CYBERSECURITY IN HEALTHCARE: A MATTER OF LIFE AND DEATH

DAYANG NUR NAZIHAH M ROSLAN
SECTION 38

UNIVERSITI TEKNOLOGI MALAYSIA

ABSTRACT

The purpose of this study is to investigate the role of cybersecurity in healthcare. The healthcare industry is increasingly reliant on digital technologies, from Electronic Health Records (EHRs) to telemedicine, which have revolutionized patient care exceptionally. Although this digital transformation provides many benefits to the healthcare industry, this sector has also been exposed to cybersecurity threats as it is such a significant sector. Cyber threats targeting healthcare systems range from ransomware and phishing attacks to insider threats and Distributed Denial of Service (DDoS) attacks. Vulnerabilities in these system, such as outdated infrastructure, lack of knowledge in phishing threats result in chaos. The study begins by outlining the various types of cyber threats facing the healthcare sector, including ransomware, phishing attacks, and more. The paper provides an in-depth analysis of high-profile cyberattacks that intend to illustrate the profound impact of cyber incidents on healthcare operations, highlighting disruptions to patient care, financial losses, and long-term repercussions on organizational trust. This case study intends to explore the critical importance of cybersecurity in healthcare, highlighting how vulnerabilities can lead to the most devastating consequences, including loss of precious life. Based on the analysis of recent cyberattacks, this study will examine the impact of these breaches and what it affects. The study further outlines the best practices for healthcare providers to enhance their cybersecurity effectiveness. The importance of regular cybersecurity training for healthcare staff is emphasized, along with the need for effective incident response and disaster recovery planning.

ABSTRAK

Tujuan kajian ini adalah untuk menyiasat peranan keselamatan siber dalam sektor Kesihatan. Industri Kesihatan semakin bergantung pada teknologi digital, dari Rekod Kesihatan Elektronik (EHR) hingga teleperubatan, yang telah merevolusikan penjagaan pesakit dengan sangat baik. Walaupun transformasi digital ini memberikan banyak manfaat kepada industri kesihatan, sektor ini juga terdedah kepada ancaman keselamatan siber kerana kepentingannya yang besar. Ancaman siber yang menyasarkan sistem Kesihatan merangkumi serangan ransomware, serangan phishing, ancaman dalaman, dan serangan Distributed Denial of Service (DDoS). Kelemahan dalam sistem ini, seperti infrastruktur yang usang dan kekurangan pengetahuan tentang ancaman phishing, mengakibatkan kekacauan. Kajian ini dimulakan dengan merangkumi pelbagai jenis ancaman siber yang dihadapi oleh sektor kesihatan, termasuk ransomware, serangan phishing, dan lain-lain. Ia memberikan analisis mendalam tentang serangan siber yang terkenal yang bertujuan untuk menggambarkan kesan mendalam insiden siber terhadap operasi kesihatan, menyoroti gangguan kepada penjagaan pesakit, kerugian kewangan, dan kesan jangka panjang terhadap kepercayaan organisasi. Kajian kes ini bertujuan untuk meneroka kepentingan kritikal keselamatan siber dalam sektor kesihatan, menyoroti bagaimana kelemahan boleh membawa kepada akibat yang paling teruk, termasuk kehilangan nyawa yang berharga. Berdasarkan analisis serangan siber terkini, kajian ini akan memeriksa kesan pelanggaran tersebut dan apa yang terjejas. Kajian ini seterusnya menggariskan amalan terbaik untuk penyedia penjagaan kesihatan bagi meningkatkan keberkesanan keselamatan siber mereka. Kepentingan latihan keselamatan siber yang berterusan untuk kakitangan kesihatan ditegaskan, bersama dengan keperluan perancangan tindak balas insiden dan pemulihan bencana yang berkesan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

HSE	-	Health Service Executive
IoMT	-	Internet of Medical Things
DDoS	-	Distributed Denial of Service
EHR	-	Electronic Health Record
EMEA	-	Europe, Middle East, and Africa
APJ	-	Asia-Pacific and Japan
SMS	-	Short Message Service
SMiShing	-	SMS Phishing
IT	-	Information Technology

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

As the healthcare industry increasingly integrates with the use of technology, it has become a prime target for cybercriminals. The privacy of healthcare data, combined with the critical need of uninterrupted access to medical services, makes the protection of this sector not only a matter of protecting sensitive information, but a matter of protecting lives.

Cyber threats such as ransomware, phishing, and Distributed Denial of Service (DDoS) attacks have becoming increasingly common. These data breaches can lead to disruption of patient care, financial losses and long-term damage to organizational trust. This investigation intends to elaborate on the critical importance of cybersecurity in healthcare, the impact of recent cyberattacks, and the steps that healthcare providers can take to preserve important data.

1.2 Problem Background

The rapid integration of digital technologies into healthcare systems created challenges in the cybersecurity sector. The exposure to cyber threats has been growing especially with interconnected networks between systems. The high value of sensitive patient data and the urgency of healthcare operations make the healthcare sector particularly a favored target for cybercriminals. The balance between maintaining patient confidentiality and accessible medical data increases the chances of becoming a target.

Moreover, the existing systems are more prone to vulnerabilities as the lack of adequate cybersecurity training among healthcare professionals fuels the issue, as human error is one of the most significant contributors to security breaches. Additionally, the rise of the Internet of Medical Things (IoMT) and the increasing complexity of healthcare networks have expanded the attack surface which has created more entry points for cybercriminals to exploit.

1.3 Project Aim

The aim of this project is to assess the impact of cybersecurity threats on healthcare systems and explore strategies to protect patient data and ensure safe healthcare operations.

1.4 Project Objectives

The objectives of the project are:

(a) To estimate the parameters affecting cybersecurity in healthcare.

(b) To identify key cybersecurity threats and vulnerabilities in healthcare systems.

(c) To analyse the impact of recent cyberattacks on healthcare operations and patient safety.

(d) To define the best practices and strategies for enhancing cybersecurity in healthcare.

1.5 Project Scope

The scopes of the project are:

(e) To explore the current cybersecurity landscape within the healthcare industry, focusing on common threats and vulnerabilities.

(f) To evaluate the effectiveness of existing cybersecurity measures and recommend strategies for improvement tailored to healthcare environments.

CHAPTER 2

Cybersecurity Threats in Healthcare

2.1 Types of cybersecurity threats

2.1.1 Malware

Malicious software – is any program or code that is created with the intent to infect, damage, or gain access to computer systems. It's designed to infiltrate your device without any signals, causing damage and disruption to the computer's system or steal confidential information. There are many types of malware, but each and every one is designed to compromise the security of systems.

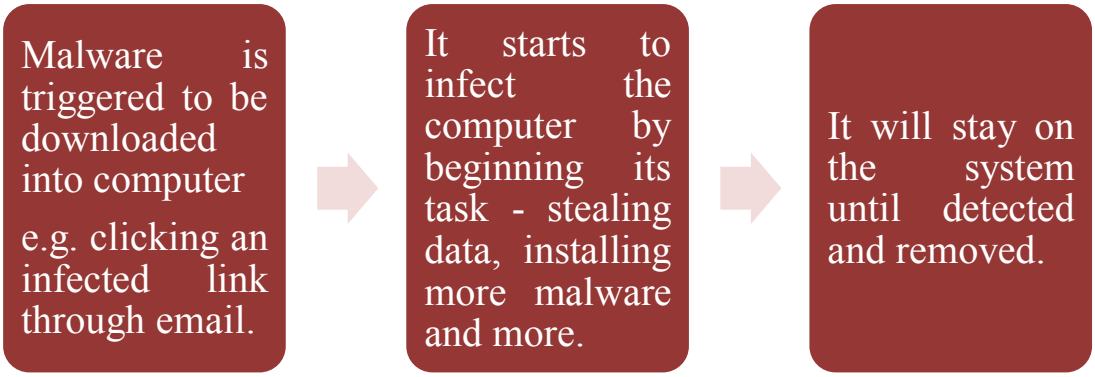


Figure 2.1.1 How Malware Works

While not all malware are essentially viruses, each and every malware installed on your computer poses a threat of data breach and harms the computer system. A common example of malware is ransomware. Ransomware is when the installed malware denies access to the system by locking and encrypting files following threats to release private information or erasing of important files unless paid a ransom. The most recent case for ransomware in the healthcare industry is a ransomware attack that disrupted multiple London hospitals. A company called Synnovis that provide pathology services to hospitals detected an incident which disrupts the blood transfusion IT system. This resulted in cancelled appointments or patients having to redirected to other service providers. This attack was done by Qilin, a Russian cybercrime group, whom shared 400GB of private data on the dark web a following their aim to extort $50 million from Synnovis. The hackers executed this breach by injecting malware that locked the entire computer system with the condition that the system will be released if the ransom was paid.

