Cyber Security threats and mitigations in the Healthcare Sector with emphasis on Internet of Medical Things.

IE3022-Applied Information Assurance

Assignment 1

3rd year 1st semester

Assignment 01

it20613518@my.sliit.lk

***Abstract*—Healthcare is one of the important things to people in world. Because of that, healthcare sector has many Cyber threats in modern world. This review paper discusses about these cyber threats, vulnerabilities/ Cyber security issues, how to mitigate threats, best practices,**

and future development areas of healthcare section.

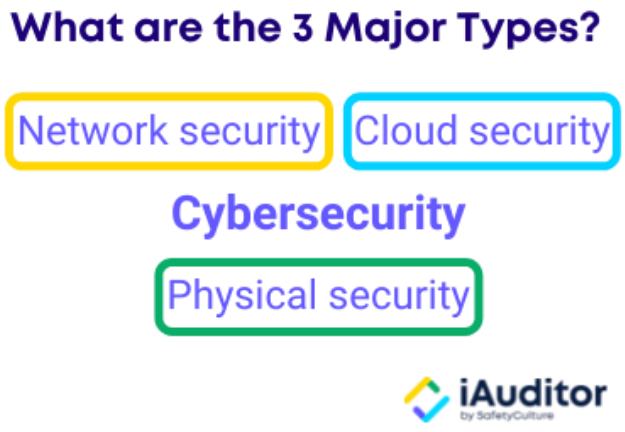
Keywords—Healthcare, Cyber Security, Cyber threats, mitigate.

1. INTRODUCTION

The Internet of Things (IoT) refers to a network of physical devices connected to the internet with the purpose of absorbing and exchanging various types of data. Computing devices and mobile phones are used as connected devices. In modern world, healthcare section has IOT devices to do treatment and other works well. These IOT devices have transformed how industrial organizations, utilities, and manufacturers function in the healthcare sector. In past, communication between the patient and doctor were happened through in-person encounters and telephone calls. But now it happens through different communication methods. So, now most of the patients use e-channelling to meet doctors. And also, Hospitals use new technology healthcare equipment to treatment patients. All the hospitals are computerized, and they are interconnected through networks. These things are result of IOT devices. So that healthcare section has more cyber threats. [1]

A. Cyber Security

Cybersecurity is a collection of best practices used to defend against unauthorized access that could be a part of coordinated cyberattacks and other harmful digital threats against a commercial enterprise. Healthcare section organizations need to improve their IOT devices security. Because lot of attackers try to attack this section in modern world. [2]



B. Cyber Threats

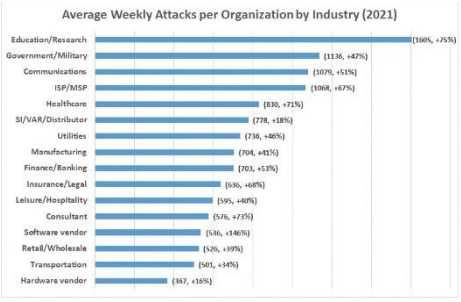
A harmful act intended to steal, corrupt, or undermine an organization's digital welfare and stability is referred to as a cyber threat. Data breaches, computer viruses, denial-of-

service attacks, and many other attack types are only a few of the many types of cyber threats. [3]

By 2025, threat actors will have successfully leveraged operational IT settings to cause human casualties, predicts Gartner. https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio# A ransomware attack that targets a hospital's operational technology (OT) systems will have disastrous effects, including locking hospital staff members out of crucial facilities, preventing them from accepting new patients, and preventing them from accessing patient information. If Gartner's prediction comes to pass, healthcare institutions would not only have to worry about patient data but also about the patients themselves. Organizations should begin concentrating on OT security in addition to IT security. Healthcare firms should stay up to date to prevent cyberattacks on everything from asset inventory to network segmentation to patch management. [3]

2. SIGNIFICANT

The patient's health is the first priority in healthcare, and it is becoming more and more dependent on medical systems and technology. The more quickly a patient obtains the proper care in the proper setting with the proper tools, the better the odds of a successful outcome. Patient safety and privacy are also at danger from cyber-attacks on programs, Personal Identification Information (PII), and Protected Health Information (PHI). Loss of access to medical equipment and records can encrypt and keep files hostage, much like a ransomware assault. Private patient information may be accessed by the hacker and taken. Additionally, the attacker may change patient data mistakenly or on purpose, which could have a major negative impact on patients' health. [4]



According to Helathcaredive, [5] a security business owned by NTT Group, 88% of all ransomware assaults in the United States last year targeted the healthcare sector. According to a study by the Ponemon Institute, [6] 89% of healthcare businesses looked at had a data breach over the previous two years that involved patient data being lost or stolen.

