Critical Infrastructure Security in the Healthcare Sector

Jaliya Amarakon Dissanayake
IT19991290
Department of Cyber Security
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
adjaliya9747@gmail.com

***Abstract*— Historically, the fundamental objective of sensitivity The purpose of infrastructure security has been to protect against environmental dangers. However, the increase in cyber-attacks has altered the emphasis — infrastructures now confront an entirely new set of challenges. A collection of dangers. A risk that poses a threat to life repercussions and the possibility of serious injury Economic losses. Typical defensive methods Clearly, they are incapable of keeping up with new and emerging dangers. Technologies for infrastructure protection Innovative and flexible individuals are required. This document investigates susceptible facilities and the dangers they pose, developing dangers and current and future threats strategies for infrastructure management. They are unable to keep up with the amount of new and emerging dangers. Technologies for infrastructure protection Innovative and flexible individuals are required. This document investigates highly sensitive facilities and the dangers they pose, developing dangers and current and prospective threats strategies for infrastructure management.**

Keywords— Critical Healthcare, Healthcare in cyber Security

1. Introduction

Over the last decade, cybercrime has posed the greatest danger to every sector on the planet. Because of its essential and vulnerable infrastructure, the health industry is an obvious target for hackers. Additionally, because healthcare organizations are highly regarded and handle sensitive personal information, exploiting their weaknesses may result in substantial financial and political rewards.

Numerous compliance difficulties occur as a result of the needs of the healthcare business. It is critical to secure data without risking the provision of essential healthcare services.

Growing interconnectivity introduces new dangers to the hospital's physical and cyberinfrastructure, which must be considered to protect the patient's welfare. Additionally, legal regulations like the GDPR in Europe must be addressed to ensure patient data protection and compliance with applicable laws.

In order to understand the risk that healthcare institutions may experience, it is essential to be aware of past security problems. It is also important to know which critical assets are present and how they impact system availability.

Then scenarios will be created and built to assist in identifying hazards that a security solution for a healthcare institution might address. The examples may control a combination of physical and cyber dangers in cascading assaults since these are the most complex and exciting problems to deal with.

2. Research Objectives

Challenges in Healthcare Sector

Standard perimeter security measures and proactive and predictive cybersecurity technology are now installed in healthcare institutions. With these cybersecurity measures, the odds of a successful attack on sensitive infrastructure (such as major IT systems, HIS hospital information systems, PACS image archiving and contact systems, LIS laboratory information systems, and other vertical software for ERED) remain low in place.

There is no other method to penetrate the perimeter defenses, even if it requires a physical assault. It is critical to connecting directly to servers and network components that are not accessible from the outside. Obtaining access via abuse, extortion, or other deceitful methods may only be regarded as a side consequence of a cyberattack in this scenario.

It is well understood that hospitals and healthcare facilities cannot function properly without IT systems, particularly the PACS and LIS, which make dealing with radiological images and laboratory testing incredibly difficult, making diagnosis and, as a result, patient treatment difficult or extremely slow. For assault injury, this may be thought of as a "multiplier effect."

Consequently, in the event of a terrorist attack and the subsequent massive influx of wounded victims, it's essential to plan for possible assaults on hospital IT infrastructure to limit hospital operational capacity and absorb patients in the emergency department. As a consequence, dangers cannot be divided into two categories: physical and electronic. It is critical to adopt an adaptable approach to fight such a varied collection of problems.

The HPH industry is broad and varied. The industry employs about 13 million people and accounts for 16.2% ($2.2 trillion) of the nation's GDP (GDP). It encompasses acute care hospitals and ambulatory healthcare and the large and complicated public-private financing structures that support such services. It includes federal, state, local, national, and territorial health authorities' population-based health services and other public health and disease monitoring responsibilities. It is made up of an extensive network of private firms that import, distribute, and market medications, vaccines, medical supplies, and facilities and a network of small businesses that provide funeral services. Many of these goods and services are provided in

and across various scientific, legislative, banking, and government policy environments.

All dangers will become less of a threat to the HPH Sector. Which would safeguard or minimize the interruption or loss of the nation's hospitals and public health system.

It will strive to safeguard its workers and preserve its ability to react swiftly and efficiently (without disrupting service in unaffected regions) and recover from normal and emergency circumstances.