2.1.2 Distributed Denial of Service (DDoS) Attacks

A malicious, targeted attack that bombards a network with false request to disrupt their business operations. Users become incapacitated to perform tasks on their computer. Attackers use malware to create a network of internet-connected devices that are infected which are used to send traffic. This botnet may include Internet of Things (IoT), phones, computers, routers and servers. This creates waves of attacks spreading further and further. Like zombies attacking humans to turn them into zombies. Once a botnet has been built, instructions are sent, directing them to flood servers with false requests. Normal traffic is denied of service due to the overwhelming amount of traffic.

Research shows that the Europe, Middle East and Africa (EMEA) region went through 86% of 7 application layer DDoS attacks. 7% each was accounted for North America and Asia-Pacific and Japan (APJ).

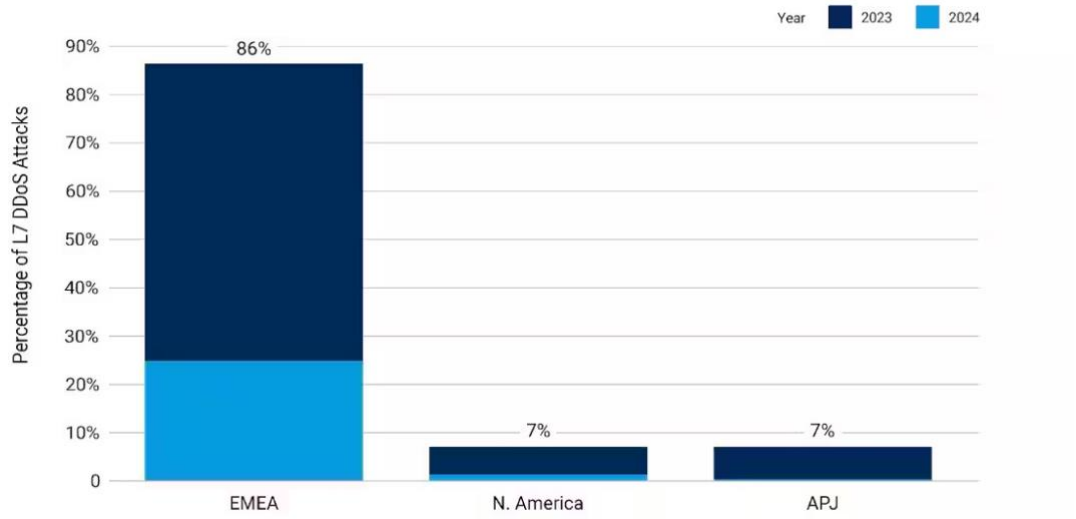


Figure 2.1.2 The statistics of 7 layer DDoS attacks in EMEA, North America and APJ between January 1, 2023 – March 31, 2024

As an example, Singapore's public healthcare institutions were disrupted through internet connectivity with DDoS attacks. The company, Synapxe detected an abnormal surge in network traffic during morning operations. The agency's firewall became overwhelmed in moments. This triggered the firewall to uphold traffic, which resulted in inaccessible any internet-reliant services. Though after the incident happened, measures were put up to protect the system which enabled it to withstand the attack and prevented data from being compromised.

2.1.3 Phishing

Phishing is a common cyberattack that utilizes emails, SMS, phone calls and other platforms to lure a victim into sharing their private information. There are a variety of phishing attacks, including:

Type	Description
Spear Phishing	Target's individuals through malicious emails.
Whaling	Targets senior executive employees to steal money or information.
SMiShing	Targets individuals through fraudulent text messages.

Table 2.1.3 Types of Phishing attacks

Not only does it trick people into sharing sensitive information, when a person clicks on illegitimate links in emails, malware can also be downloaded into their computer infecting the entire system. A recent case in the healthcare industry is

Ascension health system data breach. An individual at the facilities unintentionally downloaded a malicious file that was thought to be legitimate. They experienced a weeklong disruption where they were locked out of the system that coordinates almost all aspects of patient care. The result of this was lost lab results, medication errors and absence of routine safety checks. Black Basta, a group of cybercriminals were identified as the hackers. Files that contained protected health information were stolen.

2.2 Vulnerabilities in the Healthcare System

As the healthcare industry integrates with modern technology, more opening to cybercrimes is emerging. Without addressing these vulnerabilities, a system can easily be targeted to be exploited.

2.2.1 Legacy Systems

Legacy Systems refer to older technology that are still used because upgrades are costly. These outdated systems lack the security that can protect them from modern cybersecurity threats which make them vulnerable to attacks like ransomware and unauthorized access. As technology advances, vendors tend to withdraw support from these older software, meaning that the software are no longer being updated. With systems such as healthcare that rely heavily on their networks for day to day operations, it becomes difficult to upgrade these systems as it can be time-consuming.

A notable example is the transition of hospitals and health systems to new EHR platforms. Organizations such as Intermountain Health and Indian Health Services, faced significant difficulties in maintaining data integrity during the transition.

2.2.2 Internet of Medical Things (IoMT)

IoMT represents the evolution of technology in the healthcare industry as it encompasses a variety of interconnected medical devices used. It allows wireless and remote devices to communicate using the internet to conduct an analysis of medical data for better patient outcome.

i. In-Hospital IoMT

IoMT sensors are used to track interactions between personnel and patients so administrators can understand of what goes about the premises.

ii. In-home IoMT

Users can transmit medical data from home to care provider facilities not only to be alerted during a medical situation, but also track patient condition to monitor and predict outcomes.

iii. On-body IoMT

This IoMT is designed to be wearable to remotely track and monitor system. It can be worn and taken everywhere unlike in-home IoMT.

iv. Community IoMT

Used throughout a larger part of the geographic area. Tracks patient metrics outside of the hospital.

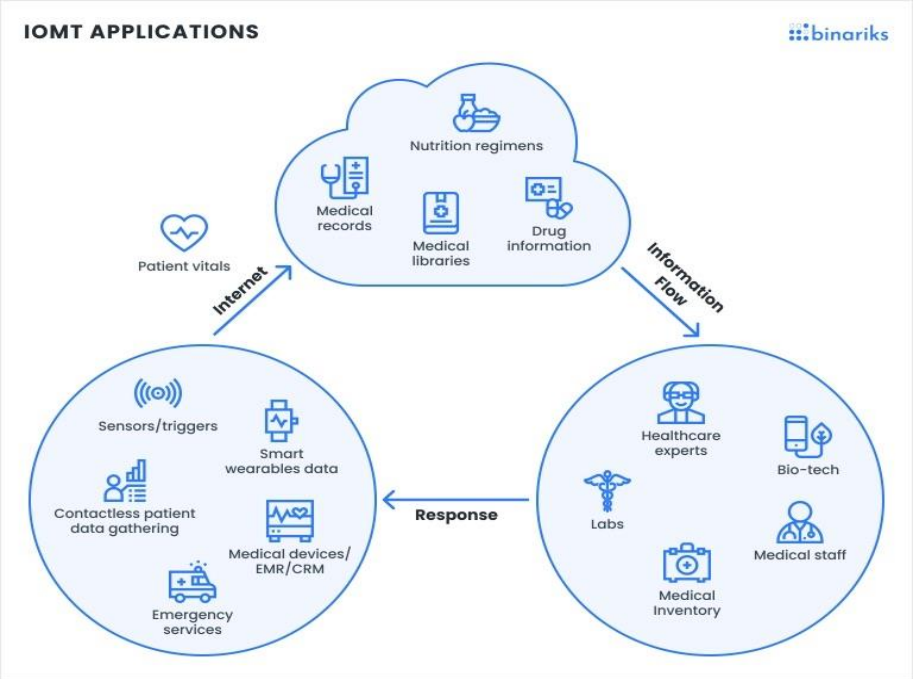


Figure 2.2.1 IoMT Applications

Having to ensure communication is seamless and all devices are compatible with each other can create issues during the process, which can leave security gaps that are not noticeable until an incident happens.

2.3 Impact on Cybersecurity Breaches

2.3.1 Patient Safety and Care Disruption

When ransomware occurs to a hospital's patient care system, EHRs tend to be held hostage. This affects the ability to access to patient data where hackers can purposely or unintentionally alter patient's data which can result in drastic medical errors. Not only that, but proper medication could also be locked away and inaccessible during a crisis.

2.3.2 Financial Cost

One of the financial impacts during a cyberthreat is the cost to recover from the situation. There are the legal fees, operational costs, investment for improvement in the IT sector which take a toll on a healthcare system's finance situation. Not to mention the possibility of hackers stealing money when already hacked into the system and ransom asked to recover the system.