At least 125 electronic data breaches of healthcare institutions have been reported since the beginning of April, according to a list compiled by the U.S. Department of Health and Human Services (HHS). [7] The Yuma Regional Medical Centre in Arizona is one such example; the hospital recently announced that it had been the target of a ransomware assault that exposed the data of 700,000 people. This is one of the largest breaches to be publicly publicized in the past five months and which is also the biggest breach to be classified as a ransomware attack. The following table shows that last 24 months data breach cases in USA.

Breach Report Results

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
0	Molina Healthcare	CA	Health Plan	8283	09/09/2022	Unauthorized Access/Disclosure	Paper/Films
0	SERV Behavioral Health Systems, Inc.	NJ	Healthcare Provider	8110	09/09/2022	Hacking/IT Incident	Network Server
0	The Sargent's Group	PA	Business Associate	1650	09/09/2022	Hacking/IT Incident	Network Server
0	Lubbock Heart & Surgical Hospital	TX	Healthcare Provider	23379	09/09/2022	Hacking/IT Incident	Network Server
0	Medical Associates of the Lehigh Valley	PA	Healthcare Provider	75828	09/09/2022	Hacking/IT Incident	Network Server
0	Wolfe Clinic, P.C.	IA	Healthcare Provider	542776	09/09/2022	Hacking/IT Incident	Electronic Medical Record
0	Empress Ambulance Service LLC	NY	Healthcare Provider	318558	09/09/2022	Hacking/IT Incident	Network Server
0	DaVita Inc.	CO	Healthcare Provider	1092	09/06/2022	Hacking/IT Incident	Laptop
0	Reiter Affiliated Health and Welfare Plan	CA	Health Plan	45000	09/02/2022	Hacking/IT Incident	Network Server
0	Reiter Affiliated Companies, LLC	CA	Business Associate	48000	09/02/2022	Hacking/IT Incident	Network Server
0	The Physicians' Spine and Rehabilitation Specialists of Georgia, P.C.	GA	Healthcare Provider	38765	09/02/2022	Hacking/IT Incident	Network Server
0	Independent Living Systems, LLC	FL	Business Associate	501	09/02/2022	Hacking/IT Incident	Network Server

3. RESEARCH STATEMENT

This review paper is written for understanding security threats, challengers, weaknesses, and mitigation methods for healthcare industry in whole world. In addition, this includes security laws, regulations, standards. Healthcare industry needs to focus on future development areas. Lastly, I include some areas as well.

4. CRITICAL EVALUATION

A. Iot Devices In Healthcare section

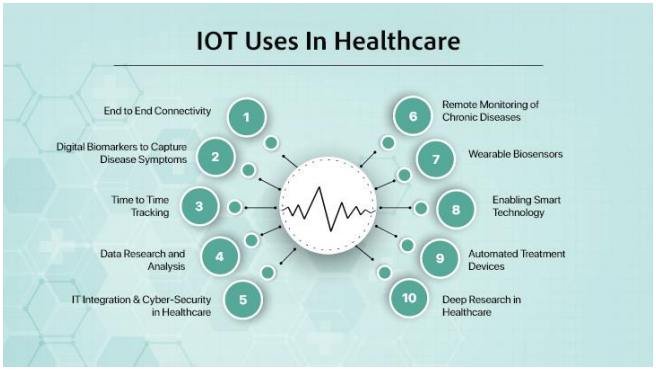
Healthcare section firstly used IOT devices for Electric health records (EHR). *[1]* Electric health records were made easy to handle hospitals system in past. This is how healthcare industry started to use IOT devices. IoT software are used for a wide range of healthcare applications, including medication management and patient monitoring. In consequence, this IoT data collection aids in more accurate study and data to comprehend patients' wellness. Patients can now arrange appointments using digital healthcare applications without having to phone a doctor's office and wait for a receptionist. Further, doctor may now continuously check on a patient's health and symptoms without doing any tests thanks to the internet of things. *[8]*

Healthcare practitioners can expand their reach outside of the conventional clinical setting thanks to the Internet of Things. There is a technology called remote patient monitoring (RPM) technology. In order to give doctors with a constant stream of real-time health data, including heart rate, blood pressure, and glucose monitoring, this technology makes use of linked devices with IoT sensors.