The HPH Sector has the mission to promote successful emergency preparedness and response to significant national dangers with the implementation of policies, threats evaluation, planning, and policy guidance, as well as guidance on preparing, defending, preventing, and responding to important national dangers through the implementation of strategies, risk assessments, planning, and policy advice. Respond as needed to assaults the nation's infrastructure and encourage infrastructure stability to recover and restore healthcare and public health services.

The HPH Sector has established four objectives in the areas of operation continuity, worker safety, physical infrastructure protection, and cybersecurity:

1. Maintain the ability to provide essential health care before and after supply or supporting service disruptions (e.g., water, electricity);

2. Workforce Protection• —Protect the sector's workforce from the negative effects of any risks that could jeopardize their health and welfare or limit their ability to perform their duties;

3. Physical Infrastructure Protection• —Reduce the risk of any hazards to the sector's physical assets; and

4. Cybersecurity• —Reduce the risk of interruption or denial of health care to the sector's workforce.

3. Review of the literature

Threats are actions that have the potential to harm an organization's critical capital. Threats often use system vulnerabilities, i.e., they exploit weaknesses in the system to produce an undesired outcome, such as asset damage or loss. It is critical to identify the possible root causes of assaults to guarantee the infrastructure's stability. According to ENISA [36], healthcare companies confront five main kinds of risks:

Malicious activities are deliberate actions performed by an internal or external entity or entity to kill, steal, or disrupt data or a device. Malicious actions include malware (e.g., viruses, ransomware), hijacking, social engineering, tampering with medical equipment, and device and data theft.

Human errors result from improper method execution, misconfiguration, or inappropriate usage of computers and information systems.

Failures in the system

Failures in the supply chain: These are the fault of third-party suppliers such as electricity providers, medical device makers, and so on.

Natural phenomena:- The person or organization in charge of carrying out these threats (threat actor) may also be classified based on their function:

Insider threat actor: This category includes medical professionals (physicians, nurses, support staff, and so forth).

Patients and visitors who are malicious

Remote attackers are actors who are not physically present in the facility.

Scenario Example 1: Cyber-physical Attack on Medical Devices

Medical equipment is an essential component of the healthcare system. They enhance patients' quality of life, but they also offer a problem due to increasing hospital access. In recent years, many medical device assaults have been recorded. Security researchers, for example, showed in 2018 that they had found security vulnerabilities in Medtronic pacemakers, exposing the lifesaving device to hackers and putting patients in danger.

An attacker may acquire physical or remote access to a medical system and then employ reverse engineering to discover and exploit a vulnerability to change patient outcomes or profit financially. The intruder will next use the medical device's vulnerability to modify its software and/or disrupt healthcare services, potentially causing damage to patients and employees. In this case, the medical equipment system is changed, or a denial of service attack is launched to disrupt the health system while scanned for vulnerabilities.

The invader may potentially steal the PC. Consequently, the medical device will be revealed, changed, or disrupted, putting patients and workers in danger.

This attack has a high probability of success.

Buildings and Facilities, such as an engineering room; Identification Systems, such as a badge (physical) or credentials (cyber); Networked Medical Devices, such as Wearable Medical IoT; Networking Equipment, such as a router; Interconnected Clinical Information Systems, such as PACS, for example; and documents and archives, such as patient information.

Security Challenges for CIs of the Healthcare Sector

To mitigate the effect of this assault, the following measures should be considered: • Implement access restrictions for vendor support personnel.

- Implement device security operations processes.
- Establish and maintain communication with the security departments of suppliers.
- Design and implement authentication mechanisms for a computer network.

Scenario Example 2: Cyber-physical Attack to Cause a Hardware Fault

The interruption of healthcare institutions' services, like that of any other critical infrastructure, has a significant impact on patients. Attackers may take advantage of this function of hospitals for financial gain, notoriety, or other reasons.

Targets for this kind of assault include extortion, sabotage, and even intimidation. Consequently, the offender is solely concerned with creating system downtime and inflicting permanent (or temporary) system damage and is indifferent about whether or not the patient is in danger.

Using social engineering, the criminal may learn about the hospital's facilities. He or she might use this knowledge to exploit a vulnerability in the system, get administrator privileges, and cause a hardware breakdown.

Because the support systems cannot operate properly due to hardware issues, the healthcare system's unavailability may result in patient death or severe damage.

Some of the characteristics affected in this scenario include networked medical instruments, such as medical devices that link with a central system, and networking equipment, such as an electronically accessible computer.

