**Sri Lanka Institute of Information Technology**



**Cyber Security Threats and Mitigations in the Healthcare Sector**

**Applied Information Assurance-IE3022**

**B.Sc. (Hons) in Information Technology Specializing Cyber Security**

* **S.A.D.H. Vishwajith**
* **IT19952376**

**Cyber Security Threats and Mitigations in the Healthcare Sector**

S.A.D. Hasintha Vishwajith

Sri Lanka Institute of Information Technology

Faculty of Computing

hasinthavishwajith98@gmail.com

***Abstract: - The increasing connection to existing computer systems has exposed the medical sector to cybersecurity risks from which they were previously protected. For the avoidance of cybersecurity events, it is necessary to understand the complexity of the operational environment as well as to catalog the technological vulnerabilities. Cybersecurity defense is not only a technical issue; it is a richer and more complicated challenge to address. An examination of the variables that lead to such a potentially unsafe environment, combined with the identification of the vulnerabilities, is crucial for understanding why these vulnerabilities persist and what the solution space should look like. This involves technological controls, governance, resilience mechanisms, unified reporting, context expertise, legislation, and standards. It is obvious that a coordinated, proactive approach to handle this complicated problem is necessary. In the meanwhile, patient safety is in jeopardy.***

***Keywords- cybersecurity, security, safety, wireless, risk, medical sector***

1. **INTRODUCTION**

There is a rising worry that the connection of medical devices may directly influence clinical treatment and patient safety. This interconnectedness renders medical equipment vulnerable to security breaches in the same manner as other networked computer systems are vulnerable to cyber-attacks, according to the World Health Organization (WHO). The integration of medical devices, networking, software, and operating systems means that the relative isolation and safety of these devices are challenged. These difficulties are referred to collectively as cybersecurity vulnerabilities. In a world where medical equipment must be approved for safety, this presents a slew of previously unnoticed issues. [1] Health care is a prominent target for cyberattack with 94 percent of health care companies having been the victim of a cyberattack, according to SANS Institute study.

Regulatory authorities have released advice for controlling cybersecurity risks and protecting patient health information. International standards community has assumed lead role in establishing and updating existing standards to address such challenges. New and creative forms of healthcare supported by potential for interoperability, while promoting advances in patient safety. [2] Safeguarding critical infrastructure in the healthcare sector includes not merely anticipating problems, but also removing risks wherever they may exist.

One respondent even went so far as to describe vital infrastructure as "anything that might have an effect on care service or place our patients in danger".

1. **OBJECTIVES**

The goal of this research was to give a review of the literature on cybersecurity and the critical health care sector, including cyber-attacks (related to the topic), and to recommend feasible remedies.

1. **REVIEW OF THE LITERATURE**

The issue of cybersecurity risk connected with medical sector requires framing as it comprises of various and dissimilar components. These include the shift from isolated devices to networked, and the tensions this causes between security and safety; why this is not merely a technological challenge; and the ensuing dispute between regulation and production. Examples of events are presented to show the diversity of the cybersecurity challenge. Traditionally, medical device information flow is unidirectional from the device to the health care practitioner. Remote contact with equipment, however, has become feasible as technology has progressed, and modern devices are networked to monitoring systems and electronic medical record (EMR) systems. [3]

To understand the structure of the vulnerabilities created by this connectivity, it is necessary to recognize that medical devices are no longer a stand-alone component of the clinical care process, and thus are no longer afforded the protection against cybersecurity attacks that stand-alone segregation once provided.

* 1. **Contention between manufacture and regulation**

The conflict between medical device manufacturing and regulation is not a new problem. The present debate surrounding the security of medical equipment mirrors that which happened with critical infrastructure devices over a decade ago. [4] Balancing this conflict with innovation, while concentrating on ensuring effectiveness and safety may be difficult. Rigorous clinical trials are not part of the procedure for approval of all devices, and in both the US and the European Union, this is addressed via pre-market submission and post-market monitoring. [5] However, this does not address non-clinical safety concerns with networked medical equipment. The truth is the frequency and reporting of assaults have risen, and medical equipment are not immune to this.