As tech companies look to capitalize on the expanding possibility in the lucrative digital health sector, wearables like the Smart Watches are now incorporating additional medical device functions in addition to measuring basic fitness levels.

In addition, IOT devices use for following tasks in healthcare. [8]

- Real time patient monitoring
- Hand hygiene monitoring
- Depression and mood monitoring
- Diseases monitoring
- Automated treatment



In Pandemic situation, patients get their treatment from IOT devices. Because doctors not able to be with patients. And also, healthcare section used PCR machines to get PCR report to know whether patient is positive or negative. [9]

B. Security issues in Healthcare inducstry IOT things.

Healthcare should always be secured from assaults because it is a crucial component of infrastructure. However one of the key reasons it is such a desirable target for an attacker is because of its criticality. Therefore, in order to prevent becoming a victim of horrifying cyberattacks, it becomes extremely important for healthcare and healthcare-related enterprises to strengthen their cybersecurity practices.

Healthcare section has huge cyber security related issues. That issues are helpful to attackers to launch attack successfully to healthcare company. So, first healthcare organizations need to identify their issues.

- A lack of strong IT security policies.
- Insufficient cybersecurity awareness and training for staff.
- A lack of cyber security professionals to healthcare section.
- A lack of or inadequate network segmentation.

In addition, 37% of critical and high vulnerabilities were in following three areas in healthcare, according to HIPPA research. [8]

- User authentication

Deficits in user authentication is the most frequent security flaws in the healthcare sector. These are mistakes in properly authenticating users and determining the degree of access that users should have to resources within an organization.

- Endpoint leakage

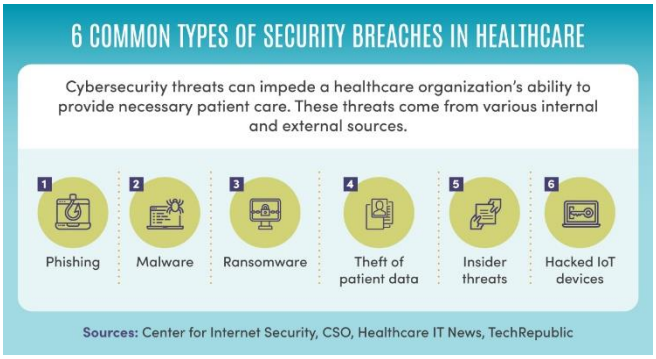
Endpoints are any end-user equipment that is linked to an organization's IT network, such as laptops, mobile devices, medical equipment, printers, servers, smartwatches, and printers. A single healthcare companies like hospital network may contain thousands of endpoints. Endpoint leakage means endpoint devices data leak to unauthorized parties. [10]

- Excessive user permissions

This happens a result of weak access controls in healthcare organizations. Attackers able to get administrative privileges to data. This is a critical vulnerability in healthcare industry. [8]

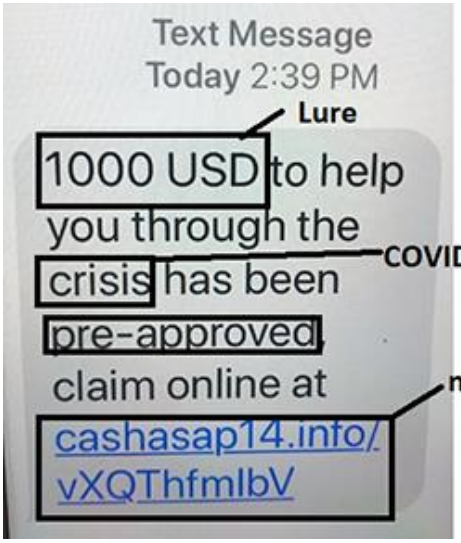
C. Cyber threats in healthcare sector

There are several cyber threats to healthcare industry. Most popular one is ransomware attacks. Attackers try to launch ransomware attacks because healthcare data like patient data are very important and critical. So, most of the organizations pay and get their data back. This is very good opportunity for attackers to gain money. Other than that, there are more attacks launch to aim healthcare section. [11]