Clinical Information Systems in Relationship.

It is essential to highlight that this attack might have been prevented at least partly if: • An effective intrusion detection device had been installed to identify the assault early; the number 162

• Is there an endpoint authentication method that prevents unrecognized devices from being attached to CIs in the healthcare sector apparatuses?

• The employees have been trained to identify odd behavior and recognize the risk. Never open attachments in emails from unknown senders.

• Devices have been modified since the patches were tested and distributed by the medical device manufacturer;

• Privileged access control tools have been deployed to report access to sensitive infrastructures. Furthermore,

• Astringent and limited access control program for clinical and vendor support personnel has been implemented.

Assess Risks

This chapter explains the methodology of the HPH Sector to risk evaluation. It covers the danger and impact assessment in the industry and offers information on specific tools for risk mitigation.

Use of Risk Assessment in the Sector

In the HPH Sector, the bulk of risk assessments are performed to guarantee that protection, physical security, and information security laws are followed. Listed below are a few examples:

• Hospitals must conduct risk assessments to comply with state regulations and obtain the certification needed for reimbursement under the Federal Medicare program.

• To guarantee that their medicines are safe and effective, pharmaceutical firms conduct risk assessments.

• Sector health plans, hospital insurers, and healthcare clearinghouses evaluate risks to systems that hold health data and guarantee compliance with protection and privacy requirements under the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

• As part of their review and certification process, federal partners conduct risk assessments to comply with the Federal Information Security Management Act (FISMA) of 2002.

Companies in the HPH Sector have a strong interest in conducting risk assessments to identify variables that may result in negative financial and reputational consequences, in addition to complying with regulatory obligations. The SSA will aid industry players in this process by identifying and sharing risk management resources.

Assessing Vulnerabilities and Consequences

The HPH Sector uses a range of methods and procedures to assess vulnerabilities and impacts.

The risk and impact assessment methods of the SSA, SCC, and GCC collaboration are detailed in this section.

Strategic Homeland Infrastructure Risk Analysis.

The Strategic Homeland Infrastructure Risk Analysis (SHIRA), which offers a broad framework for sectors to evaluate the economic, human-life, and psychological effects of terrorist activities, is led by the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC).

Over time, the model has developed to incorporate both environmental and domestic risks, enabling businesses to describe their susceptibility to and impacts from all hazards.

Using the SHIRA methodology, the RAWG creates models of real-world scenarios that may impact critical sector systems, including patient management and the medical supply chain on behalf of the HPH Sector. The RAWG has created models of the chemical, electronic, vehicle-borne explosive device and insider threats and their limits and consequences. The research favors high-impact events with a high likelihood of occurring. Processing factories, medical supply distribution facilities, and cyber networks are possible targets for biological select agents and poisons. Researchers in the area may use the data collected to look at dynamic cascade impacts on the economy, human life, and psychological well-being.

The data supplied by the SHIRA process informs other CIP-related activities, such as the implementation of capacity gap statements for R&D expenditures and the development of crucial infrastructure needs for the NCIPP. SHIRA may be utilized to guide security and consequence avoidance choices and improve project performance overall.

Network Analysis

The HPH CIP software is doing a network analysis of the industry to better understand business risk. This approach analyses sector interdependencies, external dependencies, and critical nodes using the sector's functional model. The approach identifies faults and potential areas of vulnerability, enabling the industry to evaluate and enhance risk management strategies based on the consequences of a function's failure. By incorporating modeling and simulation of various scenarios at the state, provincial, and local levels, the sector will create contingency plans, improve protection programs, guide resource utilization, and detect resource deficiencies in emergency management, rehabilitation, health monitoring, and care delivery.

Healthcare Facility Risk and Design Analysis Tool

Building owners and builders may utilize the HPH Sector's security and architectural consultation platform for healthcare facilities. In order to have the most significant security and medical surge configuration options, the tool evaluates a facility's security threats based on its venue, natural dangers, and service types.

Among other things, the tool asks questions regarding facility qualities, danger characteristics, previous risk assessments, and protection and security measures.

The program collects and synthesizes the responses to produce a facility's overall risk score. As the tool evolves, each issue will be linked to a set of mitigation actions recommended for inclusion in the facility's construction or renovation. Owners, managers, and architects would utilize the study's results to assist them in making design choices at the outset of a project. The benefits of integrating security into the design process of a facility include lower purchasing and integration costs, improved patient and staff safety during surges, and enhanced organizational sustainability during an all-hazards event.