* 1. **A cybersecurity perspective on the vulnerabilities**

Vulnerability is regarded a vulnerability that may be exploited, be it in hardware, software, firmware, operating systems, medical devices, networks, people, and processes. Risk is estimated by evaluation of the possibility that a danger can materialize along with an assessment of the severity of any potential consequence. Intrinsic in the calculation of risk is the effect of an attack, and the component of security it affects.

* **Harm of cybersecurity vulnerability**

Information security theory specifies the main aims of security protection to be confidentiality, integrity, and availability of information. As such, networked medical equipment are open to the following:

* confidentiality may be endangered from unwanted access owing to inadequate access control mechanisms.
* Integrity may be impacted via improper setup, corruption of data, or illegal modification of information.
* Availability occurs when access to information or a computer is restricted or lost.
  1. **Why are medical devices open to these vulnerabilities**
* It is a fallacy to depend on security via obscurity even if private protocols are utilized for communication. This provides a loophole for reverse engineering from which minimal protection can be provided. Using good and established cybersecurity techniques gives greater protection against cyber-attacks, argues Dr Richard Branson. [6]
* Legacy operating systems and software (usually devices, systems, and software that is over five years old or has been replaced with a new version), and incompatibility across systems creates risks such as misconfiguration and security flaws. This includes risks from non-negotiated interactions with third party software, typically via online interfaces. [7]
* Lack of timely software upgrades and fixes. This is typically where issues with workflow and service interruptions are prevalent. Although health care professionals have explored better patch management, this will remain an ongoing problem in situations where large numbers of devices are utilized. The US Veteran Affairs has explored enhancing patch management for its electronic health records. [8]
* With the growing dependence on information provided in electronic health records (EHRs), the integrity of this information is essential. Web services are a common option for interacting with existing systems, however they frequently include insecurely configured authentication and unencrypted data. This implies that information may be changed while it is transmitted to EMR systems. [7]
* Limited resources and power of medical equipment imply that encryption may slow down medical devices and decrease the useful battery life. [7]
* Achieving a balance among security and privacy objectives and health care usefulness and safety may be difficult. For instance, employing strong encryption and access control methods improve security, but put the patient at more danger in the event of an emergency. [9]
  1. **The recommended approach to Cybersecurity in healthcare**
* **Quality IT at the foundation**

For a health institution to have a solid information security posture, it needs excellent IT: at least a reliable application foundation and IT infrastructure. This is particularly difficult to accomplish in healthcare settings owing to a shortage of human resources, limitations in the budget, a history of underinvestment, and the complicated application area; nonetheless, it is essential. Although there are no defined models or methods for a health institution to utilize in assessing the quality of its IT, there are a few indicators that may provide some insight. For example, a health institution with a solid application foundation does not have helpdesk call-logs that are swamped with break/fix requests and its IT personnel is not concerned mainly with fixing malfunctioning or broken programs. [10]

Information security necessitates the use of configuration management, change management, logging, and monitoring in the IT infrastructure. System maintenance attempts to keep an up-to-date inventory of IT assets and the relationships between them. [11] Change management not only avoids unnecessary service downtime but is also useful during a cyberattack.

* **Preventative and proactive stance**

In the past, hospitals had to postpone or abstain from addressing different security holes in the operating system. There has been a recent effort to market cybersecurity as a business model among medical device and equipment makers. Cybersecurity is not just plugged in as an accident but is now one of the requirements of the design. [12]

Medical device makers must demonstrate that their equipment are able to have upgrades and security fixes deployed throughout their lifetime. The FDA mandates that a "bill of materials" be provided with purchasers of a medical device. These new regulations will apply to manufacturers, who must submit a 510(k)-pre-market filing package to the FDA. [13]

* **Risk-based approach**

Because there is no such thing as perfect cybersecurity, a risk-based strategy based on enterprise risk management is required. Even with quality IT infrastructure and practices, the risk of an attack will always persist.