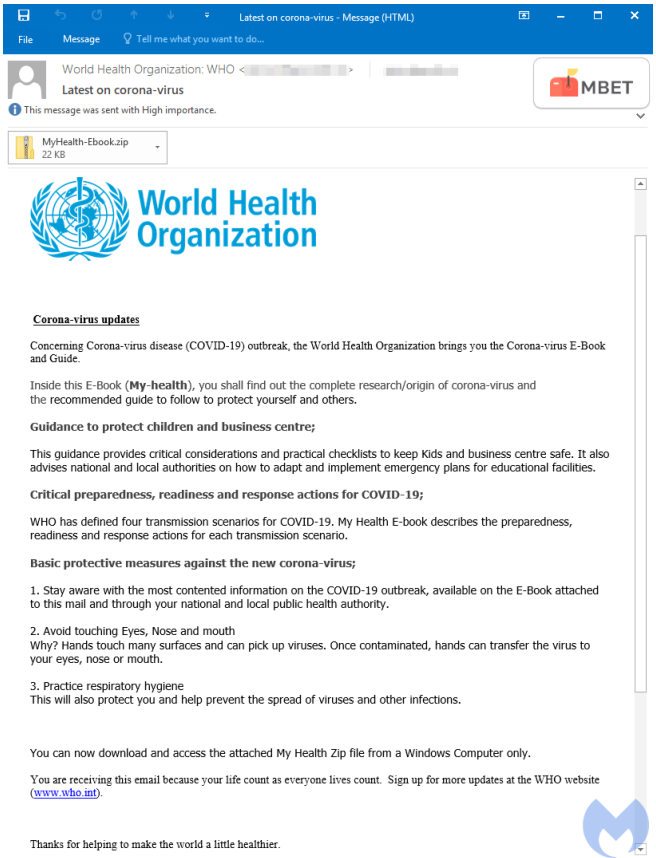
Phishing:

When a hacker pretends to be a reliable email source, they attempt to trick users into clicking a link. Hackers can acquire private data in this way, including passwords and credit card numbers. In healthcare section attackers able to gain access to patient or administrative privileges from this. Following picture is the example for phishing text message.

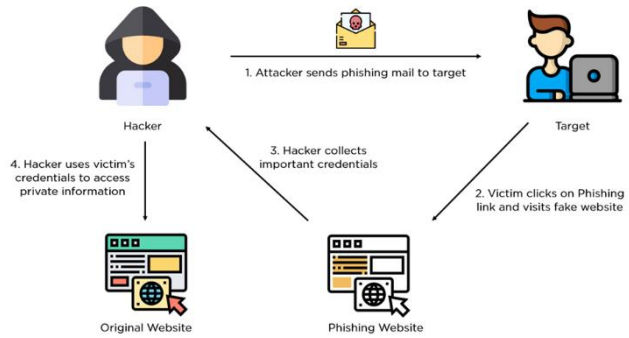


Phishing emails are the mostly used by attackers. Phishing emails sometimes make reference to a well-known medical condition to encourage link clicking. They can appear very convincing. [11]

The following is an illustration of a phishing email purporting to be from the World Health Organization. [12]



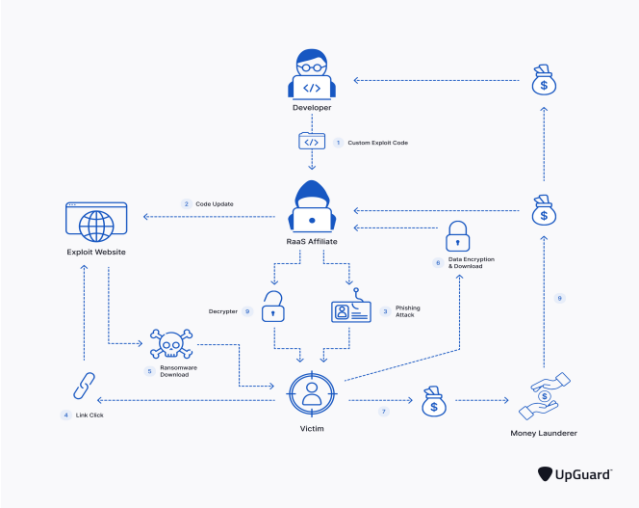
This is how phishing attack basically happens.



Malware:

Computer software designed to harm a network, a computer, or another linked system. Viruses, Trojan horses, spyware, and adware are all examples of malicious software.