Cybersecurity Risk Assessment

The HPH Industry established the CSWG to develop a cybersecurity strategy for the industry. The initiative has received support from the vendor group, cross-sector cyber experts, and owners and operators.

The Cyber Security Working Group (CSWG) has developed a system classifying cyber risks based on infrastructure functioning, data integrity, confidentiality, and privacy. The CSWG looked at threats, risks, impacts, cascade repercussions, and mitigation strategies in these hazard categories.

Current Threat Scenarios Facing the Health Care Industry

This section will go through some of the most recent cybersecurity threats and vulnerabilities impacting the healthcare sector. Cyber-attack visibility is divided into two types: threats and vulnerabilities. Why is it important to understand the difference between the two? The ability to distinguish between the two assists in deciding which cybersecurity procedures and technologies are necessary and appropriate for the business to reduce the risk of damage caused by an invader or an unskilled but authorized individual.

Explaining Threats and Vulnerabilities

Threats and vulnerabilities are connected but not the same. Internal or external threats are acts or events that have the potential to degrade the quality, performance, or profitability of your company.

Natural or artificial, purposeful or accidental, internal or external dangers may exist. Consider the power disruptions that storms and floods have caused. Examples include external, natural, and accidental hazards. Danger may also be a person, such as a present employee, who attempts to steal data or harm your company.

A threat is anything or anybody who has the potential to harm anything valued.

Take, for example, the influenza virus, which is well-known among medical experts. Almost everyone who is infected with the flu will die. An individual's sensitivity to it influences the severity of the virus. Most people would believe that an older person is more vulnerable to the flu's symptoms when compared to a collegiate athlete. What is it about the elderly that makes them more prone to attack?

Vulnerabilities are defects in a system that cause harm and, ultimately, destruction if exposed to danger. A danger will often take advantage of a vulnerability.

Based on the example above, most people will think that an older person is more vulnerable to the flu than a college athlete. The reduced function of an aging immune system, physical frailty, and even impaired mental capabilities, all of which appear in an inability to follow a suggested treatment plan, are all factors that contribute to this increased risk. Aside from these factors, not getting a flu vaccine may make an older person more susceptible to harm.

Threats to the Health-Care Industry: An Overview

Five of the most current and prevalent cyber-threats to healthcare companies are discussed in the following section. The hospital image on the next page depicts the five most recent cybersecurity challenges:

Phishing through email is the first kind of assault.

2. An assault using ransomware

4. Insider, unintentional or deliberate data loss 3. Loss or theft of equipment or data

5. Cyber-attacks on linked medical equipment that may jeopardize patient safety

Each hazard shown in the image is meant to show how these risks may affect organizations in various hospital sections and in different health care environments. Cyber-attacks may come from anywhere and at any moment.

1. **Phishing through email**

Phishing via email is an effort to trick you, a coworker, or someone else at work into divulging personal information via email. An inbound phishing email includes an active connection or file (typically an image or graphic). The email seems to come from a reliable source, such as a friend, colleague, employer, company, or even the user's email account. By clicking to open the connection or file, the user is routed to a website that may collect personal information or aggressively damage the device. You risk downloading harmful software or getting access to information stored on your device or other devices in your network by clicking on the link or downloading the file.

The scenario in the Real World: A phishing email is sent to your workers by a cyber-attacker masquerading as an IT support representative from your patient billing company. Your employees are told to update their billing program codes by clicking on a link in the email. When an employee opens the link, they are directed to a fake login page, which collects and transmits their login details to the attackers. Using the employee's login credentials, the attacker accesses the organization's financial and medical data.

Impact: According to a doctor, an attacker launched a phishing assault to obtain patient data, subsequently utilized in an identity theft crime.

2. Ransomware Infection

The HHS Ransomware Factsheet, which can be accessed at https://www.hhs.gov/sites/default/files/RansomwareFact Sheet.pdf, describes ransomware as follows: “Ransomware is a kind of ransomware used to extort money from its victims.

Malware (harmful software) is a kind of malicious software that is not like the others. It differs from other viruses in that it attempts to infect other machines. Deny access to a user's data, usually by encrypting it with a key that can only be recognized by the hacker who installed it. The virus will stay active if a ransom is paid. When a file is locked using the user's details, ransomware urges the victim to pay a ransom. Ransom payment (typically in the form of a cryptocurrency, such as Bitcoin) to the hacker. You must first spend Bitcoin in order to acquire a decryption key.

