Critical Infrastructure Security in the Healthcare Sector

Maleesha Rodrigo
Faculty of Computing
Sri Lanka Institue of Information Technology
Malabe, Sri Lanka
maleesharodrigo@gmail.com

Abstract— **The growing importance of technical and operational infrastructure network is accompanied by a significant increase in infrastructure complexity. Extreme accidents caused by natural or man made disasters have a wide range of harmful consequences as lifelines are disrupted. Critical health infrastructures are diverse networks of services, buildings and properties that generate hospitals, nursing homes, home care or pharmacies and are a vital sub sector of the interconnected critical infrastructures system.**

They are of critical importance because their destruction or incapacity will jeopardize the public's stability, economy, fitness, safety or welfare. Failures would have an effect on those especially societal classes with a poor capacity to predict, cope with resist and recover from the impact of a natural or man made danger. Reducing the insecurity of these socioeconomic services reduces a community's total vulnerability

Keywords— critical infrastructure security, critical infrastructure, healthcare, insider threat, systematic review, system, critical infrastructure protection, disclosure, securitization, public health

I. INTRODUCTION

The properties, structures, equipment, networks and other components on which society depends to sustain national security, economic vitality and public health and safety are refereed to as critical infrastructure. Vital infrastructure is recognized as the electricity used in households, the water that drink, the vehicles are used to get around, the shops and the internet and connectivity to rely on to stay in touch with family and friends. In the United States the private sector generally owns and operates this physical and cyber infrastructure while someone is maintained by federal, state or municipal governments. Not all infrastructure within a particular industrial field is vital to a country or territory. It is important to determine which infrastructure is both essential to the continued operation of facilities or functions and vulnerable to some kind of danger or hazard. Prioritizing the distribution of available capital to that subset of infrastructure will improve a country's stability, resiliency and risk management.

Transportation, power. Electricity and communications are designated as lifeline functions which means that their stable activities are so vital that a failure or failure of one of these functions can significantly impact the stability and durability of critical infrastructure within and across multiple sectors. Power investors for instance supply critical power and fuels to stakeholders in the connectivity, transportation and water industries and the energy industry depends on them for fuel distribution (transportation), electricity generation (water for manufacturing and cooling) and infrastructure management and service (communication).

Because if the interactions and interdependence between infrastructure components and sectors the lack of one or more lifeline function/s has an instant effect on the operation or task in different sectors. As a consequence further deterioration of other components can occur over time. Furthermore acknowledging and formally honouring business industries that are lifeline sectors and/or have cross sector interdependence encourages coordination and knowledge sharing which enhances operational and service sustainability. The industries given priority in outreach activities should represent an awareness of the infrastructures' interconnectivity and interdependence consider established business partnerships and agree with the functions and oversight duties of government agencies.

In addition to lifelines critical infrastructure includes tasks. Democratic infrastructure for example was declared a sub sector of the government facilities sector in 2017 due to the importance of free and fair national system as a pillar of the American way of life. Working to minimize risk in collaboration with the governmental and non governmental institutions in charge of delivering this type of vital function is a critical component in preserving public confidence in the nation's strategic infrastructure.

II. THE RESPONSIBLE FOR CRITICAL INFRASTRUCTURE

securing and resiliency of essential infrastructure is a combined effort of stakeholders including crirtical infrastructure owners and users as well as numerous government and non government organizations (including industry associations).

Roles and obligations for sustaining or upgrading infrastructures stability and readiness vary broadly and are influenced by a variety of factors including:

- Public and private ownership
- Industry regulations
- Risks and dangers to a single sector
- Decisions on whether the industry or area can prioritize efforts to protect infrastructure, mitigations effects or react to and rebound quickly from adverse reactions.

Industry associations also play a vital role in suggesting strategies while in other industries, rules may mandate specific measures – or might both apply. Any industries have state wide or national design guidelines in place that help mitigate against disruption caused by disasters such as explosions, flooding and eathquakes. In some industries, insurance companies can enforce protection standards on their policy holders. The chemical industry in the United States for example encourages preparedness through a voluntary arrangement among government and business and is partly subject to legal measures.