2.4 Chapter Summary

a) There are many types of security threats: malware disrupts systems and steals data (e.g., 2021 Synnovis ransomware), DDoS overloads networks causing service disruptions (e.g., Singapore 2023), and phishing tricks users into sharing sensitive info (e.g., Ascension Health breach).
b) Legacy systems are outdated tech lacking security updates, while IoMT introduces connected devices that may create security gaps.

c) Ransomware locking EHRs can lead to errors in patient care, and breaches incur recovery costs and potential ransom payments, impacting financial stability.

CHAPTER 3

CASE STUDIES

3.1 Introduction

Cybersecurity breaches in healthcare have become increasingly common as the industry depends more on digital systems to manage sensitive data. These breaches, including ransomware attacks and data leaks, can disrupt healthcare services and compromise patient privacy. This chapter examines key incidents, highlighting vulnerabilities in healthcare IT systems and the risks associated with third-party vendors.

3.2 Ransomware attack on HSE Ireland 2021


THE IRISH TIMES

Health

HSE cyber attack: More than 470 legal proceedings issued against health service after ransomware hit

Leak by Conti, the Russia-based crime group, compromised personal data of almost 100,000 staff and patients

Expand

More than 470 legal proceedings have been issued against the Health Service Executive (HSE) in relation to a cyber attack

Shauna Bowers

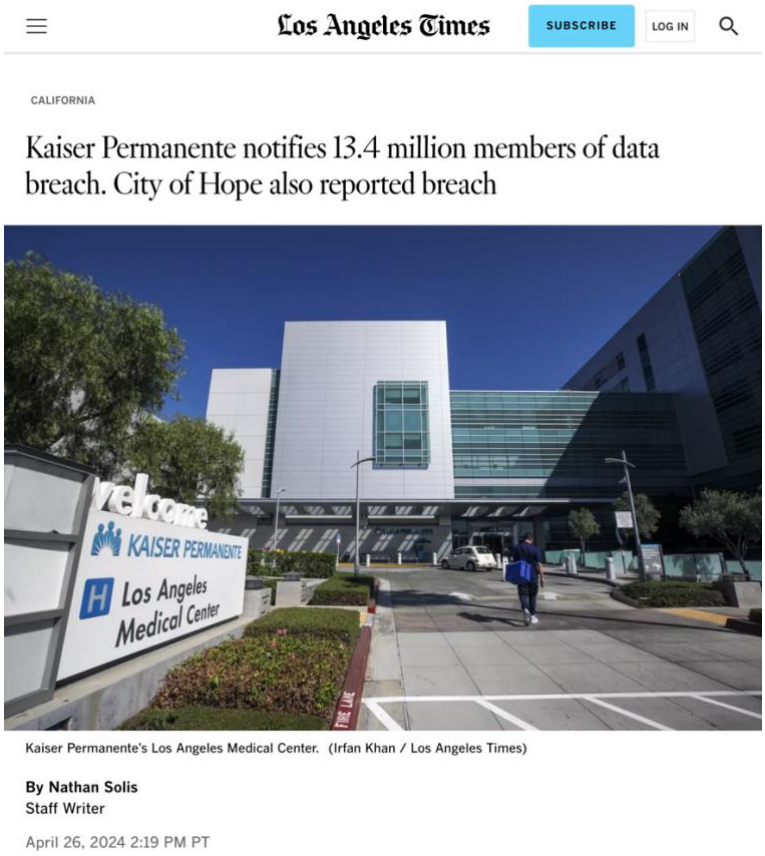
Figure 3.2.1 HSE Ireland cyber-attack 2021

In May 2021, the Health Service Executive (HSE) of Ireland faced a sophisticated ransomware attack that severely impacted its IT systems. The attack, orchestrated by the Conti ransomware group, exploited existing vulnerabilities in the HSE's digital infrastructure. Conti, known for its ability to rapidly spread across networks, encrypted the organization's data and demanded a ransom of 20 million in Bitcoin in exchange for the decryption keys. The attack caused widespread disruption, affecting patient care, diagnostic services, and general healthcare operations across Ireland.

Despite the pressure, the HSE made the decision not to pay the ransom. Instead, the organization initiated a large-scale recovery operation, relying heavily on backups to restore its systems. The Irish government supported the HSE's stance, emphasizing the importance of not giving in to criminal demands, a move that was in line with international guidance on ransomware response. Additionally, the HSE sought assistance from international cybersecurity experts to aid in mitigating the impact of attack and fortifying its IT infrastructure against future threats.

The consequences of the attack were profound, highlighting the vulnerabilities in the healthcare sector's digital systems. It also underscored the growing threat of ransomware, which targets critical services and organizations with high stakes, knowing the potential consequences of prolonged downtime. The HSE's recovery process was long and complicated, requiring significant resources and collaboration with both domestic and international entities to bring services back to full functionality. This incident prompted a re-evaluation of cybersecurity measures within the healthcare sector in Ireland and beyond, leading to a stronger focus on securing critical infrastructure from future cyber threats.

3.3 Data Breach at Kaiser Foundation Health Plan 2024


Los Angeles Times SUBSCRIBE LOG IN

CALIFORNIA

Kaiser Permanente notifies 13.4 million members of data breach. City of Hope also reported breach

Kaiser Permanente's Los Angeles Medical Center. (Irfan Khan / Los Angeles Times)

By Nathan Solis
Staff Writer

April 26, 2024 2:19 PM PT

Figure 3.3.1 Kaiser Foundation Health Plan 2024 data breach

In April 2024, Kaiser Foundation Health Plan experienced a significant data breach that impacted approximately 13.4 million individuals. The breach was not due to hacking but resulted from the unauthorized disclosure of sensitive information through tracking technologies embedded in its websites and apps. These tools collected visitor data, including potentially private health information, and shared it with third parties like Google and Meta without proper business associate agreements in place. This incident highlights the risks posed by inadequate oversight of third-party technologies in healthcare application.

The breach primarily affected individuals who interacted with Kaiser's online services. Once the issue was discovered, the organization took steps to assess the extent of the data leak and began notifying affected individuals. Given the scale o the

breach, this incident was one of the largest in healthcare for 2024 and raised concerns about the increasing reliance on digital tools in healthcare without fully understanding their privacy implications.

Following the breach, Kaiser Foundation Health Plan faced significant criticism and scrutiny from regulators and privacy advocated. It underscored the need for stronger safeguards and compliance protocols when using third-party tracking technologies, particularly in industries like healthcare, where data confidentiality is top priority. This case serves as a cautionary tale for other healthcare providers to ensure that patient privacy is protected in both traditional and digital healthcare environments.

3.4 Data Breach at MedStar Health 2024

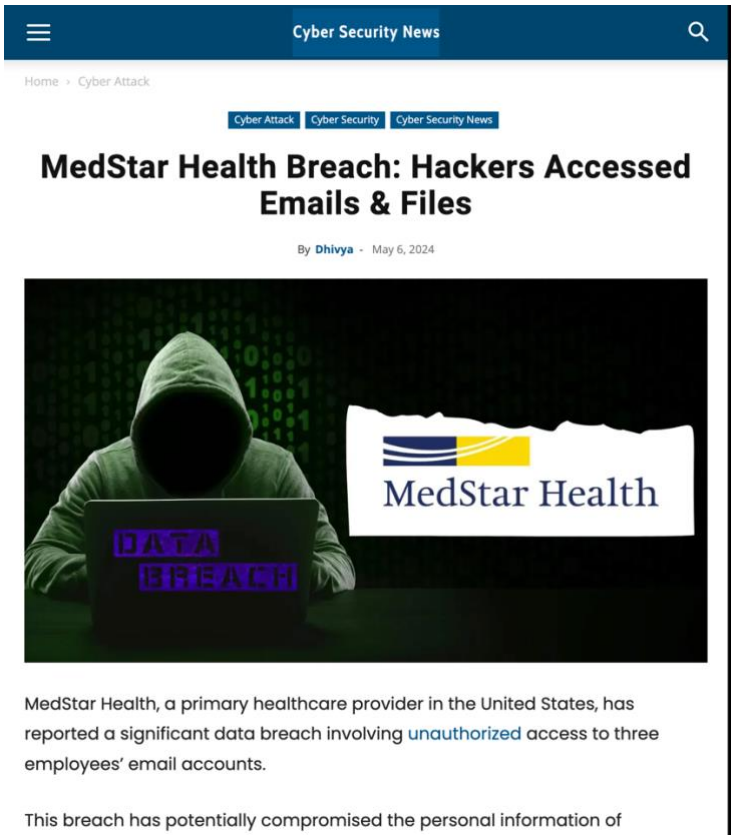


Figure 3.4.1 Data Breach at MedStar Health 2024

In April 2024, MedStar Health, a prominent healthcare provider in the U.S., experienced a significant data breach due to a security compromise at a third-party vendor responsible for billing and insurance processing. Attackers exploited vulnerabilities in the vendor's system, allowing them to gain unauthorized access to MedStar Health's sensitive patient records. This breach highlighted the risks associated with relying on external partners for critical healthcare operations.

