Critical Infrastructure Security in the HealthCare Sector (May 2021)

Tharuka G.P.H.S.
Sri Lanka Institute of Information Technology

***Abstract*— Because of their vital and fragile facilities, healthcare organizations are an easy target for cybercriminals. A few security issues have arisen as a result of the increase in digitization. It is critical to consider these critical aspects not only from a specialized standpoint, but also from a legal and managerial standpoint. It is also important to recognize the potential It is also crucial to recognize the possible danger posed by the ability to combat cybercrime. It is not as if there were just physical and cyber threats, but there is a mix of both. It is important to understand how healthcare systems can be harmed and destabilized, as well as how terrorists use them to achieve their objectives. This review journal gives an excellent overview of the major issues facing the healthcare industry, as well as a list of recent security incidents. There are five major types of risks, as well as a vital asset classification.**

***Index Terms*— Artificial Intelligence (AI), Cybercrime, Cybersecurity, ECSO, Electronic Medical Record (EMR), Healthcare and Public health (HPH), ISO, NIST, Task Force (HCIC)**

I. Introduction

CRITICAL INFRASTRUCTURE SECURITY refer to the protection of systems, networks and assets that are considered to be essential for the continued health and safety of a country, its economy and its public. However, security technologies and best procedures can help prevent or reduce the effect of a breach and relieve the risks associated with internet-connected industrial control systems, as well as the interruptions and influence an attack might have on a city or country. In 2003, the federal government recognized the Health Care and Public Health (HPH) Division as a critical infrastructure component of the United States. It is recognized that the Healthcare and Public Health (HPH) Division is essential for national security, the economy and public health, taking into account safety and resilience. Any company engaged in healthcare and medical related products and services is recognized as a representative body in the healthcare sector and is further classified under six major industries. These industries include pharmaceuticals, biotechnology, equipment, distribution, facilities and management healthcare.

Moreover, health care is a highly trusted establishment that carries valuable and personal information, which means that it can reap huge financial and political benefits by exploiting its insecurities. The needs of the health care sector pose several security challenges. As it is vital for human life, it is important to ensure the security of data without compromising access to health care. Increasing the interrelationship between the hospital's physical and cyber assets brings new threats are being considered to ensure patient safety. It is important to be aware of potential safety issues to understand the potential risks to health facilities. It is also important to know what critical assets are available and their impact on obtaining systems. Only then will it be possible to identify and plan opportunities that will help identify the threats that a security solution to a health care facility should cover. In these cases, physical and cyber threats must be used to launch attacks. Because they are the most complex and interesting threats to deal with.

The Healthcare and Public Health (HPH) Sector produces and distributes products and services that are critical to ensuring local, national, and global health welfare. Before, after, and after any event of real or possible health implications, HPH Sector services are vital in maintaining the five key task areas as well as safeguarding Sector properties, staff, and the populations they represent.

A coordinated strategy involving all appropriate collaborators and stakeholders is needed to optimize the stability and durability of the country's vital infrastructure. Healthcare and public health are critical stakeholders in achieving this goal. In an emergency, the quality of healthcare procedures is critical. They are an aid to national security because of their emergency management position, which elevates them beyond stakeholder status. In collaboration with the Department of Homeland Security, the need for a strategy specific to the sector that optimizes the interaction between health care and public health business activists is crucial. Threats to a country's vital resources have developed in modern culture, differentiating into digital and genetic networks.

The Healthcare and Public Health (HPH) Sector-Specific Plan (SSP) was developed to promote cross-division effort and coordination in order to improve the stability and durability of the industry's vital infrastructure, which is vulnerable to all hazards. The SSP's advice is meant to be customized to be specific to the important market competitors. This includes guaranteeing that the strategic advice is consistent with the healthcare and public health sector's risk environment and unique operational landscape. This prohibits the business layers from wasting resources on non-essential reasons.

.

The National Infrastructure Protection Plan of 2013 has played a key role in achieving this goal. The industry has developed an assimilated approach to handling the threats to vital infrastructure and the personnel that supports it. Furthermore, this paper describes the critical infrastructure protection and security team procedures and new technologies in the healthcare sector.

II. Research statement

The main concept of this research is to gather more than 15 sources and create a valuable research paper for everyone in the world who worries about the healthcare sector. It illustrates how critical infrastructure, artificial intelligence, and cybersecurity are being coordinated and addressed by the various teams currently assigned to the healthcare sector around the world.

The focus here is on the Health and Public Health Specific Plan (SSP), which aims to enhance the safety and resilience of critical infrastructure in industries that cover all hazards. Of particular note is the inability of the healthcare system to provide reliable and secure treatment without greater digital access. The health care system is involved, but if it is unsafe, it can jeopardize patients' safety and expose them to unwanted accidents as well as incur unaffordable personal expenses. It deserves special attention.

The Cyber Security (HCIC) Task Force was created by Congress in 2015 under the Cyber Security Act. The reason is to focus on the tasks facing the healthcare industry to protect and defend compared to cybersecurity incidents, either intentionally or unintentionally. All healthcare providers have a greater responsibility than ever to protect their procedures, medical equipment, and patient data, and many healthcare organizations face major source limitations, as operating boundaries can be as low as 1%. With regard to corporate initiatives that enhance the cyber security of healthcare organizations, it has been widely stated that it is important for healthcare organizations to assess cyber risk.
For example, identity theft, extortion software, and targeted nation-state intrusion make us understand just how insecure our health care data is. This paper also explains exactly what health care is.