Risk assessment relies on the identification of at-risk IT assets, emphasized as the first step by the Nist Cybersecurity (CSF) for critical infrastructure. An asset's worth to the business and its vulnerability to risk should define its priority in protective procedures. This involves the evaluation of an incident's effect on data and privacy protection (confidentiality), availability of data, and integrity of the information. [14]

* **Training and awareness**

Human mistake and human error may potentially offer dangers like in the event at Geneva University Hospital (HUG) in October 2019. As people are the weakest link in cybersecurity, health institutions' approaches to cybersecurity should take into consideration the necessity for increasing awareness among all users. In order to reduce risk, the ENISA publication Security and Resilience in Healthcare, among others, recommends providing cybersecurity training. [15]

* 1. **Recommended Cybersecurity measures**
* **Vulnerability/Patch Management**

Exposure and vulnerability analysis includes the discovery, assessment, and mitigation of IT issues. It depends largely on threat-monitoring procedures but also includes all the identifying stages: risk assessment, repair or mitigation measures, and reevaluation.

Risk analysis is at the heart of patch processes: Considering the sensitivity of data on the computer and an enterprise's key operations or assets exposed to an attack. [11]

* **Administrative privileges and multifactorial authentication**

The dangers involved with giving administrative rights to users in health institutions are significant.

According to Cyberhealth’s APT Privileged Account Exploitation study, the overwhelming majority of large-scale assaults that caused substantial damage and expenditures were started via the compromise of a privileged login such as that of a 3rd party provider. [16]

* **Incident response plan**

As cyberattacks have grown more common and significant in recent years, health institutions should develop an incident response and business continuity strategy. Plans should include an agreed upon procedure with the relevant parties identified. [17]

* **Information sharing**

The sharing of possible threats, indications of compromise, best practices, vulnerabilities, and of mitigation measures across stakeholders across public and private sectors is an important step in developing the cybersecurity of healthcare systems. Information sharing promotes situational awareness and a solid knowledge of risks and threat actors, their motives, campaigns, strategies, and methods. [18]

1. **FUTURE RESEARCH**

The FDA and the Department of Homeland Security have announced a joint effort to "improve coordination" in dealing with medical device concerns. In actuality, these discussions have only begun occurring in the last decade, and goods can take that long to reach the market. Manufacturers have not progressed in tandem with hospitals, while there are more discussions about how to make their products more secure.

* 1. **The Challenges of Securing Connected Devices**

Legacy systems provide many cybersecurity problems, but there are additional barriers to protecting medical equipment. Component obsolescence is one that is directly linked to older equipment. “Considering the long development timeframes associated with most devices, it is quite possible that security-related components such as operating systems and microcontrollers may cease to be maintained by the component manufacturer shortly after a medical device hits the market,” Fernando said. [19]

As a consequence, hospital maintenance operations such as security updates are no longer possible. Assume, however, that security fixes are provided by manufacturers. The time and money required to verify these updates on devices is too expensive. [18]

The consequences of a successful breach, such as financial loss and death, draw attention to the following concepts, which are intended to aid companies in establishing a basic cyber strategy.

* Keep security guards up to date.
* create strong, complex passwords, change them on a regularly, and don't allow computers store passwords.
* Encrypt data to prevent illegal use and to guarantee confidentiality.
* Restrict access to sensitive data and preserve the privacy.
* Restrict network access and regulate physical access to data, technological systems and technology, databases, and platforms; protect portable devices; and limit access to the connection.
* distinct information by maintaining isolation, stand-alone servers.

1. **CONCLUTION**

In the health care environment, patient safety will always come before cybersecurity needs. Medical devices are becoming an essential component of medical networks and their security should be an integral component of cybersecurity protection. This will need greater cooperation between medical physicists and IT professionals, as well as collaboration by medical device makers and network suppliers. The cybersecurity vulnerabilities that are associated with medical devices are similar to those associated with any other networked system. Experts believe that shifting the protection of medical devices to more mainstream cybersecurity protection would need the adoption of these devices as conventional connections in network deployment. Health care organizations must understand the cybersecurity vulnerabilities that are already present in their networked medical devices. A coordinated proactive approach that includes standard cybersecurity assessment and control is needed. In the interim, there will inevitably be adverse outcomes for patient safety while a clear, workable process is developed.