Response efforts can be led by emergency stakeholders or provincial and federal funding but accountability for recovery in a largely voluntary environment such as the one in the United States normally falls to the owners and operators who are most familiar with the infrastructure.

Participation at all layers of government and business encourages shared knowledge and trust while also encouraging knowledge sharing as well as practical collaborations. Engagement that facilitate resource prioritization, coordination, drills and preparation both contribute significantly to the effectiveness of national preparedness strategies and in particular successful and timely reactions. Such engagements also help to galvanize support for collaborative public private projects.

III. CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Security can be described as reducing the vulnerability to critical infrastructure through intrusions, threats, or the consequences of natural or man-made disasters using physical or protective cyber controls.

Resilience can be described as the capacity to anticipate and respond to changing circumstances. This includes the ability to survive and rebound quickly from disturbances, intentional assaults, collisions, or occurring naturally hazards or events. Infrastructure that is resilient must also be stable, flexible, as well as flexible.

Collaboration and knowledge exchange are the foundations of a solid essential infrastructure management and resilience program.

Collaboration is encouraged by creating the processes and structures required for government and the private enterprise to freely communicate without releasing confidential data or offering an unfair advantage; supporting a trusted information sharing atmosphere in which stakeholders share information to strengthen security and resilience; and ensuring key stakeholders are properly represented.

To share knowledge effectively, defined processes or networks must meet stakeholders on a daily basis, well before and, after, and after an event. Knowledge exchange can take multiple types, including educational events, briefings, email updates, phone calls, or meetings in safe environments to share sensitive materials about potential risks or dangers, as well as manuals with platforms that facilitate exchange experiences experienced. The latter group enhances readiness for upcoming activities.

To promote joint collaboration and coordination among critical infrastructure sectors and government organizations (central government, regional, city, local, as well as jurisdictional), the United States has established a formal partnership framework comprised of government and private sector coordinating councils that meet separately and jointly to improve critical infrastructure security and resilience. Data Exchange and Analysis Centers are used in the private industry to share information (ISACs). ISACs typically work on an enterprise framework, which means that organisations from a single critical infrastructure field (or a particular division within a field) collaborate to exchange knowledge. While most of these organisations are now important drivers of successful knowledge exchange, others do not fit perfectly into an existing field or have specific needs. There are also business sector Information Sharing and Analysis Organizations in the United States (ISAOs). ISAOs, which were established to collect, interpret, and spread information cyber threat information, provide a more adaptable approach to self-organized data sharing activities within particular groups of stakeholders.

IV. CHALLENGES IN HEALTHCARE SECTOR

Today's world, healthcare facilities are outfitted with standard perimeter safeguards as well as efficient and predictive cyber security technologies. With all these cyber security programs in place, the risk of effectively carrying out an assault on sensitive infrastructure (for instance, the key IT systems, HIS Hospital Information System, PACS Picture Archiving and Communication System as well as other LIS Laboratory Information Systems) stays extremely poor.

That is the only way to breach the perimeter defences, except with a physical attack, since connecting directly to servers and network parts that are not available from the outside is needed. In this situation, entry through abuse, burglary, or any other illegitimate means can be seen as a supplementary activity to a cyber threat.

It is well established that hospital or healthcare processes do not function adequately without IT technologies, namely the PACS as well as the LIS, without which it is incredibly challenging to deal with radiographic images with laboratory testing, rendering diagnosis and furthermore patient treatment complicated or very sluggish. This may be thought of as an injury multiplier effect.

As a result, it is critical to prepare for the possibility of attacks on hospital IT structures in order to reduce hospital operating capability and absorb patients in the emergency room in the case of a terrorist incident and subsequent maximum inflow of injured persons. Security issues can no longer be classified simply as physical or electronic. To combat such a confluence of challenges, it is important to implement an integrated strategy.

A. The protection of Critical Assets

The administration of Healthcare structures is used to facing complex challenges, such as the typical complexities of the healthcare sector and a number of internal and external emergencies that can and have occurred; however, the challenge of cybersecurity and physical security is one that most European hospitals and Healthcare structures do not yet fully understand and are unaware of.

