INFORMATICS INSTITUTE OF TECHNOLOGY

INFORMATIC INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

Resilient Cyber Security Model to Support Patient Privacy & Safety Connected Medical Devices within Critical Healthcare Infrastructure.

A Dissertation by

Mr. Chathura Wickramasinghe -20210739/w1867324

Supervised by

Mr. Sithira Hewaaracchi

Submitted in partial fulfillment of the requirements for the MSc in Cyber Security & Forensics degree at the University of Westminster.

August 2023

Abstract

The ongoing patient privacy issue in hospitals continues to raise significant concerns within the healthcare community and among patients. Despite efforts to enhance data protection measures, instances of unauthorized access to sensitive medical information persist. One of the primary challenges is the ever-evolving landscape of technology, which presents new opportunities for potential breaches. Cyberattacks, phishing attempts, and ransomware threats are on the rise, putting patient data at risk and threaten their privacy. The internal management of patient information remains a major issue. Hospitals handle vast amounts of data daily, making it challenging to maintain comprehensive control over access rights. Staff members may have access to more data than they need, creating potential vulnerabilities within the system. Furthermore, human error, such as unintentional disclosure of sensitive information or improper disposal of physical records, remains a persistent threat.

undertaken interviews with healthcare facilities chief information officers, chief information security officers, and medical care cybersecurity specialists; analysed the gathered data; and created a system dynamics model that explains how health care facilities develop their cybersecurity capabilities. the risk of malicious activity across both individual health care facilities and a network of hospitals is then examined using simulation analysis to investigate how changes to model variables affect those probabilities.

Explore a few important measures hospitals use to decrease the probability of cybercrime. End point complexity is the factor that affects cyberattack risk in a hospital the most, followed by internal stakeholder alignment. Low levels of resources could be made up for by setting a high target level of cybersecurity, given the fact that resource availability is essential for advancing efforts to close cybersecurity capacity gaps.

Keywords : Patient Privacy, Cyber Attacks, Data Privacy

Subject Descriptor: Healthcare privacy, HIPAA Compliance, Protected Health Information (PHI)