Artificial intelligence helps health care professionals better understand their patients' everyday patterns and needs, and with that understanding can provide better guidance and support to stay healthy. Therefore, artificial intelligence now occupies a prominent place in the healthcare sector. It shows how the advancement of technology can be utilized for infrastructure. The World Health Organization provides information assurance that provides a well-developed model for integrating technical and behavioral issues in the context of e-healthcare security and privacy.

The next step in this test is to look at how wellness hosts can calculate the success of security and confidentiality compliance to achieve data certification limits. The final section covers future research and findings in this regard.

III. Literature of review

Without greater digital access, the health-care system would be unable to provide reliable and secure care. If the health-care system is linked but insecure, patients' protection can be jeopardized, exposing them to needless danger and causing them to pay unaffordable personal costs. Our nation needs to figure out a way to keep our patients from having to choose between connectivity and security. The Health Care Industry Cybersecurity (HCIC) Task Force was created by Congress in the Cybersecurity Act of 2015 (the Act) to resolve the challenges that the health care industry faces in securing and defending itself against cybersecurity incidents, whether intentional or unintentional. Identity theft, ransomware, and targeted nation-state hacking are all examples of how insecure our health-care data is. Data obtained for the benefit of patients and used to develop new therapies can be misused for malicious purposes including fraud, identity theft, supply chain disturbances, theft of R&D, and stock manipulation. Most notably, cyber-attacks wreak havoc on patient care. In the United States, the health-care sector is a mosaic, with very broad health systems, sole provider practices, public and private payers, research organizations, medical product developers and software firms, and a diverse and widespread patient population. On top of that, there is a tangle of well-intentioned federal and state laws and regulations that can make it difficult to solve problems across jurisdictions. This has the potential to build obstacles to creativity and user-friendliness. Patients must be shielded from harm caused by cybersecurity vulnerabilities and exploits throughout this complex network.

All health-care delivery entities (including all the above constituents) have a greater obligation than ever before to protect their processes, medical equipment, and patient data. Since operating margins can be as poor as 1%, most health-care organizations face major resource constraints. Many businesses cannot afford to hire in-house information security experts or appoint an information technology employee with cybersecurity as a secondary responsibility. These organizations also lack the resources needed to detect and monitor threats, as well as the ability to interpret and convert threat data into actionable intelligence and act on it. Many businesses have not crossed the digital divide because they lack the technological tools and skills to deal with existing and emerging cybersecurity threats. It is possible that these groups will not realize they have been attacked until it is too late.

Furthermore, both large and small health-care delivery entities face several unsupported legacy systems (hardware, software, and operating systems) with numerous vulnerabilities and few new countermeasures that are difficult to replace. Industry would need to drastically reduce the use of less justifiable legacy and unsupported goods, as well as build and promote strategies that successfully reduce risk in future products. Many providers and other health care professionals, with the exception of IT security staff, believe that the IT network and equipment they support are in good working order and that their level of cybersecurity risk is minimal. Recent high-profile events, such as malware attacks and large-scale data breaches, have shown that this risk presumption is incorrect, and have created an impetus to improve cybersecurity knowledge and understanding in the health-care sector.

Furthermore, recent ransomware attacks have shown how a device breach will disrupt patient services at health care delivery organizations. Many technology experts have difficulties explaining the value of cyber defenses to corporate leadership prior to these attacks, and how risk avoidance would save resources and defend against reputational harm in the long run, according to members of the health ecosystem. Making the decision to emphasize cybersecurity in the health-care sector necessitates cultural transitions, expanded leadership coordination, and reforms in how providers conduct their roles in the clinical setting.

IV. HEALTHCARE SECTOR

The healthcare sector is a collection of businesses that provide products and administrations for the treatment of patients for prophylactic, beneficial, rehabilitative, and prophylactic treatment. This includes items and administrative upgrades and commercialization that help maintain and restore well-being. The state-of-the-art healthcare sector consists of three primary branches: Suppliers, Fluid and Budget. It is isolated to specific areas and groups and relies on conspiracy groups of specialists and traditional specialists who are qualified to meet the well-being needs of individuals and communities.

The healthcare sector is the largest and fastest growing market in the soil. Health services contribute more than 10% of GDP (GDP) in the creation of many countries and can be a critical part of a country's economy.

Figure 01: Current Healthcare sector

Furthermore, both large and small health-care delivery organizations are confronted by a number of unsupported legacy technologies (hardware, applications, and operating systems) that have multiple flaws and little new countermeasures and are challenging to substitute. The healthcare sector is usually split into many sectors in terms of financing and administration. According to the United Nations International Standard Industrial Classification (ISIC), the healthcare sector basically consists of:

1. Hospital activities.
2. Medical and dental practice activities.
3. Other human health activities.

This third category includes operations under the supervision of or under the supervision of nurses, midwives, physiotherapists, scientific or diagnostic laboratories, pathology centers, residential health care, or optics, hydrotherapy, medical therapy, yoga, music Is. Therapy, Occupational Therapy, Voice Therapy, Chiropractic, Homeopathy, Chiropractic, Acupuncture, and other health care professions.

The Global Market Classification Standard and the Industry Classification Benchmark separate the industry into two distinct categories.:

1. healthcare equipment and services; and
2. pharmaceuticals, biotechnology and related life sciences.

Companies and institutions that offer surgical devices, medical materials, and healthcare facilities, such as clinics, home healthcare providers, and nursing homes, make up the healthcare equipment and services sector. Corporations that manufacture bioengineering, pharmaceuticals, and other research resources are included in the above-mentioned industry category.

Other approaches to identifying the reach of the healthcare sector aim to use a wider concept that includes other primary activities related to health, such as health provider preparation and training, health service delivery policy and administration, conventional and alternative medicine coverage, and health insurance administration.