Undoubtedly, the IT sectors of Healthcare systems have had to deal with a multitude of ransomware attack campaigns in recent years (the most well-known are Wannacry, NotPetya, and CryptoLocker) that are not directly aimed at a single form of structure.

For certain hospitals, the disruption was worse than predicted (due to a variety of factors, such as the spread of device clients of various management and origin), but this has the advantage of alerting systems and management to the problem and seeing it as a potential danger, much like any other.

Mostly in past years (primarily in the United States and Asia) have serious attacks on medical facilities been recorded (like orangeworm, kwampirs, medjack). This reinforced an unavoidable fact: hospitals are not immune to viruses as well as ransomware cyber attacks.

In certain situations, vulnerabilities in medical device systems have been exploited; medical devices were not considered a possibility, most likely due to cultural reasons, combined with the fact that medical device suppliers themselves did not consider an attack possible and were not prepared to deal with the repercussions. Evidently, it is important to understand the specific medical equipment market:

- Limited series productions, often very small series (for instance, in Radiation therapy)
- Highly sophisticated and advanced technologies necessitate high research and development costs.
- Broad sector regulations (MDD, MDR, IVD, IVR), with the requirement to credential each standard
- As a result, it is impossible to keep operating systems and antivirus software up to date

In past years, several municipal health structures have been confirmed to have been hit by major ransomware attacks, resulting in the complete blockade of some departments, such as the emergency room and hospitalizations, with the single exception of the most critical patients who were not moved elsewhere (in danger of life, in other words, negotiable without the help of a computer system). A criminal assault with the overt order for a cash ransom, a larger-scale operation than the usual ransomware now prevalent at the individual level personal computers, more centralized as whole networks and data servers are affected, rendering entire medical facilities inaccessible.

Of course, we just know what was reported in the press—in several circumstances, it has been reported that the relatively few compromised machines were reformatted and recovered without major data loss; in others, the government admitted that it wanted to pay the ransom for several days. However, most operators believe that the circumstances revealed are just a subset of those that have been confirmed and are never widely publicized for apparent purposes of poor publicity.

The most recent attacks mentioned in the press occurred in October 2019. (USA and Australia). Once more, with regard to the United States, the study leads specialists to conclude that attackers are especially reliant on portals, patients that are becoming increasingly common, since they are linked with EMR/EHR (Electronic Medical/Health Record). Around the same time, in recent years in Europe (at least after severe attacks on overloaded and sensitive infrastructure such as trains, subways, as well as airports), all critical structures are likely to be expected to be attacked. Till now, just assaults on hospitals with bombs have been reported in the East and Middle East.

In brief, European institutions must be trained for the worse in prepared to comply with all these threats systematically, precisely since it is clear that certain challenges will reach the old continent sooner rather than later. Not to mention the significant latency caused by the quest for appropriate alternatives and the time required to implement them in the systems.

- ❖ To understand the reference context (and the resulting difficulties and facilities), consider the following aspects of a typical European healthcare structure: Entrances and access control—unlike public offices or other public buildings, no hospital or healthcare structure has the option of restricting access to one or two single points of entry, nor is the commissioning of check points at a visitor control desk, with the control and filling of identify documents, possible.

The causes may be many, but one that stands out is the fact that having previously speculated the need to defend these structures from unique threats attacks (an unquestionably incorrect cultural aspect). We must also consider:

- Significant inflows—tens of thousands of patients for certain European hospital districts
- The measurements (hectares) of hospital enclosures within the sense of the urban fabric, often in architectural settings and historical buildings
- The combined participation of numerous institutions, such as colleges, with the resulting additional inflows of learners and other attendees

1) Critical assets: Hospital structures are distinguished by the having a large number of vital properties, most often of limited size as compared to industrial plants, but with the simultaneous presence of a large variety of different types of implants and different specialized protection mechanisms (idem—as compared to industrial plants). Cryogenic devices, RX systems, treating radioactive isotopes, massive magnetic field systems, gas reservoirs, hyperbaric systems, and so forth, for instance, and also with the biggest problems arising from the involvement of a great amount of people: patients, tourists, learners (the highest number being about 10–20 thousand people).

