2014). Simple tasks like timely updating security patches were a problem in 63% of the healthcare entities surveyed. This is just one of the basic things that health care institutions need to do when anyone needs to do to ensure that they're guarding against whatever the latent threat is. fashion possible