V. CRITICAL INFRASTRUCTURE AND ARTIFICIAL INTELLIGENCE

There are 16 critical infrastructure sectors whose assets, structures, and networks, whether physical or virtual, are deemed so important to the US that their incapacitation or destruction will have a crippling effect on defense, national economic security, national public health or protection, or some combination of these.

As an antidote to artificial intelligence, healthcare providers will be able to understand the day-to-day habits and desires of the patients they care about, and as a precautionary measure, this understanding will be able to provide better inputs, advice, and motivations to stay healthy. Artificial intelligence is on the verge of becoming a game-changing power in healthcare. How will the effects of AI-driven tools favor physicians and patients? There are virtually infinite ways to use technologies to deploy more accurate, effective, and impactful treatments at just the right moment in a patient's treatment, from infectious diseases and cancer to radiology and risk management. Artificial intelligence is primed to be the catalyst that pushes improvements across the treatment spectrum as payment systems expand, patients expect more from their services, and the amount of available data continues to grow at a staggering pace.

Standard analytics and clinical decision-making approaches have a number of drawbacks, and AI has a few of them. When learning algorithms engage with training results, they can become more precise and reliable, giving humans unparalleled insight into diagnostics, care procedures, medication variability, and patient outcomes.

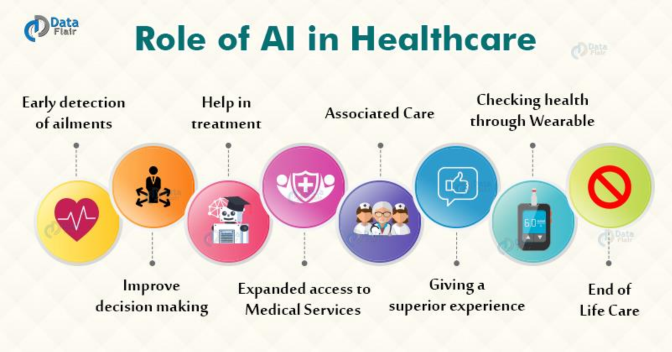

Data Flair
Role of AI in Healthcare
Early detection of ailments
Help in treatment
Associated Care
Checking health through Wearable
Improve decision making
Expanded access to Medical Services
Giving a superior experience
End of Life Care

Figure 02: Role of AI in Healthcare

Predictive analytics and clinical decision support tools that alert caregivers to challenges well before they would otherwise understand the need to respond would be driven by artificial intelligence, which will provide much of the bedrock for the evolution. For disorders like epilepsy or sepsis, AI may have earlier alerts, which also necessitate rigorous review of large datasets.
Machine learning will also aid in determining whether or not to continue caring for chronically ill patients, such as those who have gone into a coma after cardiac arrest. Since it began to play a part in healthcare, AI has progressed. The effect of AI on healthcare has the potential to change people's lives. It would not only benefit patients and service staff, but it would also save a large amount of money in the healthcare industry.

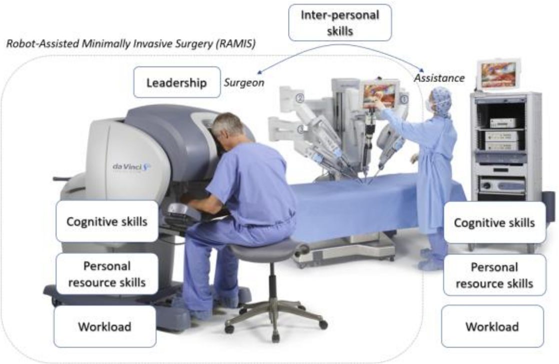


Figure 03: Surgical Robots

- **Empowered Surgical Robots -** AI can make a difference in the lives of patients in particular. AI is part of the computer science that people love and has the ability to learn artificially. In the early days, these robots were only used as slaves, but today these robots have managed to act like doctors.

Figure 04: Virtual Nursing Assistant

- **AI and The Virtual Nursing Assistant -** This virtual nurse helps patients remember to take medications on time. Assists know about patient's medical information and medical history. For doctors, their schedules are reminded. These virtual nursing assistants are better at caring for patients. They make zero mistakes because of their intelligence. It can be an advantage for everyone.

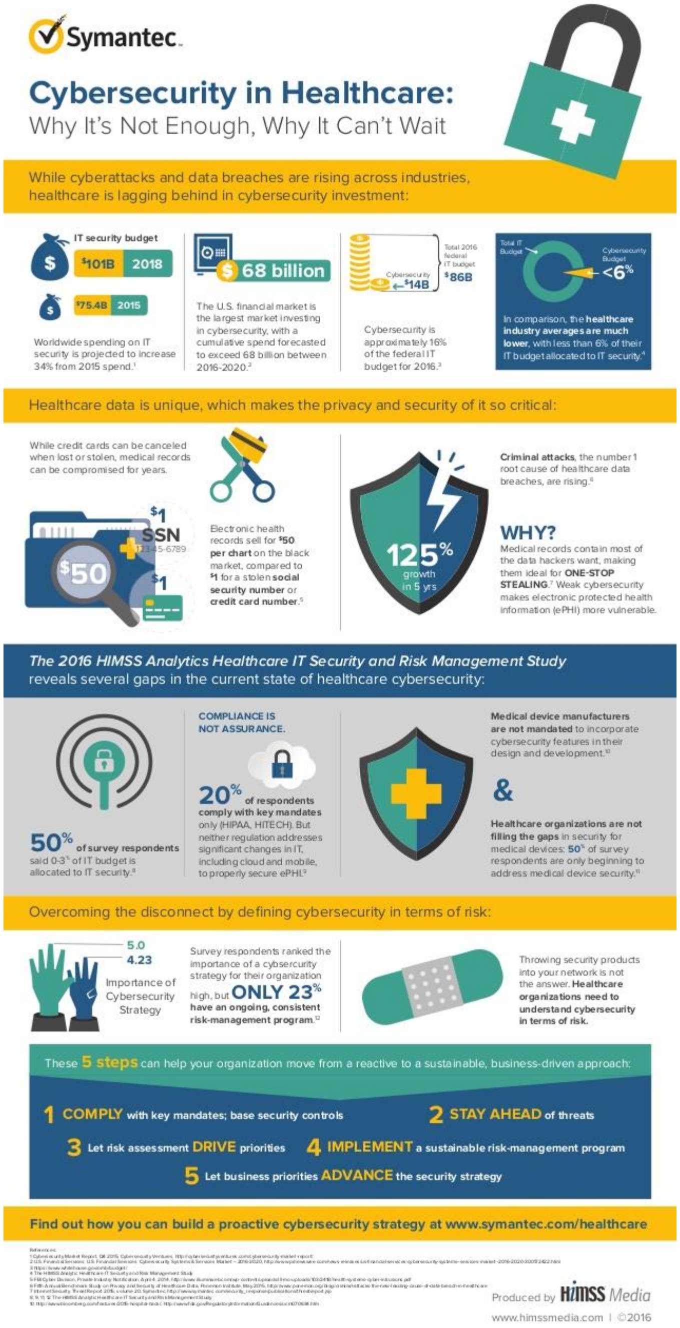
Figure 05: AI helped and provided medical diagnose.