The breach resulted in the exposure of personal, medical, and financial information for more than 500,000 patients. Compromised data included names, Social Security numbers, medical histories, and insurance details, raising concerns about potential identity theft and fraud. The incident demonstrated how vulnerabilities in third-party systems can have a direct and severe impact on organizations that depend on these services, even when their own internal systems are secure.

MedStar Health responded by immediately working with the third-party vendor to secure the affected systems and prevent further access. They also engaged cybersecurity experts to investigate the breach, assess the damage, and ensure compliance with federal healthcare privacy regulations. The organization began notifying affected patients and offering identity theft protection services to mitigate the risk of personal and financial harm. This breach underscored the importance of stringent cybersecurity measures not only within healthcare organizations themselves but also among the vendors and partners they rely on to process sensitive information.

3.5 Chapter Summary

a) In May 2021, the ransomware attack on HSE Ireland by Conti ransomware group severely impacted the organization's IT systems, disrupting healthcare services. The HSE refused to pay the ransom and instead relied on backups for recovery, with international assistance. The attack

highlighted vulnerabilities in healthcare infrastructure and emphasized the growing threat for ransomware.

b) In April 2024, Kaiser Foundation Health Plan experienced a data breach that exposed the sensitive information of 13.4 million individuals. The breach occurred due to the use of third-party tracking technologies that shared user data with companies like Google and Meta. The incident highlighted those risks of relying on third-party tools in healthcare and emphasized the need for better oversight of digital privacy practices.

c) In April 2024, MedStar Health experienced a data breach caused by vulnerabilities in a third-party services and the need for stringent security measures for both healthcare organization and their partners.

CHAPTER 4

CYBERSECURITY STRATEGIES AND BEST PRACTICE FOR HEALTHCARE

4.1 Introduction

In healthcare, protecting patient information is more than just a technical challenge – it's about safeguarding lives and maintaining trust. Every day, healthcare providers rely on digital systems to deliver care, while patients trust that their personal and medical details are kept safe. However, as these systems grow more complex, so do the risks of cyberattacks. From protecting private health records to ensuring hospitals can function without disruption, cybersecurity in healthcare has never been more important. This section highlights practical strategies and best practices to help keep patient data secure and healthcare systems resilient.

4.2 Data Encryption and Secure Connection

One of the ways to ensure sensitive data will not be exposed is by using software that can assist with data encryption. For instance, utilizing apps with end-to-end encryption for internal communications such as Telegram, Whatsapp, iMessage and others. Not only messaging apps, but encrypted email services are also a crucial factor in preventing cyberattacks such as phishing from occurring to a healthcare system. Another way for encryption is using Virtual Private Network (VPN) which can encrypt internet traffic and hides IP addresses. This can ensure data is secured during transmission.

4.3 Regular Security Training

Frontliners in healthcare also need cyber awareness, without it many can be tricked that can result in cyberattacks. This can prepare the employees to recognize and report potential security incidents promptly to reduce the risk of human errors that can lead to data breaches. By educating employees about the latest cybersecurity and best practices, employees can be more aware of and adhere to data protection regulations.

4.4 Implementing Incident Response and Disaster Recovery Planning

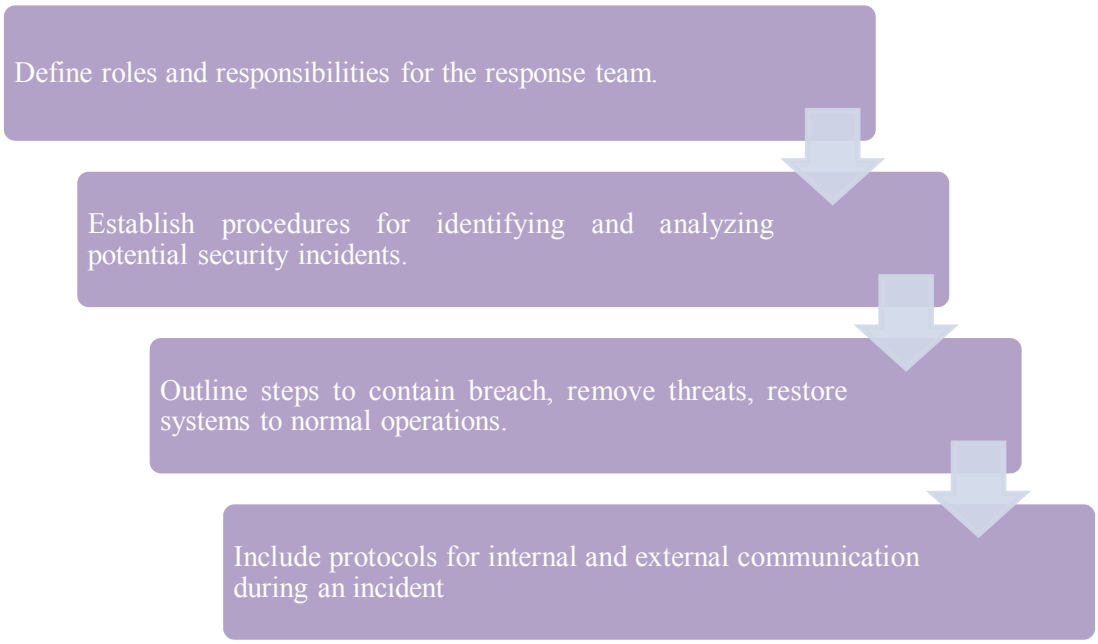


Figure 4.4.1 Incident Response and Disaster Recovery Planning

The figure above shows the steps for incident response and disaster recovery planning. Without a proper policy, the affected personnel could easily enter a panicked state during a crisis. This can lead to even more consequences that impact on the system that would be difficult for the recovery process.

4.5 Chapter Summary

a) Data encryption and secure connection can be achieved through encryption techniques. Healthcare providers should use encrypted communication apps (e.g., Telegram, Whatsapp) and email services to prevent breachers, along with VPNs to secure internet traffic during transmission.
b) Regular security training for healthcare employees is crucial to minimize human errors that could lead to data breaches. Training improves awareness and enhances the ability to identify and report security threats.
c) Incident response and disaster recovery planning are essential for healthcare systems to recover quickly and effectively from cyberattacks. Proper planning helps mitigate panic and reduces the impact of a crisis, facilitating smoother recovery

CHAPTER 5
CONCLUSION

5.1 Research Outcomes

Cybersecurity threats in healthcare, particularly breaches, pose significant risks to patient data, healthcare operations and public safety. With the increasing reliance on electronic health records (EHRs) and interconnected medical devices, healthcare organizations are more vulnerable to cyberattacks. Each year, healthcare institutions globally experience data breaches affecting millions of patients, highlighting the urgent need for enhanced security measures.

With the growing awareness of these challenges within the healthcare sector, governments, stakeholders, and experts are collaborating to develop better security frameworks, invest in more advanced infrastructure and implement comprehensive response plans to protect healthcare data and maintain patient safety.

5.2 Contributions to Knowledge

The findings of this study contribute to the ongoing efforts of healthcare providers, IT specialists and policymakers to strengthen cybersecurity in healthcare systems. This research can provide valuable insights for healthcare organizations, government agencies and cybersecurity professionals.

REFERENCES

CrowdStrike. (2024, May 31). *12 most common types of cyberattacks today - CrowdStrike*. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

Critical incident declared as ransomware attack disrupts multiple London hospitals. (n.d.). https://therecord.media/london-hospitals-ransomware-attack-critical-incident-declared

Dean-Foster, E., & Dean-Foster, E. (2024, July 19). *Ransomware Assault on NHS: A Deep Dive into the Synnovis Data Breach*. Intercede. https://www.intercede.com/ransomware-assault-on-nhs-a-deep-dive-into-the-synnovis-data-breach/

Ascension: Cyberattacker stole files likely containing protected health, identity data. (2024, June 12). Fierce Healthcare. https://www.fiercehealthcare.com/providers/systems-clinical-operations-interrupted-ascension-amid-apparent-cybersecurity-event

LaPointe, J. (2024, March 18). 63% of known exploited vulnerabilities found on healthcare networks. *Healthtech Security*. https://www.techtarget.com/healthtechsecurity/news/366593999/63-of-known-exploited-vulnerabilities-found-on-healthcare-networks

2024: The year of health IT transformation and evolution in patient care - Health Data Management. (2024, January 12). Health Data Management. https://www.healthdatamanagement.com/articles/2024-the-year-of-health-it-transformation-and-evolution-in-patient-care

Ordr. (2024, July 5). *IoMT and its Transformative Impact on Healthcare Security - Ordr*. https://ordr.net/article/what-is-iomt

16 apps that use end to end encryption. (n.d.). https://www.sliksafe.com/blog/16-apps-that-use-end-to-end-encryption