1. **ACKNOWLEDGEMENT**

I'd want to express my gratitude to my professor, who is in charge of the Applied Information Assurance module, for his essential supervision, support, and mentorship during the semester. My thanks go to the Faculty of Computing for providing me with the funds to pursue my studies at the Department of Cyber Security, Sri Lanka Institute of Information Technology (SLIIT)

1. **REFERENCES**
2. D.-T. Craigen D, "Defining Cybersecurity.," Technology Innovation Management Review, 2014
3. S. Institute, "Widespread Compromises Detected, Compliance Nightmare on Horizon. Firkins B: 2014. [Accessed June 9, 2015]. Available from: http://www.sans.org/reading-room/whitepapers/firewalls/health-care-cyberthreat-report-widespread-compromises-detected-compliance-ni," Health Care Cyberthreat Report.
4. M. Rule, "US Food and Drug Administration," 2011. [Online]. Available: http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/MedicalDeviceDataSystems/ucm251897.html
5. P. J. K. T. Rinaldi SM, "Identifying, understanding, and analyzing critical infrastructure interdependencies. Control Systems," 2001.
6. R. R. Curfman GD, "Medical Devices," Balancing Regulation and Innovation. N Engle J Med, 2011.
7. C. S. R. B. Burleson W, "Proceedings of the 49th Annual Design Automation Conference; San Francisco, CA.," Design challenges for secure implantable medical devices, 2012.
8. W. P. McCauley V, "Trusted interoperability and the patient safety issues of parasitic health care software," 9th Australian Information Security Management Conference. Perth: secau-Security Research Centre, Edith Cowan University, 2011.
9. A. H, "VA Addresses medical device security," 2011. [Online]. Available: http://www.healthcareinfosecurity.com/interviews.php?interviewID=1163.
10. W. P. McCauley V, "Trusted interoperability and the patient safety issues of parasitic health care software," 9th Australian Information Security Management Conference. Perth.
11. "A guide to service asset and configuration management. Oxford: UCSIA ITIL," 2014. [Online]. Available: https://www.academia.edu/29873674/ITIL\_guide\_to\_SA\_and\_CM\_management\_pdf.
12. V. D., "A practical methodology for implementing a patch management process.," Swansea: SANS Inst Inf Secure Read Room.
13. S. a. a. M. D. (. S.), "Clinical Evaluation Guidance for Industry and Food and Drug Administration Staff," 2017. [Online]. Available: https://www.fda.gov/media/100714/download.
14. M. V, "Korah I. Lack of security of networked medical equipment in radiology. Am J Roentgenol.," 2015.
15. E. I. R. G. Center, "Internet of Things. Connected medical & health devices and connected vehicles. Workshop report. Lausanne," 2017.
16. J. T. Frederick B, "a systematic review of modern threats and trends," Cybersecurity in healthcare, 217.
17. "New Report Connects Privileged Account Exploitation to Advanced Cyber Attacks," 2013. [Online]. Available: https://www.cyberark.com/press/new-report-connects-privileged-account-exploitation-advanced-cyber-attacks/.
18. ENISA, "SMART Hospitals," https://doi.org/10.2824/28801, 2013.
19. W. D. o. H. Security, "Healthcare and Public Health Sector-Specific Plan.," 2015. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf.
20. B. M. R. B. e. a. Kramer DB, " An Analysis of FDA Post market Surveillance," Security and Privacy Qualities of Medical Devices, 2012.
21. **ATHOR PROFILE**

**S.A.D. Hasintha Vishwajith** was born in Kottawa, Western Province, **Sri Lanka** in 1998. He is 3rd year Information Technology undergraduate **Specializing in Cyber Security** degree at **Sri Lanka Institute of Information Technology (SLIIT)** in Malabe. He went to Kottawa Dharmapala Vidyalaya for **primary education**. For **advanced level education**, he went to Pannipitiya Dharmapala Vidyalaya.