Hackers, on the other hand, may employ ransomware alone or in conjunction with other software to encrypt or exfiltrate files." Paying a ransom does not guarantee that the culprit will be able to decode or unlock the data that has been compromised. Other threats may employ methods or procedures similar to or identical to those used by ransomware assaults. For example, successful phishing attempts may lead to the installation of ransomware.

Real-World Scenario: An email that seems to have originated from a credit card provider leads a user to a fake website and convinces them to install a security update. The alleged security update is malicious software that looks for and encrypts data, rendering it inaccessible. The user is then told that to decrypt or unencrypt the data, he or she must pay a ransom.

Impact: Due to a ransomware assault that has rendered the EHR system unavailable, a practitioner cannot see patient records.

3. Equipment or data loss or theft

Every day, laptops, tablets, cellphones, and USB/thumb drives go stolen or are hacked, ending up in the hands of hackers.

Theft of equipment and data is a constant and growing threat to all companies. From January 1 to August 31, 2018, the Office for Civil Rights published reports of 192 fraud occurrences affecting 2,041,668 individuals.

Although the system's value is based on a single failure, the consequences of deleting a device that contains sensitive data are much more severe. Unwanted or illegal access, dissemination, and use of sensitive data may result from losing a computer that was not adequately secured or password protected. Furthermore, even if the computer is discovered, the data on it may have been permanently erased. Data loss or malicious usage may disrupt business and endanger patient safety, requiring notification of customers, regulatory agencies, and the media.

Real-Life Scenario: A surgeon goes to a coffee shop for a coffee cup and uses public Wi-Fi to scan radiology data. As the physician moves away from the table to fetch his coffee, an intruder steals the laptop. The laptop has gone by the time the doctor arrives at the bench.

Impact: The loss of personal papers may lead to patient identity fraud. With thousands of data potentially destroyed, the physician's credibility could be compromised if any medical records are sold on the dark web.

4. Data Loss: Insider, Accidental, or Intentional

Insider hazards exist when employees, suppliers, or other customers gain access to the organization's technological systems, network, or databases. Insider assaults may be deliberate or accidental.

An unexpected insider threat is caused by unintentional harm caused by benign mishaps, such as being misled, technological weaknesses, or a degree of ineptitude.

Being the victim of a phishing attack through email, for example, is an unintended insider threat. A purposeful insider threat is a fraud or failure performed for personal benefit or to cause harm to the company or another entity by an employee, contractor, or another user of the organization's technological system, network, or databases.

The scenario in the Real World: An intruder pretends as a representative from a physical therapy institution and requests that a hospital staff verifies patient information. The impostor gets the whole patient's medical record by impersonating a member of the medical team.

Impact: The patient's personal information was taken and utilized in an identity theft scheme.

5. Cyber-Attacks on Connected Medical Devices that may jeopardize patient safety

The Food and Drug Administration (FDA) defines a medical device as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory that is recognised in the official National Formulary, the United States Pharmacopoeia, or any supplement to them; intended for use in the diagnosis, treatment, or prevention of disease."

The scenario in the Real World:

A cyber attacker gains access to a care provider's computer network and takes command of a file server to which a cardiac monitor is connected through an email phishing assault. When scanning the network for equipment, the intruder takes control (e.g., power off, continuously reboot) of all cardiac monitors in the ICU, putting numerous patients in danger.

Impact:

Patients are in severe danger when a heart attack disables cardiac monitoring, placing them at risk during surgery and other procedures.

4. Future research:

This study showed the complexity of the worldwide threat environment by evaluating the most significant hazard and risk to the HPH market. The effect of ransomware on the HPH industry revealed the sector's susceptibility.

Its present predicament stems from a scarcity of high-quality required postures and, consequently, a lack of execution of such postures. As a consequence, it is recommended that the HPH sector collaborates with lawmakers to create higher-quality prescribed postures for the industry and that such postures be implemented to guarantee consistency across the board.

HHS must work with politicians to modify and create higher-quality requirements that enhance the healthcare system's cybersecurity and resilience.

Because the threat environment is continuously changing, policymakers must account for the time it takes to evaluate mandates daily to ensure that they stay relevant. In addition, HHS and lawmakers must consider creating proactive solutions to the HPH sector's cybersecurity problems.