Ordr. (2024, July 5). *Healthcare Cybersecurity strategy to secure medical Assets - OrdR*. https://ordr.net/article/what-is-healthcare-cybersecurity

Bowers, S. (2024, May 14). HSE cyber attack: More than 470 legal proceedings issued against health service after ransomware hit. *The Irish Times*.

https://www.irishtimes.com/health/2024/05/14/hse-cyber-attack-more-than-470-legal-proceedings-issued-against-health-service-after-ransomware-hit/

Solis, N. (2024, April 30). Kaiser Permanente notifies 13.4 million members of data breach - Los Angeles Times. *Los Angeles Times*. https://www.latimes.com/california/story/2024-04-26/kaiser-permanente-notifies-13-4-million-members-of-data-breach

Dhivya. (2024, May 6). MedStar Health Breach: Hackers Accessed Emails & Files. *Cyber Security News*. https://cybersecuritynews.com/medstar-health-breach/

Appendix A Presentation Slide

COMMON EXAMPLE

Ransomware
Blackmails you

Botnet
Turns your PC into a zombie

Trojans
Sneaks malware onto your PC

TYPES OF CYBER THREATS

Distributed Denial of Service (DDoS)

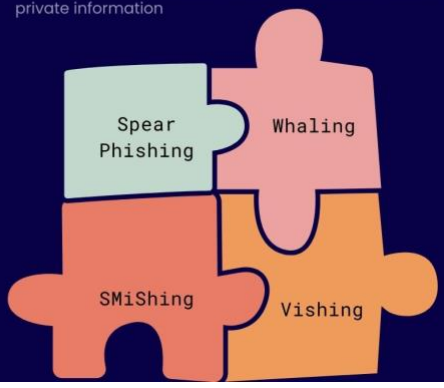
- targeted attack that bombards a network with false request
- disrupts business operations

1. Malware -> network of infected devices
2. "Botnet" floods server's traffic with false request
3. Normal traffic is denied of service

TYPES OF CYBER THREATS

Phishing

- Utilizes emails, SMS, phone calls to lure victims into sharing their private information



danaconnect.com

VULNERABILITIES IN THE HEALTHCARE SYSTEM

1. LEGACY SYSTEM

old technology used in systems

- ✗ security
- ✗ updates
- ✓ costly to replace

VULNERABILITIES IN THE HEALTHCARE SYSTEM

2. INTERNET OF MEDICAL THINGS (IOMT)

interconnected medical devices analysis of medical data for better patient outcome

- seamless communication and compatibility are key factors in a smooth operation
- when not executed, security gaps that are invisible until revealed are created

IMPACT OF CYBERSECURITY BREACHES

1. PATIENT SAFETY AND CARE DISRUPTION

1. compromised patient data
   - hackers can alter patient data that can lead to medical errors
   - identify theft, fraud
2. delayed or inadequate care
   - disrupted access during ransomeware or other incidents, EHRs cannot be accessed for procedures

IMPACT OF CYBERSECURITY BREACHES

2. FINANCIAL COST

1. recovery costs
   - investment in remedition
2. direct financial lost
   - hackers steal money from ransomware

CASE STUDIES

CASE STUDIES

RANSOMWARE ATTACK ON HSE IRELAND 2021

- Date: May 2021
- Target: Health Service Executive (HSE) of Ireland

Attack Vector:

- Sophisticated ransomware attack
- Exploited vulnerabilities in IT systems
- Used Conti ransomware, known for rapid spread across networks
- Ransom Demand: 20 million in Bitcoin

Response:

- HSE refused to pay the ransom
- Relied on backups and IT recovery efforts
- Engaged international cybersecurity experts for assistance

CASE STUDIES

DATA BREACH AT UNITYPOINT HEALTH 2024

- Date: March 2024
- Target: UnityPoint Health, a major nonprofit health system in the Midwest, US

Attack Vector:

- Phishing campaign targeted employees with emails that mimicked trusted sources.
- Attackers gained access to email systems and patient databases after several employees provided their login credentials.

Data Compromise:

- The breach exposed sensitive personal and medical data of over 1.5 million patients.

Response:

- UnityPoint Health quickly secured compromised accounts and systems.
- Cybersecurity experts were engaged to investigate and assess the breach.
- Patients were notified promptly, with offers of free credit monitoring and identity theft protection.

CASE STUDIES

DATA BREACH AT MEDSTAR HEALTH 2024

- Date: April 2024
- Target: MedStar Health, a major healthcare provider in the U.S.

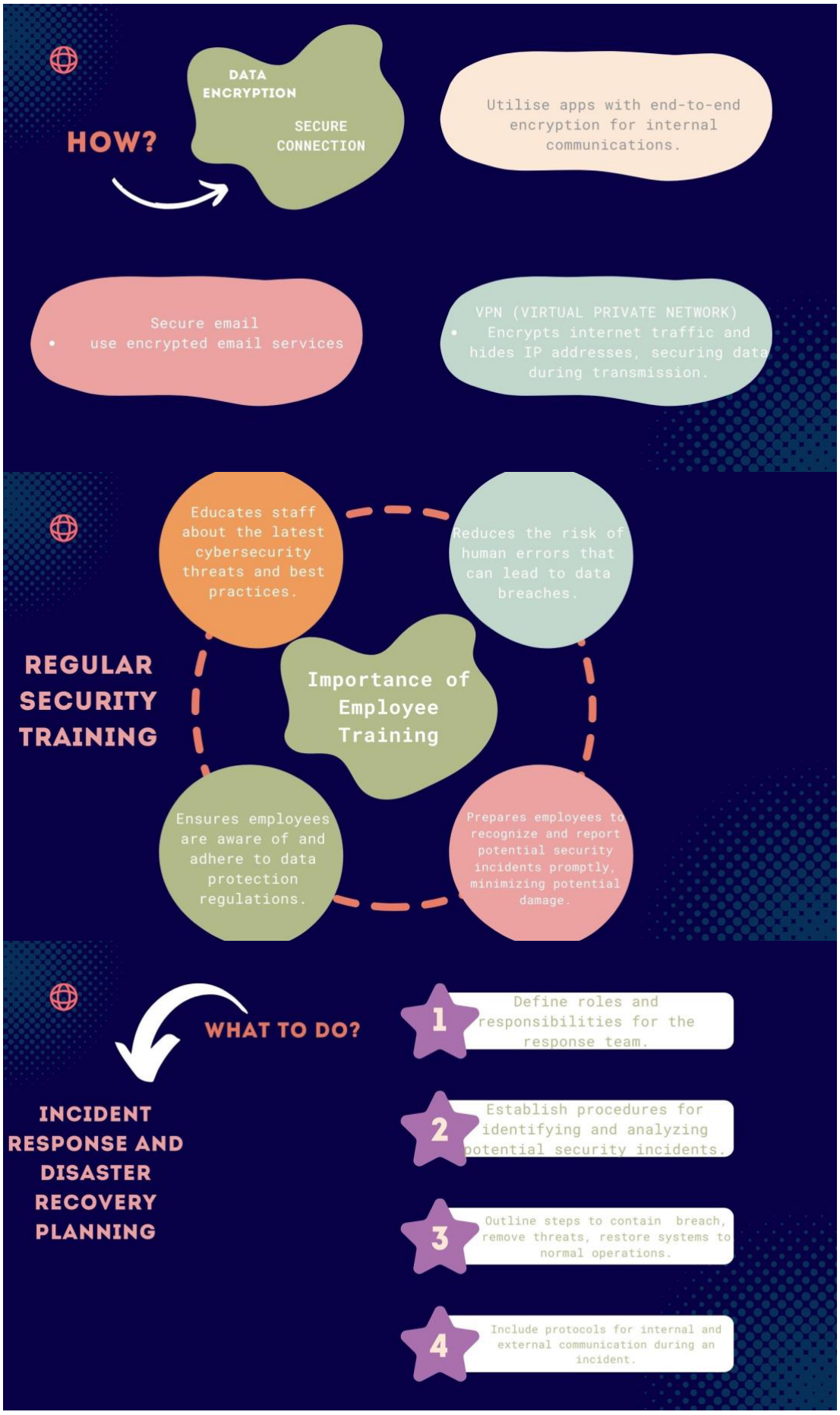
Attack Vector:

- Third-Party Vendor Compromise:
- MedStar Health's patient data was exposed due to a security breach at a third-party vendor handling billing and insurance processing.
- Attackers exploited vulnerabilities in the vendor's system to gain unauthorized access to MedStar Health's patient records.

Data Compromise:

- The breach involved the exposure of personal, medical, and financial information for over 500,000 patients.