Malware known as ransomware employs encryption to prevent users from accessing systems or to threaten to make user data public unless a ransom is paid. Recently, ransomware attacks have new variation called Ransomware-as-a-Service (Raas). It processes happens like following picture. [13]



Patient information theft:

Stolen medical records may be used to commit fraud, such as posing as someone else to apply for payment for healthcare services. [13]

Insider threats:

Key systems are put at danger by those who unintentionally or voluntarily have access to them. Insider risks in the healthcare industry may originate from current or former workers, contractors, or vendors. [12]

Hacked IOT devices:

IoT devices that have been compromised The Internet of Things has enabled billions of items to be interconnected, ranging from security camera sensors to portable medical

gadgets. Hackers may get access to systems containing confidential medical data by taking advantage of holes in these links. [13]

Data Breaches:

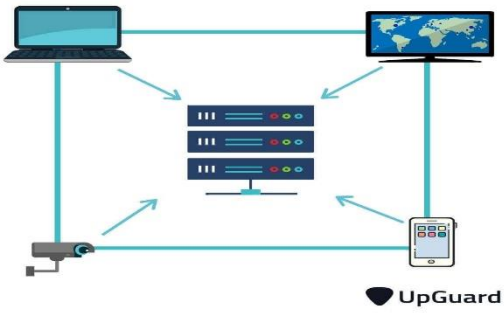
Comparatively speaking, the healthcare sector has a disproportionately high number of data breaches. In the healthcare industry, there were 1.76 data breaches on average every day in 2020. HIPAA lays forth stringent guidelines for preventing unauthorized access to sensitive information like health data, but many healthcare organizations have trouble putting its security rules into practice.

Despite efforts to limit these occurrences through frameworks like HIPAA, such cybersecurity gaps give cyber attackers access points via which they can continue to compromise the security of medical care data.

DDoS Attacks:

A distributed denial-of-service (DDoS) attack is a malicious attempt to obstruct a server, service, or network's regular traffic by saturating the target or its surrounding infrastructure with an excessive amount of Internet traffic.

This effect healthcare section heavily because this can Interrupt operations of patients and other healthcare resources. So, this attack can be responsible to patients' death also. Therefore, this is a very dangerous attack to healthcare industry. [14]



D. Security controls for Healthcare industry.

1) CYBERSECURITY EDUCATION:

Educating healthcare employees about fundamental cybersecurity principles, such never clicking a link in an email from an unknown sender, can help significantly reduce cyber dangers. For that, healthcare organizations can organize awareness training programmes. [11]

2) Quickly implementing software updates:

Make sure that systems are running the most recent software version because software upgrades frequently include patches to remedy weak security. Because old software updates can be vulnerable to attacks. Therefore, installing security and software updates are mandatory. [11]

3) Putting into use tested cybersecurity software:

Healthcare cybersecurity experts may assist with problem resolution in addition to deploying cybersecurity software on all connected devices. There are some software's that vulnerable to attacks. So, before installing software, healthcare organizations need to test software. [11]

4) Enhancing system access restrictions:

Risk can be reduced by limiting access to those who require it. For this healthcare organizations need to implement proper access control mechanism. Then, organizations can ensure limit user permissions for their systems. [11]

5) promoting best practices, such as upgrading system passwords, to:

Everyone who used healthcare systems are responsible for system security. So, users need to choose strong passwords with contain capital and simple letters, numbers, and special characters. Further, users need to change their passwords per every 30 days to perfection system security. In addition, users should enable multi-factor authentications to their user accounts in healthcare. [11]

6) Conduct regular risk assessments:

A risk assessment is a process to identify potential hazards and analyse what could happen if a hazard occurs. These risk assessments are helpful to organizations to identify risks before it comes. [15]

7) Hire Cyber security professionals:

Cyber security professionals have more experiences and knowledge about security domain. So, they can use to do risk assessments and penetration testing to identify risks, threats and vulnerabilities in systems.

8) Maintain cloud backups:

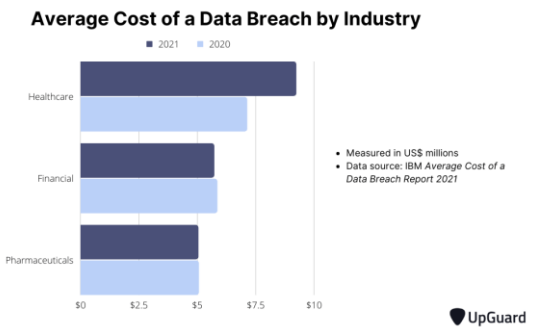
Maintaining backups is important thing to healthcare organizations. Because when ransomware attack happens, they can easily restore their data from backups without paying ransom.