- **AI Helped and Provided Medical Diagnose -** Artificial intelligence helps to diagnose diseases. This is very easy because these robots know everything about the patient and their medical history. Not only does it provide an advantage in cost and time, but it also provides a 100% accurate diagnosis.

Several ways in which AI can be used to improve and enhance the health sector were explained. Everything is easy and efficient because of AI.

VI. CYBER SECURITY IN HEALTHCARE SECTOR

Effective protection of the health sector is paramount and, as mentioned earlier, the healthcare sector is the collection of sectors with public access to physical facilities, semi-private, private, and critical infrastructure.


Symantec.

Cybersecurity in Healthcare:
Why It's Not Enough, Why It Can't Wait

While cyberattacks and data breaches are rising across industries, healthcare is lagging behind in cybersecurity investment:

IT security budget
$101B 2018
$75.4B 2015

Worldwide spending on IT security is projected to increase 34% from 2015 spend.[1]

$ 68 billion

The U.S. financial market is the largest market investing in cybersecurity, with a cumulative spend forecasted to exceed 68 billion between 2016-2020.[2]

Total 2016 federal IT budget $86B
Cybersecurity $14B

Cybersecurity is approximately 16% of the federal IT budget for 2016.[3]

Total IT Budget
Cybersecurity Budget <6%

In comparison, the **healthcare industry averages are much lower**, with less than 6% of their IT budget allocated to IT security.[4]

Healthcare data is unique, which makes the privacy and security of it so critical:

While credit cards can be canceled when lost or stolen, medical records can be compromised for years.

$1 SSN 123-45-6789
$50
$1

Electronic health records sell for **$50 per chart** on the black market, compared to **$1** for a stolen **social security number** or **credit card number**.[5]

Criminal attacks, the number 1 root cause of healthcare data breaches, are rising.[6]

125% growth in 5 yrs

WHY?
Medical records contain most of the data hackers want, making them ideal for **ONE-STOP STEALING**.[7] Weak cybersecurity makes electronic protected health information (ePHI) more vulnerable.

The 2016 HIMSS Analytics Healthcare IT Security and Risk Management Study reveals several gaps in the current state of healthcare cybersecurity:

50% **of survey respondents** said 0-3% of IT budget is allocated to IT security.[8]

COMPLIANCE IS NOT ASSURANCE.

20% **of respondents comply with key mandates** only (HIPAA, HITECH). But neither regulation addresses significant changes in IT, including cloud and mobile, to properly secure ePHI.[9]

Medical device manufacturers are not mandated to incorporate cybersecurity features in their design and development.[10]

&

Healthcare organizations are not filling the gaps in security for medical devices: 50% of survey respondents are only beginning to address medical device security.[11]

Overcoming the disconnect by defining cybersecurity in terms of risk:

5.0
4.23
Importance of Cybersecurity Strategy

Survey respondents ranked the importance of a cybsercurity strategy for their organization high, but ONLY 23% **have an ongoing, consistent risk-management program.**[12]

Throwing security products into your network is not the answer. **Healthcare organizations need to understand cybersecurity in terms of risk.**

These 5 steps can help your organization move from a reactive to a sustainable, business-driven approach:

1 COMPLY with key mandates; base security controls
2 STAY AHEAD of threats
3 Let risk assessment DRIVE priorities
4 IMPLEMENT a sustainable risk-management program
5 Let business priorities ADVANCE the security strategy

Find out how you can build a proactive cybersecurity strategy at www.symantec.com/healthcare

References:
1 Cybersecurity Market Report, Q4 2015, Cybersecurity Ventures, http://cybersecurityventures.com/cybersecurity-market-report/
2 U.S. Financial Services: U.S. Financial Services Cybersecurity Systems & Services Market – 2016-2020, http://www.prnewswire.com/news-releases/[illegible]
3 https://www.whitehouse.gov/omb/budget/
4 The HIMSS Analytic Healthcare IT Security and Risk Management Study
5 FBI Cyber Division, Private Industry Notification, April 4, 2014, [illegible] health-systems-cyber-intrusions.pdf
6 Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, May 2015, http://www.ponemon.org/blog/criminal-attacks-the-new-leading-cause-of-data-breach-in-healthcare
7 Internet Security Threat Report 2015, volume 20, Symantec, http://www.symantec.com/security_response/publications/threatreport.jsp
8, 9, 11, 12 The HIMSS Analytic Healthcare IT Security and Risk Management Study
10 http://www.bloomberg.com/features/2015-hospital-hack/; http://www.fda.gov/RegulatoryInformation/Guidances/ucm070634.htm