Adopting a cybersecurity framework for the HPH market, or creating a customized platform, would aid providers in fulfilling the updated quality enforcement requirements of constructive solutions.

HHS and policymakers must collaborate closely to address the HPH sector's current weakness and establish improvement targets. The HPH industry should strive for the Adaptive Level of cybersecurity and risk management, using the NIST model as a reference. As the SSA, HHS must start by establishing a framework and supporting providers in carrying it out and enforcing these rules.

This research emphasized the absence of law enforcement during cybersecurity incidents. Because law enforcement cannot react until after an attack has occurred, they must become more alert to minimize the danger of an assault. Consequently, it is suggested that HHS and legislators utilize requirements to incentivize law enforcement and regulatory agencies to implement positive cybersecurity measures.

The CENC recommends that the government handle cybersecurity, and industry leaders urge to create a body whose primary purpose is to supervise cybersecurity. On the other hand, this research showed the high cost of this option by examining the growth of DHS. Nonetheless, regulatory and monitoring agencies capable of implementing these proactive requirements remain in place.

The expansion of these organizations will save the HPH sector money on establishing and operating a new agency.

This research discovered a high-performing company with the capability to carry out these constructive activities. It is recommended that the LA MFCU put this concept to the test by including a cybersecurity enforcement component into its computer forensics department. The LA MFCU should also work with the LDH/DHH and HHS to revise the Medicaid provider arrangement contract to include proactive quality assurance testing of new cybersecurity requirements. If the additions are excellent, Barbara Zellner of NAMFCU should work with HSS to make them mandatory for all MFCUs in the United States.

The HPH sector may get closer to achieving an Adaptive Level of cybersecurity by implementing better quality requirements, establishing a cybersecurity strategy, and constructively enforcing

these postures. This suggested change would also assist the HPH sector in becoming more stable and robust, resulting in a more secure and resilient national infrastructure and fulfilling PPD-21's mandate.

Because of the limitations of this article, further research on the risks of fragile medical equipment in the HPH area is required. Senators Bill Cassidy (R-LA) and Sheldon Whitehouse (D-RI) proposed the Transparent Ratings on Usability and Security to Transform Information Technology (TRUST IT) Act of 2015 in October 2015. TRUST IT requires the ONC to provide a methodology for assessing product security, usability, and interoperability" (ICIT, 2016, p. 69). The TRUST IT Act requires medication ratings and availability on the ONC website. Sen is also questioned in this research.

Senators Cassidy and Whitehouse are considering the implementation of an HPH provider rating system. Like how the Health Department evaluates restaurants, providers should be graded yearly based on their cybersecurity and risk management infrastructure. This rating system would boost trust in the safety and security of patient data.

5. Conclusion

For criminals, healthcare institutions are a profitable target. The growing convergence of cyber and physical networks and linked devices in its ecosystem presents new security problems for these businesses. To meet the difficulties of the healthcare technology era, hospitals must integrate cyber and physical safeguards, minimizing the risks that may harm patients, property, and the environment.

This chapter has covered the most critical security problems in the healthcare ecosystem, not only from structural management but also from a legal perspective. A study of previous security incidents was performed to explain the vulnerabilities targeted by criminals in the health industry. As a consequence of this research, five main categories of risks and classification of essential assets were established. Finally, the EBIOS method identifies two hybrid cyber and physical vulnerability models, which are briefly explained. All of this information may assist the reader in comprehending and being aware of the security issues that healthcare facilities confront in this smart hospital era.

6. Appendix

Acronym/ Abbreviation	Definition
HPH	Health Care and Public Health
HHS	Department of Health and Human Service
ONS	Office for National Statistics
SSA	The United States Social Security Administration
PHI	Personal Health Information

7. Acknowledgment

First of all, I should like to thank Mr. Kanishka Yepa, a professor at the Informatics Institute in Sri Lanka, for his continuous support throughout my studies and his patience, dedication, enthusiasm, and extensive knowledge. His tips for studying and writing this paper were helpful, and I could not have requested a more delicate teacher and mentor for my graduation.

I owe an outstanding debt of appreciation to my friends in the Sri Lankan Institute of Information Technology cyber security team for inspiring me and helping me to complete this task effectively.

Finally, I would want to thank my family for their spiritual guidance throughout my studies.

References:

[1] *Researchgate.net*. [Online]. Available: https://www.researchgate.net/publication/267391571_A_Survey_of_Critical_Infrastructure_Security. [Accessed: 17-May-2021].