9) Implement Zero-Trust Architecture (ZTA)

Everything must be verified before being permitted to connect to a system, according to zero-trust security models. Zero-trust models assess the security of an access request using techniques like multi-factor authentication, encryption, and analytics in order to take into consideration an open structure. Even then, zero-trust models only give access that is absolutely necessary to complete the task at hand. [16]

E. Security Laws, regulations and standards related to Healthcare

Healthcare incurred the greatest overall average data breach cost of any sector in 2021, totaling US$9.23 million. Furthermore, 2021 was the second-highest year for records that were breached, with 44,993,618 health records being stolen or disclosed. [17]



Healthcare is most critical industry therefore healthcare industry has many laws and regulations to secure.

1) **National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure.**

This regulation has set of organizational guidelines to mitigate from attacks. Healthcare organizations in any country can adopt to NIST framework. [18]

2) **Appoint An Information Security Officer.**

An information security officer is very important person to healthcare organizations. In Sri Lanka, there is a regulation about an information security officer. As mentioned in it, it is crucial to designate a responsible officer for information security who can take the initiative and responsibility for the institution's health information security. In addition, this person should be held accountable to the administration for decisions made regarding information security programs, the implementation of security controls, risk and incident management, and the execution of awareness campaigns in accordance with the Health Information Security and Privacy Act. [19]

3) **Center for Internet Security (CIS) Critical Security Controls**

The Critical Security Controls were created by CIS to defend both public and private entities against online threats. This has 18 controls to organizations. This is not a mandatory requirement to implement these controls, but these controls increase organizations security. [18]

- Inventory and Control of Enterprise Assets
- Inventory and Control of Software Assets
- Data Protection
- Secure Configuration of Enterprise Assets and Software
- Account Management
- Access Control Management
- Continuous Vulnerability Management
- Audit Log Management
- Email Web Browser and Protections
- Malware Defenses
- Data Recovery
- Network Infrastructure Management
- Network Monitoring and Defense
- Security Awareness and Skills Training
- Service Provider Management
- Application Software Security
- Incident Response Management
- Penetration Testing

4) **Control Objectives for Information and Related Technology (COBIT)**

This IT governance and control developed by the Information Systems Audit and Control Association (ISACA). COBIT has six policies and COBIT is globally recognized framework. [18]

- Provide Stakeholder Value
- Holistic Approach
- Dynamic Governance System
- Governance Distinct from Management
- Tailored to Enterprise Needs
- End-to-End Governance System

5) **ISO/IEC 27001**

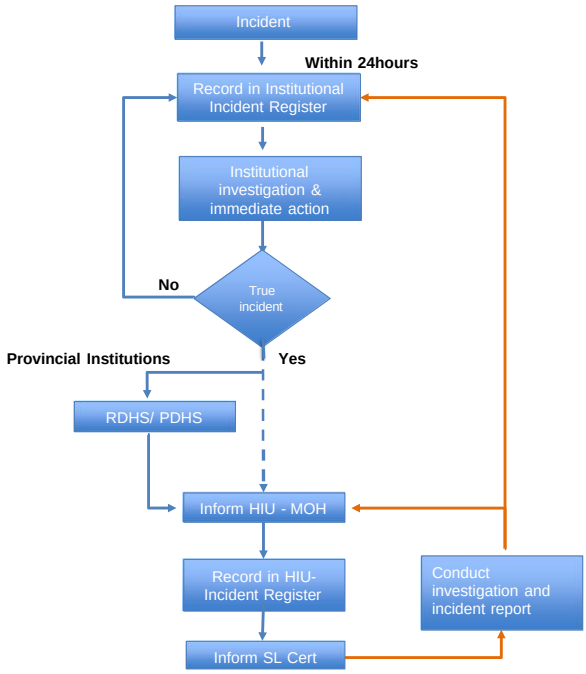
Most of the organizations use ISO 27001 standard to their organizations in modern world. Because this is very popular standard. The implementation of ISO 27001 is a successful strategy for healthcare businesses to regulate, manage, and handle sensitive data, such as patient information. [18]

6) **Payment Card Industry Data Security Standards (PCI DSS)**

This standard uses to ensure payment cards security. Today, most of the healthcare organizations allow users to pay via digital payment cards. [18]

7) **Information Security Incident Management**

According to Ministry of Health in Sri Lanka, there is a process to manage incident in healthcare section. Following graph shows the process. [19]



8) Third-Party Security Management

Most of the security threats to healthcare come from third-party. In Sri Lankan health organizations signed a Non-Disclosure Agreement (NDA) before deal. This NDA documents should have following requirements. [19]

- Clear explanation of the rights of the supplier.
- Levels and constraints on access.
- Legal obligations and the protection of confidential information.
- prevent unlawful copying, sharing, or storage of information.