Produced by HIMSS Media
www.himssmedia.com | ©2016

Figure 06: Cybersecurity in Healthcare

There are many types of buildings in the health sector. Some buildings will always have patients, some only during daylight hours, some have important and expensive medical equipment, and some contain clients. Buildings may have physical medical records, staff computers may have access to personal data, and clients may store personal data, critical information, and critical software for the healthcare sector. In addition to the usual software used for an office building, internal software in the healthcare sector is used to handle patients' medical data and to operate and control medical equipment and machinery. To protect all of this, the healthcare sector is expanding security systems in their facilities, so it is common to have several security systems to handle different security sectors as no system covers everything.

This section will present an overview of how a video management system, an access control system, a fire detection system, SCADA, ICS, and smart building sensors, as well as a Cybersecurity protection system works to make the healthcare sector a more secure environment. As introduced previously, the healthcare sector faces unprecedented risks and compounding regulatory compliance requirements. Healthcare organizations have many assets that are essential to their functioning and must be protected. Attackable assets include facilities and buildings, mobile devices, data, interconnected clinical information systems, network equipment, detection systems, networked medical equipment, and remote care systems. The two most critical hospital assets are the interconnected clinical information system and networked medical equipment (Independent Security Assessment, 2016). The most interesting information for attackers may be personal identification information (PII) and secure health information (PHI) in patient reports. Healthcare Organizations and Their Assets Technological Risks (Applications and Operating Systems, Control Gaps and Lack of Design, Incompatible Devices, Unsecured Networks, Weak Credentials, Cyber Threat Prevention and Detection, Lack of Smart Sensors, Remote Access Policies, Lack of Employee Training And awareness etc.) or organizational and social (user behavior, human error, etc.). These vulnerabilities can be exploited in different ways by attackers that use different types of malicious actions (e.g., virus, ransomware, hijack). The probability of these attacks can increase as healthcare organizations suffer also from system failures (e.g., software, hardware and network failure, inadequate firmware); human errors (users systems' misuse, unauthorized access, absence of audits and logs, etc.); and natural phenomena. Attackers have different purposes. They can be categorized as damaging, extorting, disrupting service, or collecting data to prepare for future attacks, as they hope.

As such, health infrastructure is identified as a significant potential target of cyberattacks, which highlights the need to enhance protection from them. It is important for healthcare organizations to prevent unauthorized access, use, sabotage, deletion, and minimization of pollution, to respond effectively, quickly, and efficiently, and to minimize the impact of attacks on their networks and systems in the following organizations: And to take technical action. With regard to organizational measures that will enhance cybersecurity in healthcare organizations, it has been widely claimed that it is important for healthcare organizations to assess cyber risks. Cyber risk assessments are used to identify, estimate, and prioritize risk for corporate assets, corporate operations, individuals, other organizations, and national interests due to the implementation and use of information systems *(NIST, 2019b)*. In addition, healthcare organizations have developed and integrated general and case-specific laws, standards, plans and policies that outline cybersecurity measures and crisis management practices such as the NIS Order *(EU, 2016)* and *ISO 27001 (ISO, 2019).* should. Security measures are in place to protect the location and other sensitive, critical, or valuable assets and areas (e.g., computer room, central clients, clinical information systems, and electronic health records) from attacks.

As the human factor is a major security threat in the health sector, it is important for people to be aware of basic cybersecurity issues and improve their skills - both technical and behavioral *(ECSO, 2018)*. In addition, healthcare professionals (including researchers, administrators, desktops, physicians, copywriters, IT copyright holders, and technical staff) should be properly trained in cybersecurity security and crisis management issues, standards, planning and protocols *(Martin And al., 2017).* In doing this, stakeholders that find themselves affected by, or actively seek involvement in crisis management processes, can manage and cooperate effectively and in timely fashion on security planning, preparedness, response, recovery, and impact mitigation. With regard to technical measures, it has been reported that healthcare organizations should adopt and implement different practices that will enhance data, systems, devices, and networks security, such as the following, according to *ISO (2018)* and *NIST (2019a):*

- • **Authentication** guarantees that the asserted names of the people involved in conversation are correct, and that no one is trying to replay a prior communication without permission.
- **Access control (authorization)**—much like physical access control, described above—guarantees that only individuals, as well as software and IT infrastructure, can only gain access to, and perform operations on, stored information and flows that they are authorized for. Unlike physical access control, different access levels can be granted to systems, devices, and networks.
- • **Availability** is a security feature that guarantees permitted access to network components, storage data, information flows, utilities, and applications is not denied as a result of network incidents.
- **Reliability** has been defined as the ability of the system to perform its functions for a period of time. This is a high-level security requirement and to be achieved different mechanisms should be implemented (e.g., availability, communication security), as described in the respective sections above.
- • **Non-reputation** is the power to deter an agent or agency from refusing performing a certain data-related activity by making evidence of multiple network-related activities visible.
- **Data confidentialities** make sure that the data content cannot be understood by unauthorized entities.
- **Data Integrity** is a security dimension that guarantees the accuracy or precision of data. Data must be protected compared to illicit alterations, deletions, creations and alterations, and a warning of these unauthorized activities must be provided.
- **Backup** is the process of backing up the operational state, architecture, and stored data of database software.
- **Tracing systems** should log access and errors to the collected and stored data (e.g., time, date, users' accessing the system, fails, wrong password).
- **Log files** are automatically produced files, recording events, messages from certain software and operating systems.
- **Communication security** is a level of security that ensures that information flows only between properly separated endpoints and does not interfere with or interfere with the process. To obtain communication security, mechanisms such as encryption through Secure Sockets Layer (SSL), Virtual Private Networks (VPNs), timestamps, auditing and restricting access per-user-group should be implemented.

