Cybersecurity in Hospitals

Natalie Waugh | LIS 4934 BSIS Senior Capstone | Dr. Vanessa Reyes

UNIVERSITY of SOUTH FLORIDA

Abstract

Cybersecurity is a major concern in hospitals and has become a focal topic within the community due to malicious attacks. Cybersecurity is an ongoing process and requires innovation to respond to escalating attacks. In order to gain knowledge and insight into the topic, academic literature and scientific research was reviewed. Using the information gained, recommendations were provided with the purpose of improving cybersecurity measures in hospitals.

Thesis

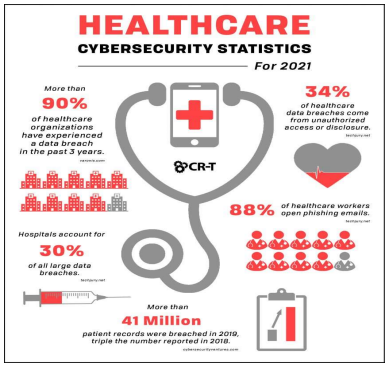
A cybersecurity system is vital to protecting patient information in a hospital system, and requires effective security policies, ongoing education, and diligence to defend against evolving cyber-attacks.

Introduction

Cybersecurity in hospitals is incredibly important to the field of information studies due to the mission of protecting patient information. Hospitals face many threats from malicious hackers due to the sensitivity of its information. An effective cybersecurity system is necessary to maintain patient safety and compliance with HIPPA laws. It is also necessary to allow healthcare workers to provide safe delivery of healthcare services.

Objective

The objective of this research project is to identify security vulnerabilities and challenges, common cybersecurity practices, pertinent policies, and provide recommendations to improve cybersecurity systems within hospitals.

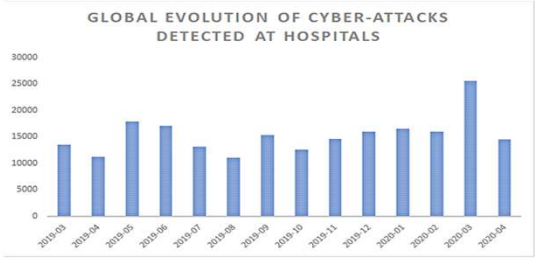


Methods

Academic literature was studied and analyzed with resources being gathered to provide information for the research paper. Qualitative research included studying interview responses from security professionals who worked in hospitals. Quantitative research included studying statistics on cyberattacks and evaluation models on the cybersecurity capabilities of different hospitals. These research methods were necessary to gain insight and analysis.

Outcomes

Threats and vulnerabilities that were identified included common cyberattacks such as email phishing, ransomware, and attacks against connected medical devices.



The Covid-19 pandemic also resulted in increased attacks in the form of digital scams related to PPE and medical supply fraud. The shift from paper documentation to electronic health records and systems prompts a need for hospital staff to receive cybersecurity awareness training and improve on digital literacy. Cybersecurity practices included both technical and practical approaches. Practical approaches included training and educating hospital staff and implementing a strong cybersecurity team. Technical approaches consisted of intrusion detection systems, firewalls, multi-authentication measures, and privileged access restrictions. There is a need for strong policies that focus on data privacy and information security. It also should provide guidelines on how to report incidents to the chain of command.

Conclusion

There is a constant need for innovation to respond to evolving and escalating cyberattacks against hospitals. Recommendations include ongoing cybersecurity awareness training for hospital employees to identify suspicious activity and social engineering attacks. Keeping login information private, practicing a clean desk policy, and logging out of devices when not used is also beneficial. Security measures such as risk identification, intrusion detection systems, network audits, firewalls, anti-virus scans, and privilege access restrictions could be helpful. Compliance with software updates and collaboration with manufacturers would improve the security of devices. Cybersecurity policies should set guidelines, roles and responsibilities, and behavioral expectations on how to maintain a secure environment. Establishing an open dialogue where cybersecurity teams from different hospitals share cybersecurity incidents and solutions would benefit the industry. A hospital cybersecurity registry could be an effective approach to share ideas.