Further, this security management mentions these things.

- All normal maintenance tasks and specific breakdown repairs should be entered into a registry along with the technician's contact information.
- All personally identifiable information should be removed or destroyed (where possible) with a backup if physical devices need to be removed from the institution's premises.
- Removing the established connections, such as user accounts with third-party software after their service is complete, and properly disposing of the uninstalled hardware components. [19]

Sri Lanka has information security related acts. Healthcare section can adopt those acts as well. [20]

- Electronic Transactions Act No. 19 of 2006.
- Payment devices frauds Act No. 30 of 2006.
- The Intellectual property rights Act.
- Computer crimes Act No. 24 of 2007.

7. *FUTURE DEVELOPMENT AREAS IN HEALTHCARE SECTION SECURITY.*

Healthcare industry security should be tied in future. Otherwise, attackers will try new methods to launch attacks to healthcare section.

1. Use right technology

There are systems and endpoint IOT devices in healthcare. So, these things need to implement right technology. This will increase healthcare section security. [21]

2. Prioritizing threat intelligence sharing:

Each institution in the healthcare system is dependent on and impacted by the others. The creation of a centralized platform for exchanging threat intelligence need to be a top priority.

3. Fostering a culture best practice for security.

If users have enough best security practices, then attackers not able to any vulnerabilities in system. So, organizations need to make security practices as a culture.

4. Invest more money for security.

Investing money for security is not a wasting thing. Because the loss money from cyber-attacks is higher than investing money. So, health organizations can hire security professionals and implement framework like ISO 27001 and install antivirus software's to the system. This will give better security for organizations.

5. Be updated about the new cyber-attack methodology.

In future, Attackers will find new methodology to launch attacks. So, organizations need to aware about these thing and strength security.

8. CONCLUTION

Healthcare section is very critical service to people in world. Because health is very important thing to us. Today, most of the healthcare organizations like hospitals use IOT systems to treat their patients well. Therefore, these IOT devices aim to cyber-attacks because of criticality. In this review paper, first discusses about the security important of healthcare section and then shows what are the IOT devices that use. Next, Healthcare section has security failures and weakness like lack of strong security policies, endpoint leakage, user authentication etc. These security failures and weaknesses need to have mitigation and prevention methods to secure healthcare section. Then there are multiple cyber-attacks like phishing, malware, ransomware, data breaches, and dos attacks. Therefore, next discusses about mitigation and prevention methods like, cybersecurity awareness, implement proper access control, implement antivirus software etc.

Organizations can implement security frameworks like ISO 27001, CIS, COBIT to increase security strength. And also, healthcare organizations security has laws in Sri Lanka and World. These laws and frameworks also discuss in this

review paper. Finally, Healthcare sections need to develop their security in future. So, those future development areas discuss lastly.

9. ACKNOWLEDGMENT

A special thank goes to our lecturer of the Applied Information Assurance Mr. Kanishka Yapa whom gave knowledge, guidance and motivated me to do this review paper.

10. REFERENCES

[1] Mikel, "How IoT is Transforming into the Healthcare Industry?," ConstultingWhiz, 23 03 2021. [Online]. Available: https://www.consultingwhiz.com/blog/iot-transformation-in-healthcare/#:~:text=In%20general%2C%20IoT%20powered%20devices%20interact%20with%20the,health%20conditions%20and%20send%20to%20the%20functioned%20devices.. [Accessed 20 09 2022].

[2] "What is Cyber Security?," Kaspersky, [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Accessed 20 09 2022].

[3] R. Roy, "What Is a Cyber Threat? Definition, Types, Hunting, Best Practices, and Examples," Spiceworks, 23 08 2021. [Online]. Available: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cyber-threat/#:~:text=A%20cyber%20threat%20or%20cybersecurity%20threat%20is%20defined,denial%20of%20service%2C%20and%20numerous%20other%20attack%20vectors.. [Accessed 20 09 2022].

[4] A. VAGHELA, "Importance of Cybersecurity in Healthcare and Medical Devices," Einfochips, 06 10 2021. [Online]. Available: https://www.einfochips.com/blog/importance-of-cybersecurity-in-healthcare-and-medical-devices/. [Accessed 20 09 2022].