The above countermeasures will be completed with a security planning approach, focusing on cyber security requirements for new devices or systems that need to be designed and implemented from the outset of the procurement, design, development, and maintenance phase.

VII. INFORMATION ASSUARENCE

Information assurance (IA) encompasses characteristics of security services, information, and security countermeasures. Since a flaw in one will result in a failure in the whole system, the emphasis of IA is on balancing the relationships between these. The details may be in storage, encoding, or transmission mode right now. Security Services are supported not only by technical information including device compatibility, data integrity, user verification, and secrecy, but also by operations and practices, and, most importantly, individuals. How safe the system is essentially determined by whether an individual develops a policy and uses Information assurance technology.

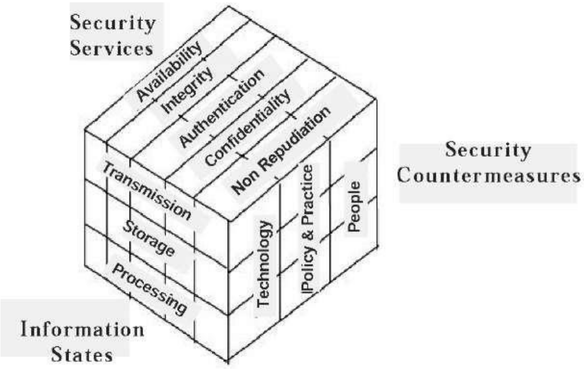


Figure 07: Information Assurance Model

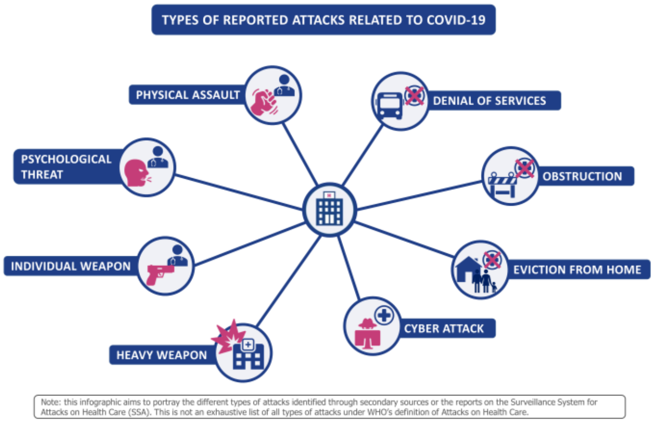
In the field of e-Healthcare protection and privacy, knowledge assurance offers a well-developed paradigm for integrating technical and behavioral problems. Information security can only be successful if e-healthcare is carefully planned and monitored for compliance. In the context presented for this research, information assurance is inherent in security and confidentiality policy compliance and provides the framework for integrating different research areas. Therefore, a theoretically strong framework has been proposed for the inclusion of TRA and TAM in the context of health care information certification to bridge the gap between policy making and policy compliance.

With the help of government resources from the National Institute of Standards and Technology (NIST) related to health and human services, information is being transformed into a variable model for certification and compliance. The Department of Health and Human Services provides consumer-centric and information-rich healthcare: a framework for strategic activism, readiness to change healthcare, and a framework for activism and leadership. NIST offers policy and safety frameworks as well as healthcare tools and other support from both the clinical and administrative sectors.

VIII. COVID-19

The best example facing the healthcare sector these days is COVID-19. The security measures and infrastructure they use are done using the latest technology.

"*Ensuring access to health services is the cornerstone of a successful health response. Any verbal or physical act of violence, obstruction or threat that interferes with the availability, access and delivery of such services*" is defined as attack on health care by the World Health Organization (WHO).



Note: this infographic aims to portray the different types of attacks identified through secondary sources or the reports on the Surveillance System for Attacks on Health Care (SSA). This is not an exhaustive list of all types of attacks under WHO's definition of Attacks on Health Care.

Figure 08: Types of reported attacks related to COVID-19.

The following statistics show the nature of attacks on health services related to COVID-19, ranging from the use of heavy weapons aimed at health facilities to the disrepute of health workers. In the end, whether they take the form of a cyber-attack or a physical attack, they deprive people of their urgent needs. Danger to health care providers. Disrupts health systems. The COVID-19 epidemic has put some health systems under severe pressure. Therefore, it is necessary to use every health resource to respond to this public health emergency and to successfully mitigate its effects. During the epidemic, the international community, governments, and civil society took the first steps to protect health systems by attacking health care as well as its roots.

The World Health Organization (WHO) continues to gather information and data to improve our understanding of COVID-19 related attacks, to inform its partner network, and to document good practices.

IX. FUTURE RESEARCH

The health-care system is constantly changing, and the systems involved are shaping how patients are cared for. The EHR (Electronic Health Report), which includes the authentication of a patient's lifetime health record by each health care provider, is the ultimate objective of EMR adoption. Smart card technology is emerging as a new technology that allows patients to keep their own virtual medical charts in their pockets. This EHR is a virtual roadmap that guides the doctor's medical decisions. Having this information on hand, even if it is a portable device, allows physicians access to critical information to exchange data while geographically dispersed. Further research on this technology is very exciting and research reports related to this should be produced in the future.