CYBERSECURITY STRATEGIES AND BEST PRACTICE FOR HEALTHCARE


HOW?
DATA ENCRYPTION
SECURE CONNECTION
Utilise apps with end-to-end encryption for internal communications.
Secure email
use encrypted email services
VPN (VIRTUAL PRIVATE NETWORK)
Encrypts internet traffic and hides IP addresses, securing data during transmission.
REGULAR SECURITY TRAINING
Educates staff about the latest cybersecurity threats and best practices.
Reduces the risk of human errors that can lead to data breaches.
Importance of Employee Training
Ensures employees are aware of and adhere to data protection regulations.
Prepares employees to recognize and report potential security incidents promptly, minimizing potential damage.
WHAT TO DO?
INCIDENT RESPONSE AND DISASTER RECOVERY PLANNING
1
Define roles and responsibilities for the response team.
2
Establish procedures for identifying and analyzing potential security incidents.
3
Outline steps to contain breach, remove threats, restore systems to normal operations.
4
Include protocols for internal and external communication during an incident.

CONCLUSION

Cybersecurity is crucial for safeguarding patient data and maintaining trust in healthcare systems.

Key Strategies:

- Data Encryption: Keeps sensitive information secure and compliant with regulations.
- Secure Communication: Ensures confidentiality during data transmission.
- Employee Training: Reduces risk through awareness and preparedness.
- Incident Response: Prepares for and mitigates impacts of security breaches.

Outcome: Adopting these practices enhances data security, complies with regulations, and supports operational resilience.

QNA

Cybersecurity Presentation

THANK YOU FOR ATTENTION

See You Next ⟶

Appendix B Turnitin Originality Report

Document Viewer

Turnitin Originality Report

Processed on: 02-Oct-2024 19:56 +08
ID: 2472578721
Word Count: 4179
Submitted: 1

si dayang.docx By Dayang Nur Nazihah M ROSLAN

Similarity Index	Similarity by Source	
4%	Internet Sources:	2%
	Publications:	0%
	Student Papers:	3%

include quoted | include bibliography | excluding matches < 1% | mode:
quickview (classic) report | print | download

1% match (student papers from 11-Feb-2021)
Submitted to Universiti Teknologi Malaysia on 2021-02-11

1% match (student papers from 17-Aug-2024)
Submitted to Universiti Teknologi Malaysia on 2024-08-17

1% match (student papers from 20-Feb-2023)
Submitted to Universiti Teknologi Malaysia on 2023-02-20

1% match (Internet from 09-Apr-2024)
https://sppga.ubc.ca/wp-content/uploads/sites/5/2023/06/CSIS_Report_2023.pdf

1% match (Internet from 01-Aug-2024)
https://www.trendmatrix.com/newcomputing/the-evolving-cyber-landscape-adapting-to-new-threats-and-technologies/

CYBERSECURITY IN HEALTHCARE: A MATTER OF LIFE AND DEATH DAYANG NUR NAZIHAH M ROSLAN SECTION 38 UNIVERSITI TEKNOLOGI MALAYSIA ABSTRACT The purpose of this study is to investigate the role of cybersecurity in healthcare. The healthcare industry is increasingly reliant on digital technologies, from Electronic Health Records (EHRs) to telemedicine, which have revolutionized patient care exceptionally. Although this digital transformation provides many benefits to the healthcare industry, this sector has also been exposed to cybersecurity threats as it is such a significant sector. Cyber threats targeting healthcare systems range from ransomware and phishing attacks to insider threats and Distributed Denial of Service (DDoS) attacks. Vulnerabilities in these system, such as outdated infrastructure, lack of knowledge in phishing threats result in chaos. The study begins by outlining the various types of cyber threats facing the healthcare sector, including ransomware, phishing attacks, and more. The paper provides an in-depth analysis of high-profile cyberattacks that intend to illustrate the profound impact of cyber

incidents on healthcare operations, highlighting disruptions to patient care, financial losses, and long-term repercussions on organizational trust. This case study intends to explore the critical importance of cybersecurity in healthcare, highlighting how vulnerabilities can lead to the most devastating consequences, including loss of precious life. Based on the analysis of recent cyberattacks, this study will examine the impact of these breaches and what it affects. The study further outlines the best practices for healthcare providers to enhance their cybersecurity effectiveness. The importance of regular cybersecurity training for healthcare staff is emphasized, along with the need for effective incident response and disaster recovery planning. ii ABSTRAK Tujuan kajian ini adalah untuk menyiasat peranan keselamatan siber dalam sektor Kesihatan. Industri Kesihatan semakin bergantung pada teknologi digital, dari Rekod Kesihatan Elektronik (EHR) hingga teleperubatan, yang telah merevolusikan penjagaan pesakit dengan sangat baik. Walaupun transformasi digital ini memberikan banyak manfaat kepada industri kesihatan, sektor ini juga terdedah kepada ancaman keselamatan siber kerana kepentingannya yang besar. Ancaman siber yang menyasarkan sistem Kesihatan merangkumi serangan ransomware, serangan phishing, ancaman dalaman, dan serangan Distributed Denial of Service (DDoS). Kelemahan dalam sistem ini, seperti infrastruktur yang usang dan kekurangan pengetahuan tentang ancaman phishing, mengakibatkan kekacauan. Kajian ini dimulakan dengan merangkumi pelbagai jenis ancaman siber yang dihadapi oleh sektor kesihatan, termasuk ransomware, serangan phishing, dan lain-lain. Ia memberikan analisis mendalam tentang serangan siber yang terkenal yang bertujuan untuk menggambarkan kesan mendalam insiden siber terhadap operasi kesihatan, menyoroti gangguan kepada penjagaan pesakit, kerugian kewangan, dan kesan jangka panjang terhadap kepercayaan organisasi. Kajian kes ini bertujuan untuk meneroka kepentingan kritikal keselamatan siber dalam sektor kesihatan, menyoroti bagaimana kelemahan boleh membawa kepada akibat yang paling teruk, termasuk kehilangan nyawa yang berharga. Berdasarkan analisis serangan siber terkini, kajian ini akan memeriksa kesan pelanggaran tersebut dan apa yang terjejas. Kajian ini seterusnya menggariskan amalan terbaik untuk penyedia penjagaan kesihatan bagi meningkatkan keberkesanan keselamatan siber mereka. Kepentingan latihan keselamatan siber yang berterusan untuk kakitangan kesihatan ditegaskan, bersama dengan keperluan perancangan tindak balas insiden dan pemulihan bencana yang berkesan.

Things Distributed Denial of Service Electronic Health Record Europe, Middle East, and Africa Asia-Pacific and Japan Short Message Service SMS Phishing Information Technology viii LIST OF APPENDICES APPENDIX TITLE PAGE Appendix A Presentation Slide 27 CHAPTER 1 INTRODUCTION 1.1 Introduction As the healthcare industry increasingly integrates with the use of technology, it has become a prime target for cybercriminals. The privacy of healthcare data, combined with the critical need of uninterrupted access to medical services, makes the protection of this sector not only a matter of protecting sensitive information, but a matter of protecting lives. Cyber threats such as ransomware, phishing, and Distributed Denial of Service (DDoS) attacks have becoming increasingly common. These data breaches can lead to disruption of patient care, financial losses and long-term damage to organizational trust. This investigation intends to elaborate on the critical importance of cybersecurity in healthcare, the impact of recent cyberattacks, and the steps that healthcare providers can take to preserve important data. 1.2 Problem Background The rapid integration of digital technologies into healthcare systems created challenges in the cybersecurity sector. The exposure to cyber threats has been growing especially with interconnected networks between systems. The high value of sensitive patient data and the urgency of healthcare operations make the healthcare sector particularly a favored target for cybercriminals. The balance between maintaining patient confidentiality and accessible medical data increases the chances of becoming a target. Moreover, the existing systems are more prone to vulnerabilities as the lack of adequate cybersecurity training among healthcare professionals fuels the issue, as human error is one of the most significant contributors to security breaches. Additionally, the rise of the Internet of Medical Things (IoMT) and the increasing complexity of healthcare networks have expanded the attack surface which has created more entry points for cybercriminals to exploit. 1.3 Project Aim The aim of this project is to assess the impact of cybersecurity threats on healthcare systems and explore strategies to protect patient data and ensure safe healthcare operations. 1.4 Project Objectives The objectives of the project are: (a) To estimate the parameters affecting cybersecurity in healthcare. (b) To identify key cybersecurity threats and vulnerabilities in healthcare systems. (c) To analyse the impact of recent cyberattacks on healthcare operations and patient safety. (d) To define the best practices and strategies for enhancing cybersecurity in healthcare. 1.5 Project Scope The scopes of the project are: 2 (e) To explore the current cybersecurity landscape within the healthcare industry, focusing on common threats and vulnerabilities. (f) To evaluate the effectiveness of existing cybersecurity measures and recommend strategies for improvement tailored to healthcare environments. CHAPTER 2 Cybersecurity Threats in Healthcare 2.1 Types of cybersecurity threats 2.1.1 Malware Malicious software – is any program or code that is created with the intent to infect, damage, or gain access to computer systems. It's designed to infiltrate your device without any signals, causing damage and disruption to the computer's system or steal confidential information. There are many types of malware, but each and every one is designed to compromise the security of systems. Malware is triggered to be downloaded into computer e.g. clicking an infected link through email. It starts to infect the computer by beginning its task - stealing data, installing more malware and more. It will stay on the system until detected and removed. Figure 2.1.1 How Malware Works While not all malware are essentially viruses, each and every malware installed on your computer poses a threat of data breach and harms the computer system. A common example of malware is ransomware. Ransomware is when the installed malware denies access to the system by locking and encrypting files following threats to release private information or erasing of important files unless paid a ransom. The most recent case for ransomware in the healthcare industry is a ransomware attack that disrupted multiple London hospitals. A company called Synnovis that provide pathology services to