2) Separate administration of IT resources (IT department) and medical device assets (clinical engineering department), for historical and cultural reasons; this division was traditionally driven in the previous century due to the lack of networked medical device networks, at least those few that were computerized. Nowadays, the reverse is true: relatively few medical instruments are automated and linked to an IT network. Without ignoring the unique expertise of the two team members (IT and CE), there is indeed a clear need for management teamwork in cybersecurity aspects.

3) Emergency plans: All hospital systems have a well-developed culture of trust and have long established numerous emergency procedures, such as maximum patient influx, patient evacuation, and so on; the workforce is thereby prepared for even catastrophic situations and can therefore face the repercussions affected by attacks.

4) Provision of video survilliance systems: Because of the difficulty in implementing access controls, many hospital facilities are outfitted with multiple video monitoring devices, video cameras, as well as a video server, mostly for crime reduction purposes (only with video-recording).

B. *Recent security incidents*

Hospitals, according to the World Health Organization (WHO), supplement and enhance the efficacy of certain aspects of the health system by ensuring uninterrupted provision of care for urgent and structural way. They are an important component of health programs because they facilitate patient delivery and collaboration and play an important role in assisting some healthcare professionals along with general practice, awareness programs, including home-based services. As a result of these factors, cyber and physical assaults on hospitals, staff, healthcare personnel, and services have been on the rise around the world.

A few cyberattacks on the healthcare sector have been documented, and some examples are given below:

- The year 2017 The WannaCry ransomware attack compromised over 300,000 machines worldwide, demanding that users pay bitcoin ransoms. The WannaCry cyber attack was directed at the United Kingdom's National Health Service (NHS). The hackers were able to infect at least 16 health centers and 200,000 machines by leveraging a Windows loophole, resulting in the termination of almost 20,000 appointments and the paralysis of more than 1,200 pieces of diagnostic equipment. Furthermore, according to US newspapers, the Presbyterian Medical Centre was forced to close for ten days before a $17,000 ransom was paid.
- According to the press, in January 2019, hackers carried out an extortion attack on a heart specialist clinic in Melbourne, where they targeted patient data. As little more than a consequence, some medical reports were unavailable to personnel for more than three weeks. The Clinic may well have lessened the effect if data had been adequately and effectively supported, as well as if they had regularly invested in IT protection.
- In 2019, it was announced that American Medical Collection Agency, a billing services vendor, has been exploited for eight months between August 1, 2018, and March 30, 2019. After the attack was exposed, at least six protected organizations have come forward to report that the hack compromised their medical records. Up to 25 million clinicians have been infected so far.

C. *Threat and Risk Analysis*

Threats are behavior that may have a detrimental effect on an organization's important capital. Generally, threats manipulate device vulnerabilities, — for example, they take control of any flaws in the system to cause an undesirable result, such as asset harm or failure.

It is important to identify the potential root causes of attacks in order to ensure the stability of the infrastructure. As per ENISA, there are five major types of risks that healthcare organisations face:

a) Malicious actions: Malicious activities are intentional acts committed by an internal or external entity or agency to kill, rob, or disrupt a device. Malware – for example, viruses, ransomware and hijacking, social engineering, medical equipment interference, and software and data theft are all instances of malicious behavior.

b) Human errors: Human errors due to misconfiguration or inappropriate use of computers and information systems, as well as incorrect process execution.

c) System failures

d) Supply chain failures: Failures in the supply chain caused by third-party vendors, for instance power suppliers, medical device manufacturers, and so on.

e) Natural phenomena

The individual or organization responsible for carrying out these threats (threat actor) may also be categorized based on its role:

- Insider threat actor: This category includes hospital employees (physicians, nurses, administrative staff, etc.)
- Patients and visitors who are malicious
- Actors that are not physically present in the hospital are referred to as remote attackers.
- Other triggers include: including natural disasters or unintentional equipment malfunction