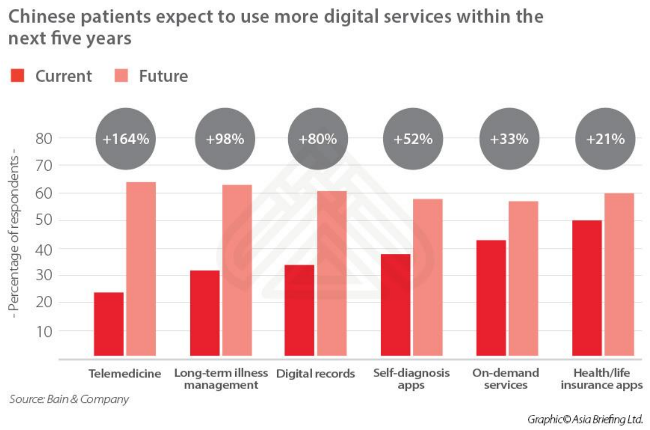


Figure 09: Chinese patients expect to use more digital services within the next five years.

In the future, there will be more ethical and financial problems to deal with. The regulatory implications of telemedicine and EMR implementation need to be clarified. Who holds the Electronic Medical Record (EMR)? Who will be held accountable for illegal access attempts? Would the patient be able to access and edit their electronic medical records, such as adding a living will or organ donation predilections? What happens if a provider is used to retailer healthcare data for an enterprise, then the vendor goes out of business? Would telemedicine consultations be reimbursed by insurance companies? In order for healthcare processes to be successful, these legal, economic, and technical challenges must be addressed, and decisions must be made as to how best to care for the patient, regardless of how, when, or what evidence is used to obtain the best medical care.

More research papers are needed in the future to explain these doubts, including legal and financial concerns.

Patient data is vital, and it necessitates the use of appropriate technologies to protect, sustain, and deploy appropriate healthcare services. To reap the full benefits of Artificial Intelligence in the healthcare sector, a massive effort to justify legal and well-suited policymaking is needed.

The next research in the future should be on how to deal with epidemic viruses, how to measure the success of healthcare security and privacy policy compliance to achieve information certification limits.

X. Conclusion

This review paper offers an extensive overview of potential studies that can help to promote the area of health information certification research and training. The Internet has the potential to make significant improvements in the world of health care, enabling doctors and nurses to do their best by facilitating an efficient and successful transition. Allowing everyone to concentrate more on treatment not only saves time and money by reducing management, but it also saves lives.

The critical infrastructure facilities, processes, and skilled workforce of the HPH Sector function in a diverse and competitive risk setting. As previously said, this risk system consists of a complex and varied combination of manmade and naturally occurring risks and hazards. Scheduled to the spirit of its "open access" assignment, physical services and processes, supply chains, and system interconnectedness, HPH Sector transportation is large and highly dispersed, rapidly mutually dependent and intertwined, and fundamentally fragile. Given these challenges, HPH government and private sector stakeholders must collaborate to create and incorporate collective frameworks customized to the experiences of the Sector's policy, organizational, and risk contexts in order to understand and resolve current and emerging threats.

The critical infrastructure of the HPH Sector, as well as the factors that influence it, function in a diverse and progressively more complex environment. The changing goal posts caused by technical advancements and political changes may cause uncertainty when it comes to managing the professional workforce, structures, and properties. The professional workforce, systems and systems operate in a very complex and risky environment. For example, the repeal of the Patient Protection Act has forced the entire market to adapt to new realities. Similarly, climate change poses natural risks, while others argue that they are artificial. The scale of the market, as well as the interconnection of its networks, exacerbates the issue. This section is insecure due to the unrestricted access to many clinical services, physical facilities, procedures, and system interconnections. Cooperation between the government and the HHP sector is crucial to enhancing preventive measures in a risky environment.

The sector must make the most of the immense tools available to it, which include digital capabilities, consulting resources, and other government agencies. The ability of the promoters to leverage a diverse range of tools is critical to the program's progress. Info sharing is not an alternative, but rather the program's assumption. Since the industry is still changing, the sector should be able to accommodate changes and reprioritization of risk management techniques in order to improve protection. The sector's leadership should assess success in adopting the guidelines on a regular basis to find any flaws.

The final conclusion of this research is that critical infrastructure security in the health sector is linked to new technology. Technology improves the security of the health sector. It is everyone’s job, among other things, to protect our most valuable sector. Special thanks to the Health Services Task Force and other teams who are doing their utmost to safeguard the health sector.

XI. Acknowledgment

Without the special support of my lecturer Mr. Kanishka Yapa, this paper and the research behind it would not have taken place. His enthusiasm, knowledge and attention to detail were a great inspiration for this and helped me to carry out my work properly. Piyumi Abhilashi and Umesh Sithara, my friends also explored my research and helped me with the language and content. I am grateful for the intelligent comments that anonymous peer reviewers hope to present to this research paper.

The generosity and uniqueness of all has enhanced this study in countless ways and saved me from many mistakes; Inevitably the rest are entirely my responsibility. I really appreciate the contribution of Bilal Reza, My Colleagues at Sri Lanka Institute of Information Technology, Have Also Looked Over My Research Paper And spent so much time reading every version of this article and finding and correcting the shortcomings.
I will never forget my family members in the pursuit of this project. I thank my parents for being with me in anything I pursue. They are role models.

Finally, I would like to thank my University, Sri Lanka Institute of Information Technology for creating someone like me who gives 100% effort to complete any assignment given by the lecturers.