hospitals detected an incident which disrupts the blood transfusion IT system. This resulted in cancelled appointments or patients having to redirected to other service providers. This attack was done by Qilin, a Russian cybercrime group, whom shared 400GB of private data on the dark web a following their aim to extort $50 million from Synnovis. The hackers executed this breach by injecting malware that locked the entire computer system with the condition that the system will be released if the ransom was paid. 2.1.2 Distributed Denial of Service (DDoS) Attacks A malicious, targeted attack that bombards a network with false request to disrupt their business operations. Users become incapacitated to perform tasks on their computer. Attackers use malware to create a network of internet-connected devices that are infected which are used to send traffic. This botnet may include Internet of Things (IoT), phones, computers, routers and servers. This creates waves of attacks spreading further and further. Like zombies attacking humans to turn them into zombies. Once a botnet has been built, instructions are sent, directing them to flood servers with false requests. Normal traffic is denied of service due to the overwhelming amount of traffic. Research shows that the Europe, Middle East and Africa (EMEA) region went through 86% of 7 application layer DDoS attacks. 7% each was accounted for North America and Asia-Pacific and Japan (APJ). Figure 2.1.2 The statistics of 7 layer DDoS attacks in EMEA, North America and APJ between January 1, 2023 – March 31, 2024 As an example, Singapore's public healthcare institutions were disrupted through internet connectivity with DDoS attacks. The company, Synapxe detected an abnormal surge in network traffic during morning operations. The agency's firewall became overwhelmed in moments. This triggered the firewall to uphold traffic, which resulted in inaccessible any internet-reliant services. Though after the incident happened, measures were put up to protect the system which enabled it to withstand the attack and prevented data from being compromised. 2.1.3 Phishing Phishing is a common cyberattack that utilizes emails, SMS, phone calls and other platforms to lure a victim into sharing their private information. There are a variety of phishing attacks, including: Type Description Spear Phishing Target's individuals through malicious emails. Whaling Targets senior executive employees to steal money or information. SMiShing Targets individuals through fraudulent text messages. Table 2.1.3 Types of Phishing attacks Not only does it trick people into sharing sensitive information, when a person clicks on illegitimate links in emails, malware can also be downloaded into their computer infecting the entire system. A recent case in the healthcare industry is Ascension health system data breach. An individual at the facilities unintentionally downloaded a malicious file that was thought to be legitimate. They experienced a weeklong disruption where they were locked out of the system that coordinates almost all aspects of patient care. The result of this was lost lab results, medication errors and absence of routine safety checks. Black Basta, a group of cybercriminals were identified as the hackers. Files that contained protected health information were stolen. 2.2 Vulnerabilities in the Healthcare System As the healthcare industry integrates with modern technology, more opening to cybercrimes is emerging. Without addressing these vulnerabilities, a system can easily be targeted to be exploited. 2.2.1 Legacy Systems Legacy Systems refer to older technology that are still used because upgrades are costly. These outdated systems lack the security that can protect them from modern cybersecurity threats which make them vulnerable to attacks like ransomware and unauthorized access. As technology advances, vendors tend to withdraw support from these older software, meaning that the software are no longer being updated. With systems such as healthcare that rely heavily on their networks for day to day operations, it becomes difficult to upgrade these systems as it can be time-consuming. A notable example is the transition of hospitals and health systems to new EHR platforms. Organizations such as Intermountain Health and Indian Health Services, faced significant

difficulties in maintaining data integrity during the transition. 2.2.2 Internet of Medical Things (IoMT) IoMT represents the evolution of technology in the healthcare industry as it encompasses a variety of interconnected medical devices used. It allows wireless and remote devices to communicate using the internet to conduct an analysis of medical data for better patient outcome. i. In-Hospital IoMT IoMT sensors are used to track interactions between personnel and patients so administrators can understand of what goes about the premises. ii. In-home IoMT Users can transmit medical data from home to care provider facilities not only to be alerted during a medical situation, but also track patient condition to monitor and predict outcomes. iii. On-body IoMT This IoMT is designed to be wearable to remotely track and monitor system. It can be worn and taken everywhere unlike in-home IoMT. iv. Community IoMT Used throughout a larger part of the geographic area. Tracks patient metrics outside of the hospital. Figure 2.2.1 IoMT Applications Having to ensure communication is seamless and all devices are compatible with each other can create issues during the process, which can leave security gaps that are not noticeable until an incident happens. 2.3 Impact on Cybersecurity Breaches 2.3.1 Patient Safety and Care Disruption When ransomware occurs to a hospital's patient care system, EHRs tend to be held hostage. This affects the ability to access to patient data where hackers can purposely or unintentionally alter patient's data which can result in drastic medical errors. Not only that, but proper medication could also be locked away and inaccessible during a crisis. 2.3.2 Financial Cost One of the financial impacts during a cyberthreat is the cost to recover from the situation. There are the legal fees, operational costs, investment for improvement in the IT sector which take a toll on a healthcare system's finance situation. Not to mention the possibility of hackers stealing money when already hacked into the system and ransom asked to recover the system. 2.4 Chapter Summary a) There are many types of security threats: malware disrupts systems and steals data (e.g., 2021 Synnovis ransomware), DDoS overloads networks causing service disruptions (e.g., Singapore 2023), and phishing tricks users into sharing sensitive info (e.g., Ascension Health breach). b) Legacy systems are outdated tech lacking security updates, while IoMT introduces connected devices that may create security gaps. c) Ransomware locking EHRs can lead to errors in patient care, and breaches incur recovery costs and potential ransom payments, impacting financial stability. CHAPTER 3 CASE STUDIES 3.1 Introduction Cybersecurity breaches in healthcare have become increasingly common as the industry depends more on digital systems to manage sensitive data. These breaches, including ransomware attacks and data leaks, can disrupt healthcare services and compromise patient privacy. This chapter examines key incidents, highlighting vulnerabilities in healthcare IT systems and the risks associated with third-party vendors. 3.2 Ransomware attack on HSE Ireland 2021 Figure 3.2.1 HSE Ireland cyber-attack 2021 In May 2021, the Health Service Executive (HSE) of Ireland faced a sophisticated ransomware attack that severely impacted its IT systems. The attack, orchestrated by the Conti ransomware group, exploited existing vulnerabilities in the HSE's digital infrastructure. Conti, known for its ability to rapidly spread across networks, encrypted the organization's data and demanded a ransom of 20 million in Bitcoin in exchange for the decryption keys. The attack caused widespread disruption, affecting patient care, diagnostic services, and general healthcare operations across Ireland. Despite the pressure, the HSE made the decision not to pay the ransom. Instead, the organization initiated a large-scale recovery operation, relying heavily on backups to restore its systems. The Irish government supported the HSE's stance, emphasizing the importance of not giving in to criminal demands, a move that was in line with international guidance on ransomware response. Additionally, the HSE sought assistance from international cybersecurity experts to aid in mitigating the impact of attack and fortifying its IT infrastructure against