TABLE I. ASSET CATEGORIES

Category	Example
Specialist personnel	Employees, people with special functions, and so forth
Identification systems	Tags, bracelets, badges, biometric scanners, and CCTV (video surveillance) surveillance), RFID systems, and so on.
Networking equipment	Transmission media, network access cards, network equipment (such as hubs, switches, routers, and so on), telecommunications systems, and so on.
Operating resources	Medicinal goods, medical consumables, laundry supplies, sterile supplies, food supplies, and other items

V. MITIGATIONS

As outlined in this article, one rational solution for reducing social insecurity in a local or regional environment is to assist operators in vulnerable industries in the the durability of their facilities against acute circumstances. However, it was also shown that any facility in every sector is vulnerable because it relies on the dependable operation of many more infrastructures, and conversely.

As a result, a second column must be installed to complement risk assessment efforts at the specific point of care with federal catastrophe resilience networks. These networks will draw together stakeholders from all industries, such as industry, local and regional governments, organizations, and so on, to facilitate dialogues about the joint danger condition, sectoral dependencies and vulnerabilities, and reliability criteria.

The Infrastructure Security Partnership (TISP)5 has released a Guide for Developing an Action Plan on Regional Disaster Resilience for the United States of America. This document develops approximately 150 statements based on twelve fundamental objectives, such as awareness and comprehension of interdependencies, risk management and prevention, cooperation and teamwork, roles and obligations, business sustainability and continuity of activities, and public information/risk communications. In addition, a seven-step action plan framework is proposed to demonstrate how a regional formally or informally cooperative program can be applied.

VI. ACKNOWLEDGMENT AND FUTURE RECOMMENDATIONS

Critical infrastructure is the cornerstone upon which everyday crucial social and economic functions depend, and any damage or failure of critical infrastructure has the potential to have a significant effect on our lives. Collaboration and the exchange of best practices, approaches, and perspectives will continue to foster and improve national and global sensitive infrastructure protection and stability today and in the future.

VII. REFERENCES

Agency, C. a. (n.d.). *A Guide to Critical Infrastructure Security and Resilience.*

Ani, U. D. (2019). *A REVIEW OF CRITICAL INFRASTRUCTURE.* PETRAS/IET Conference Living in the Internet of Things: Cybersecurity of the IoT.

Aradau, C. (2010). *Security that matters: critical infrastructure and objects of protection.* oro.open.ac.uk.

Coordinating, H. S. (May 2007). *Department of.* Healthcare Sector Coordinating.

Engelhardt, M. A. (October 2017). *Hitching Healthcare to the Chain:.* Technology Innovation Management Review.

Jain, M. (n.d.). *Employability implications of artificial.* emeraldgrouppublishing.

Katina, P. F. (2012). *ON CRITICAL INFRASTRUCTURE INTERDEPENDENCY.* International Annual Conference of the American Society for Engineering Management.

Kun, L. (January 2009). *Protection of the Health Care and Public Health Critical Infrastructure and.* https://www.researchgate.net.

Manan, l.-l. A. (n.d.). *A Study on Significance of Adopting Cloud.* Universiti Teknologi Malaysia, Malaysia.

Manan, l.-l. A. (n.d.). *A Study on Significance of Adopting Cloud.* Universiti Teknologi Malaysia, Malaysia.

Meri, A. (2019). *Modelling the utilization of cloud health information systems in the.* ScienceDirect.

O’Neill, P. (n.d.). *Protecting Critical Infrastructure by.* timreview.ca.

Riegel, C. (n.d.). *Risk Assessment and Critical Infrastructure Protection in.*

Services, U. D. (2016 May). *healthcare and public health sector specific plan.* U.S. Department of Health and Human Services.

WALKER-ROBERTS, S. (n.d.). *A Systematic Review of the Availability and.* IEEE.

Yaqoob, I. (n.d.). *Blockchain for Healthcare Data Management: Opportunities, Challenges, and Future Recommendations.*