References

[1] John Soldatos, James Philpot and Gabriele Giunta, *CYBER-PHYSICAL THREAT INTELLIGENCE FOR CRITICAL INFRASTRUCTURES SECURITY*, US: Hanover, MA 02339, 2020. [Online]. Available: https://library.oapen.org/bitstream/handle/20.500.12657/47871/9781680836875.pdf?sequence=1

[2] “HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE,” US, June. 2017. [Online]. Available: https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf

[3] Luis Kun, “Protection of the healthcare and public health critical infrastructure and key assets,” Systems Management, IRM College, National Defense University, 300 5th Avenue, SE, Building 62, Fort McNair, Washington, DC 20319 USA. E-mail: KunL@ndu.edu, April 2009. [Online]. Available: https://www.hawaii.edu/csati/summit/Protection_of_The_HC&PH_Kun.pdf

[4] Homeland Security, (2016). *Healthcare and Public Health Sector-Specific Plan.* Washington, D.C: Department of Homeland Security.

[5] Perakslis, E. D. (2014). Cybersecurity in health care. *The New England journal of medicine*, *371*(5), 395.

[6] "Healthcare and Public Health Critical Infrastructure Sector." All Answers Ltd. nursinganswers.net, November 2018. Web. 14 May 2021. [Online]. Available: https://nursinganswers.net/essays/healthcare-public-health-critical-infrastructure-3730.php?vref=1.

[7] Myrsini Athinaiou, “Cyber security risk management for health-based critical infrastructures”
School of Computing, Engineering and Mathematics University of Brighton, Brighton, United Kingdom. [Online]. Available: https://ieeexplore.ieee.org/document/7956566/

[8] Dimitra Liveri, Dr. Athanasios Drougkas, Antigone Zisi, EU Agency for Cybersecurity, “Cloud security for healthcare services”, January 2021.

[9] Cavoukian, A., Fisher, A., Killen, S. et al., “Remote home health care technologies: how to ensure privacy?” Build it in: Privacy by Design, Identity in the Information Societey IDIS, Vol. 3, 2020, pp. 363–378, https://doi.org/10.1007/s12394-010-0054-y

[10] Davenport, T., and Kalakota, R., “The potential for artificial intelligence in healthcare”, Future Healthcare Journal Vol. 6 No 2, 2019, pp. 94-98. doi: 10.7861/futurehosp.6-2-94

[11] Lee Kim, BS, JD, CISSP, CIPP/US, FHIMSS, “Healthcare and cross-sector cybersecurity report”, vol 33- April 2020. [Online] Available: https://www.himss.org/resources/himss-healthcare-and-cross-sector-cybersecurity-report

[12] Jessica Davis, “Biggest Healthcare security threats, Ransomware Trends into 2021” Email: **jdavis@xtelligentmedia.com** [Online] Available: https://healthitsecurity.com/features/biggest-healthcare-security-threats-ransomware-trends-into-2021

[13] Mime Asia Team, “Here are 3 roles of Artificial intelligence in Healthcare” 2019. [Online] Available: https://www.mime.asia/here-are-3-roles-of-artificial-intelligence-in-healthcare/

[14] Amit Dua, Co-Founder at signity solutions, “Role of AI and Machine Learning in Healthcare Industry”, September 11, 2020. [Online] Available: https://www.signitysolutions.com/blog/role-of-machine-learning-ai-in-healthcare/

[15] Health IT Analytics, xtelligent Healthcare media, “Top 12 ways Artificial Intelligence will impact Healthcare” [Online] Available: https://healthitanalytics.com/news/top-12-ways-artificial-intelligence-will-impact-healthcare

[16] Ben Rossi and Adam Spiby, Healthcare Matters, “The future of the internet of things in the healthcare sector” July 19, 2017. [Online] Available: https://www.information-age.com/future-internet-things-healthcare-sector-123467408/

[17] Solanas, A., Patsakis, C., Conti, M., Vlachos, I. S., Ramos, V., Falcone, F. & Martinez-Balleste, A. (2014). Smart health: a context-aware health paradigm within smart cities. *IEEE Communications Magazine*, *52*(8), 74-81.

[18] Justin Snair, “Healthcare and public health critical infrastructure sector”, December 17-31, 2013 open-source issue report, Jan 10, 2014. [Online] Available: https://www.naccho.org/blog/articles/healthcare-and-public-health-critical-infrastructure-sector-december-17-31-2013-open-source-issue-report

[19] Mary Hodges, “The role of local public health in healthcare critical infrastructure protection”, Oct 21, 2015. [Online] Available: https://www.naccho.org/blog/articles/the-role-of-local-public-health-in-healthcare-critical-infrastructure-protection

[20] what-when-how in-Depth Tutorials and Information, “Changing Healthcare Institutions with large information technology projects. [Online] Available: http://what-when-how.com/medical-informatics/changing-healthcare-institutions-with-large-information-technology-projects/

G.P.H. Shihani Tharuka

Born in Colombo 07, Sri Lanka on December 04, 1997. Studying at University of Sri Lanka Institute of Information Technology, Malabe, Sri Lanka. Received the Diploma in PHP/MySQL at University of Sri Lanka Institute of Information Technology, Kollupitiya, Sri Lanka, in 2019. Following BSc (Hons) in Information Technology Specializing in Cyber Security degree, Sri Lanka Institute of Information Technology University, Malabe, Sri Lanka, From February 2019 to February 2023.

She currently works as DATABASE AND SYSTEM OPERATOR at Matara Group of Companies (PVT)Ltd, Colombo 05. Worked as a PRODUCT ASSOCIATOR at Innodata Lanka (PVT)Ltd, Colombo 12. Her primary research interests include Critical infrastructure security in healthcare sector, Artificial intelligence, 5G-toWIFI security vulnerabilities, and Cyber Crimes.

Miss. Tharuka is a member of ISACA community at University of SLIIT. And won first place at school, scoring highest marks in Information and Communication Technology module.