[2] *Researchgate.net*. [Online]. Available: https://www.researchgate.net/publication/224348148_Protection_of_the_Health_Care_and_Public_Health_Critical_Infrastructure_and_Key_Assets_An_Overview. [Accessed: 17-May-2021].

[3] *8.-Security-Challenges-for-the-Critical-Infrastructures-of-the-Healthcare-Sector*. [Online]. Available: http://8.-Security-Challenges-for-the-Critical-Infrastructures-of-the-Healthcare-Sector. [Accessed: 17-May-2021].

[4] U. D. Ani, J. D. McK Watson, J. R. C. Nurse, A. Cook, and C. Maples, "A review of critical infrastructure protection approaches: improving security through responsiveness to the dynamic modelling landscape," in *Living in the Internet of Things (IoT 2019)*, 2019.

[5] E. Izycki *et al.*, "Critical Infrastructure Security," *Academia.edu*. [Online]. Available: https://www.academia.edu/Documents/in/Critical_Infrastructure_Security. [Accessed: 17-May-2021].

[6] A. Silvast, R. Kongsager, T.-K. Lehtonen, M. Lundgren, and M. Virtanen, "Critical infrastructure vulnerability: a research note on adaptation to climate change in the Nordic countries," *Geogr. Tidsskr.*, vol. 00, no. 00, pp. 1–12, 2021.

[7] M. S. Jalali, S. Razak, W. Gordon, E. Perakslis, and S. Madnick, "Health care and cybersecurity: a bibliometric analysis of the literature (Preprint)," *J. Med. Internet Res.*, vol. 21, no. 2, p. e12644, 2018.

[8] A. Sardi, A. Rizzi, E. Sorano, and A. Guerrieri, "Cyber risk in health facilities: A systematic literature review," *sustainability*, vol. 12, no. 17, p. 7002, 2020.

[9] E. Maia *et al.*, "8. Security challenges for the critical infrastructures of the healthcare sector," in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical*

Protection of Modern Critical Infrastructures, Now Publishers, 2020.
[10]
L. Kun, “Protection of the health care and public health critical infrastructure and key assets,” *IEEE Eng. Med. Biol. Mag.*, vol. 27, no. 6, pp. 8–13, 2008.
[11]
“Critical Infrastructure Sectors,” *Cisa.gov*. [Online]. Available: https://www.cisa.gov/critical-infrastructure-sectors. [Accessed: 17-May-2021].
[12]
“Identifying critical infrastructure during COVID-19,” *Cisa.gov*. [Online]. Available: https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19. [Accessed: 17-May-2021].
[13]
Critical Infrastructure, “Public Health & Healthcare,” *Phe.gov*. [Online]. Available: https://www.phe.gov/Preparedness/planning/cip/Documents/healthssp_08_508.pdf. [Accessed: 17-May-2021].
[14]
“Overview of the healthcare sector,” *Sebokwiki.org*. [Online]. Available: https://www.sebokwiki.org/wiki/Overview_of_the_Healthcare_Sector. [Accessed: 17-May-2021].
[15]
“Articles,” *Saludydesastres.info*. [Online]. Available: http://www.saludydesastres.info/index.php?option=com_content&view=category&id=119&lang=en. [Accessed: 17-May-2021].
[16]
“Healthcare Sector,” *Investinganswers.com*. [Online]. Available: https://investinganswers.com/dictionary/h/healthcare-sector. [Accessed: 17-May-2021].
[17]
Abiresearch.com. [Online]. Available: https://www.abiresearch.com/market-research/product/1015806-critical-infrastructure-security-healthcar/. [Accessed: 17-May-2021].
[18]
“Risks of cyber attacks on the healthcare sector leave public health of communities vulnerable - NACCHO,” *Naccho.org*. [Online]. Available: https://www.naccho.org/risks-of-cyber-attacks-on-the-health-care-sector-leave-public-health-of-communities-vulnerable. [Accessed: 17-May-2021].

Author profile

A.D.Jaliya was born in Tangalle, Sothern Province, **Sri Lanka**, in 1997. He is **currently studying** at the Sri Lanka Institute of Information Technology in Malabe. He went to Rajapashe central college weeraketiya. He studies **BSc.(Hons) in Information Technology Specialization in Cyber Security** degree program at SLIIT in Malabe, Sri Lanka.