[5] H. Caspi, "Healthcare its own enemy in attracting 88% of U.S. ransomware attacks," Healthcaredive, 09 09 2016. [Online]. Available: https://www.healthcaredive.com/news/healthcare-its-own-enemy-in-attracting-88-of-us-ransomware-attacks/425990/. [Accessed 20 09 2022].

[6] P. I. LLC, "Sixth Annual Patient Privacy & Data Security Report," 05 2016. [Online]. Available: https://lpa.idexpertscorp.com/acton/attachment/6200/f-04aa/1/-/-/-/-/Resources%20-%20Sixth%20Annual%20Benchmark%20Study%20on%20Privacy%20and%20Security%20of%20Healthcare%20Data%20.pdf?cm_mmc=Act-On%20Software-_-email-_-ID%20Experts%20Download%20-%20Sixth%. [Accessed 20 09 2022].

[7] U. D. o. H. a. H. Services, "Cases Currently Under Investigation," [Online]. Available: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. [Accessed 20 09 2022].

[8] S. A. "Most Common Security Weaknesses in Healthcare Identified," journal, HIPPA, 28 12 2018. [Online]. Available: https://www.hipaajournal.com/most-common-security-weaknesses-in-healthcare/#:~:text=The%20most%20common%20security%20weaknesses%20in%20healthcare%20were,that%20users%20should%20have%20to%20an%20organization%E2%80%99s%20resources.. [Accessed 21 09 2022].

[9] A. Meola, "IoT Healthcare in 2022: Companies, medical devices, and use cases," InsiderIntelligent, 15 04 2022. [Online]. Available: https://www.insiderintelligence.com/insights/iot-healthcare/. [Accessed 20 09 2022].

[10] J. McKeon, "Why Endpoint Security is Critical For Healthcare Cybersecurity," HealthITSecurity, [Online]. Available: https://healthitsecurity.com/features/why-endpoint-security-in-healthcare-is-critical-for-cybersecurity. [Accessed 21 09 2022].

[11] M. UNIVERSITY, "4 Healthcare Cybersecurity Challenges," 21 09 2022.

[12] H. Shah, "Top 10 Cybersecurity Challenges in the Healthcare Industry," GlobalSign, 05 05 2022. [Online]. Available: https://www.globalsign.com/en/blog/10-cybersecurity-challenges-healthcare. [Accessed 22 09 2022].

[13] E. Kost, "Biggest Cyber Threats in Healthcare (Updated for 2022)," UpGuard, 08 08 2022. [Online]. Available: https://www.upguard.com/blog/biggest-cyber-threats-in-healthcare. [Accessed 23 09 2022].

[14] Cloudflare, "What is a DDoS attack?," Cloudflare, [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. [Accessed 22 09 2022].

[15] "Risk Assessment," Ready, [Online]. Available: https://www.ready.gov/risk-assessment. [Accessed 22 09 2022].

[16] T. Baker, "Zero Trust Architecture for Healthcare – 7 Common Pitfalls to Avoid," BLOG, 07 04 2022. [Online]. Available: https://www.forescout.com/blog/zero-trust-architecture-for-healthcare-7-common-pitfalls-to-avoid/. [Accessed 22 09 2022].

[17] "What is Health Care Security Law?," Winston & Strawn LLP, [Online]. Available: https://www.winston.com/en/legal-glossary/health-care-security.html. [Accessed 23 09 2022].

[18] C. Chipeta, "Top 8 Healthcare Cybersecurity Regulations and Frameworks," UpGuard, 15 04 2022. [Online]. Available: https://www.upguard.com/blog/cybersecurity-regulations-and-frameworks-healthcare. [Accessed 23 09 2022].

[19] S. L. Ministry of Health, "Information Security Guidlines for Healthcare Institute," 01 2021. [Online]. Available: http://www.health.gov.lk/moh_final/english/public/elfinder/files/images/2021/information%20security%20gudeline_1.0.pdf. [Accessed 23 09 2022].

[20] W. R. Yasas, "LAWS IN SRI LANKA TO PREVENT CYBER-ATTCKS," SSRN, University of Plymouth, 2020.

[21] P. Jones, "Modern Security for Future Healthcare," Microsoft, 22 09 2022. [Online]. Available: https://news.microsoft.com/en-ca/2022/09/22/modern-security-for-future-healthcare/. [Accessed 22 09 2022].

10. AUTHOR PROFILE

Madhusanka D.N.V

IT20613518

Cyber Security Researcher

3rd year Undergraduate at SLIIT