future threats. The consequences of the attack were profound, highlighting the vulnerabilities in the healthcare sector's digital systems. It also underscored the growing threat of ransomware, which targets critical services and organizations with high stakes, knowing the potential consequences of prolonged downtime. The HSE's recovery process was long and complicated, requiring significant resources and collaboration with both domestic and international entities to bring services back to full functionality. This incident prompted a re-evaluation of cybersecurity measures within the healthcare sector in Ireland and beyond, leading to a stronger focus on securing critical infrastructure from future cyber threats. 3.3 Data Breach at Kaiser Foundation Health Plan 2024 Figure 3.3.1 Kaiser Foundation Health Plan 2024 data breach In April 2024, Kaiser Foundation Health Plan experienced a significant data breach that impacted approximately 13.4 million individuals. The breach was not due to hacking but resulted from the unauthorized disclosure of sensitive information through tracking technologies embedded in its websites and apps. These tools collected visitor data, including potentially private health information, and shared it with third parties like Google and Meta without proper business associate agreements in place. This incident highlights the risks posed by inadequate oversight of third-party technologies in healthcare application. The breach primarily affected individuals who interacted with Kaiser's online services. Once the issue was discovered, the organization took steps to assess the extent of the data leak and began notifying affected individuals. Given the scale o the breach, this incident was one of the largest in healthcare for 2024 and raised concerns about the increasing reliance on digital tools in healthcare without fully understanding their privacy implications. Following the breach, Kaiser Foundation Health Plan faced significant criticism and scrutiny from regulators and privacy advocated. It underscored the need for stronger safeguards and compliance protocols when using third-party tracking technologies, particularly in industries like healthcare, where data confidentiality is top priority. This case serves as a cautionary tale for other healthcare providers to ensure that patient privacy is protected in both traditional and digital healthcare environments. 3.4 Data Breach at MedStar Health 2024 Figure 3.4.1 Data Breach at MedStar Health 2024 In April 2024, MedStar Health, a prominent healthcare provider in the U.S., experienced a significant data breach due to a security compromise at a third-party vendor responsible for billing and insurance processing. Attackers exploited vulnerabilities in the vendor's system, allowing them to gain unauthorized access to MedStar Health's sensitive patient records. This breach highlighted the risks associated with relying on external partners for critical healthcare operations. The breach resulted in the exposure of personal, medical, and financial information for more than 500,000 patients. Compromised data included names, Social Security numbers, medical histories, and insurance details, raising concerns about potential identity theft and fraud. The incident demonstrated how vulnerabilities in third-party systems can have a direct and severe impact on organizations that depend on these services, even when their own internal systems are secure. MedStar Health responded by immediately working with the third-party vendor to secure the affected systems and prevent further access. They also engaged cybersecurity experts to investigate the breach, assess the damage, and ensure compliance with federal healthcare privacy regulations. The organization began notifying affected patients and offering identity theft protection services to mitigate the risk of personal and financial harm. This breach underscored the importance of stringent cybersecurity measures not only within healthcare organizations themselves but also among the vendors and partners they rely on to process sensitive information. 3.5 Chapter Summary a) In May 2021, the ransomware attack on HSE Ireland by Conti ransomware group severely impacted the organization's IT systems, disrupting healthcare services. The HSE refused to pay the ransom and instead relied on backups for recovery,

with international assistance. The attack highlighted vulnerabilities in healthcare infrastructure and emphasized the growing threat for ransomware. b) In April 2024, Kaiser Foundation Health Plan experienced a data breach that exposed the sensitive information of 13.4 million individuals. The breach occurred due to the use of third-party tracking technologies that shared user data with companies like Google and Meta. The incident highlighted those risks of relying on third-party tools in healthcare and emphasized the need for better oversight of digital privacy practices. c) In April 2024, MedStar Health experienced a data breach caused by vulnerabilities in a third-party services and the need for stringent security measures for both healthcare organization and their partners. CHAPTER 4 CYBERSECURITY STRATEGIES AND BEST PRACTICE FOR HEALTHCARE 4.1 Introduction In healthcare, protecting patient information is more than just a technical challenge – it's about safeguarding lives and maintaining trust. Every day, healthcare providers rely on digital systems to deliver care, while patients trust that their personal and medical details are kept safe. However, as these systems grow more complex, so do the risks of cyberattacks. From protecting private health records to ensuring hospitals can function without disruption, cybersecurity in healthcare has never been more important. This section highlights practical strategies and best practices to help keep patient data secure and healthcare systems resilient. 4.2 Data Encryption and Secure Connection One of the ways to ensure sensitive data will not be exposed is by using software that can assist with data encryption. For instance, utilizing apps with end-to- end encryption for internal communications such as Telegram, Whatsapp, iMessage and others. Not only messaging apps, but encrypted email services are also a crucial factor in preventing cyberattacks such as phishing from occurring to a healthcare system. Another way for encryption is using Virtual Private Network (VPN) which can encrypt internet traffic and hides IP addresses. This can ensure data is secured during transmission. 4.3 Regular Security Training Frontliners in healthcare also need cyber awareness, without it many can be tricked that can result in cyberattacks. This can prepare the employees to recognize and report potential security incidents promptly to reduce the risk of human errors that can lead to data breaches. By educating employees about the latest cybersecurity and best practices, employees can be more aware of and adhere to data protection regulations. 4.4 Implementing Incident Response and Disaster Recovery Planning Define roles and responsibilities for the response team. Establish procedures for identifying and analyzing potential security incidents. Outline steps to contain breach, remove threats, restore systems to normal operations. Include protocols for internal and external communication during an incident Figure 4.4.1 Incident Response and Disaster Recovery Planning The figure above shows the steps for incident response and disaster recovery planning. Without a proper policy, the affected personnel could easily enter a panicked state during a crisis. This can lead to even more consequences that impact on the system that would be difficult for the recovery process. 4.5 Chapter Summary a) Data encryption and secure connection can be achieved through encryption techniques. Healthcare providers should use encrypted communication apps (e.g., Telegram, Whatsapp) and email services to prevent breachers, along with VPNs to secure internet traffic during transmission. b) Regular security training for healthcare employees is crucial to minimize human errors that could lead to data breaches. Training improves awareness and enhances the ability to identify and report security threats. c) Incident response and disaster recovery planning are essential for healthcare systems to recover quickly and effectively from cyberattacks. Proper planning helps mitigate panic and reduces the impact of a crisis, facilitating smoother recovery CHAPTER 5 CONCLUSION 5.1 Research Outcomes Cybersecurity threats in healthcare, particularly breaches, pose significant risks to patient data, healthcare operations and public safety. With the increasing reliance on

electronic health records (EHRs) and interconnected medical devices, healthcare organizations are more vulnerable to cyberattacks. Each year, healthcare institutions globally experience data breaches affecting millions of patients, highlighting the urgent need for enhanced security measures. With the growing awareness of these challenges within the healthcare sector, governments, stakeholders, and experts are collaborating to develop better security frameworks, invest in more advanced infrastructure and implement comprehensive response plans to protect healthcare data and maintain patient safety. 5.2 Contributions to Knowledge The findings of this study contribute to the ongoing efforts of healthcare providers, IT specialists and policymakers to strengthen cybersecurity in healthcare systems. This research can provide valuable insights for healthcare organizations, government agencies and cybersecurity professionals.

REFERENCES CrowdStrike. (2024, May 31). 12 most common types of cyberattacks today - CrowdStrike. crowdstrike.com. https://www.crowdstrike.com/cybersecurity- 101/cyberattacks/most-common-types-of-cyberattacks/ Critical incident declared as ransomware attack disrupts multiple London hospitals. (n.d.). https://therecord.media/london-hospitals-ransomware-attack-critical-incident- declared Dean-Foster, E., & Dean-Foster, E. (2024, July 19). Ransomware Assault on NHS: A Deep Dive into the Synnovis Data Breach. Intercede. https://www.intercede.com/ransomware-assault-on-nhs-a-deep-dive-into-the- synnovis-data-breach/ Ascension: Cyberattacker stole files likely containing protected health, identity data. (2024, June 12). Fierce Healthcare. https://www.fiercehealthcare.com/providers/systems-clinical-operations-interrupted- ascension-amid-apparent-cybersecurity-event LaPointe, J. (2024, March 18). 63% of known exploited vulnerabilities found on healthcare networks. Healthtech Security. https://www.techtarget.com/healthtechsecurity/news/366593999/63-of-known- exploited-vulnerabilities-found-on-healthcare-networks 2024: The year of health IT transformation and evolution in patient care - Health Data Management. (2024, January 12). Health Data Management. https://www.healthdatamanagement.com/articles/2024-the-year-of-health-it- transformation-and-evolution-in-patient-care Ordr. (2024, July 5). IoMT and its Transformative Impact on Healthcare Security - Ordr. https://ordr.net/article/what-is-iomt 16 apps that use end to end encryption. (n.d.). https://www.sliksafe.com/blog/16-apps- that-use-end-to-end-encryption Ordr. (2024, July 5). Healthcare Cybersecurity strategy to secure medical Assets - OrdR. https://ordr.net/article/what-is-healthcare-cybersecurity Bowers, S. (2024, May 14). HSE cyber attack: More than 470 legal proceedings issued against health service after ransomware hit. The Irish Times. https://www.irishtimes.com/health/2024/05/14/hse-cyber-attack-more-than-470- legal-proceedings-issued-against-health-service-after-ransomware-hit/ Solis, N. (2024, April 30). Kaiser Permanente notifies 13.4 million members of data breach - Los Angeles Times. Los Angeles Times. https://www.latimes.com/california/story/2024-04-26/kaiser-permanente-notifies-13- 4-million-members-of-data-breach Dhivya. (2024, May 6). MedStar Health Breach: Hackers Accessed Emails & Files. Cyber Security News. https://cybersecuritynews.com/medstar-health-breach/