Forum:	Commission on Science and Technology for Development
Issue:	Preventing Hacking of Surgical Robots and Medical Infrastructure
Student Officer:	Ioannis Pitsiavas
Position:	President

PERSONAL INTRODUCTION

Dear delegates,

I am delighted to welcome you all to the 13th Platon School Model United Nations conference, and specifically to the Commission on Science and Technology for Development committee (CSTD).

My name is Giannis Pitsiavas, I am 17 years old and an IB year 2 student at Geitonas School. I started MUN when I transferred schools, going from a public school to my current one, and since then I have been to ten conferences as a delegate in multiple committees, thus, I am fairly confident for my ability to tackle various topics from different angles, which is exactly what we are looking for in our committee. This will be my second time chairing and my first as the President of a committee. I am looking forward to meeting you all, hearing your opinions on the topics of our committee, and of course, coordinating the debate in the best way that I can.

CSTD is a subsidiary body of the Economic and Social Council (ECOSOC), holding annual forums for discussion between Member States, on issues affecting science, technology and development. Technology and science are advancing on fast rates, and humanity must keep up with them in order to advance and achieve sustainability -a goal set by the United Nations. This is exactly what the CSTD does. It contributes by sharing and transferring knowledge, skills and solutions in science and technology fields, thus making it a vital part of the UN.[1]

You can always reach me at the following email address: ip11675@geitonas.edu.gr. If you need assistance or have any questions regarding my topic, please do not hesitate to contact me. Of course, aside from this guide, you need to conduct your own additional research to gather information on the topic and on your country's stance on it.

[1] "About the CSTD." UNCTAD, unctad.org/topic/commission-on-science-and-technology-for-development/about. Accessed 09 Nov. 2023.

I hope that there will be a fruitful debate that will help you gain new knowledge leaving the conference. I am looking forward to meeting you all.

Kind regards,

Ioannis Pitsiavas

INTRODUCTION

In a time characterized by remarkable developments in technology and innovation, our quest for progress has revealed a significant paradox that overlaps with the vital field of healthcare.

The paradoxical nature of progress becomes increasingly evident when one contemplates the significant advancements achieved in the field of modern medicine. The arrival of surgical robots has significantly transformed the healthcare industry, offering a new level of precision and efficiency. However, in the current era of advanced medical technology, we are confronted with an unanticipated obstacle - the susceptibility of our medical infrastructure to potential hacking risks. As the healthcare industry continues to advance its capabilities (the logistic processes in hospitals, the data management or even the way physicians practice medicine), it becomes imperative to acknowledge the potential for harmful use of these innovations which would not only result in the -unintentional- malpractice of some doctors, but it may even result in the death of thousands of patients.

The theme of this conference, “The Paradox of Progress”, is truly highlighted in this topic. As technology and science advances, and seemingly helps more people with its new and enhanced features, the devastating effects that may come up, have not been taken into consideration. So, is it really important to develop our understanding and the way that we practice medicine by risking patients’ lives?

In the following discussion, we will delve into the complex links of this paradox. This study guide aims to explore the remarkable capabilities of surgical robots and the profound impact of interconnected medical infrastructure. At the same time, we will address the urgent and practical demand to safeguard these systems against cyber threats that have the potential to compromise patient well-being and the effectiveness of healthcare practices. The investigation into the topic of "Preventing Hacking of Surgical Robots and Medical Infrastructure" illustrates the inherent conflict of technological advancement, serving as an important reminder that as we develop new innovations, it is imperative to maintain a state of constant monitoring, strength, and dedication to protecting the fundamental pillars on which our healthcare systems rely.

DEFINITION OF KEY TERMS

Healthcare Infrastructure

Healthcare infrastructure involves the individuals, the non-material facilities, and the buildings, that are required to deliver world-class healthcare.[2]

Robotic Surgery

"Robotic surgery allows doctors to perform more types of complex procedures with precision, flexibility and control than is possible with conventional techniques. Robotic surgery is usually associated with minimally invasive surgery – procedures performed through tine incisions. It is also sometimes used in certain traditional open surgical procedures." [3]

da Vinci system

The da Vinci surgical system gives the surgeon an advanced set of instruments to use in performing robotic assisted minimally invasive surgery. The surgeon performs surgery with da Vinci by using instruments that he or she guides via a console. This robotic system is not autonomous, and it can only be operated by humans. [4]

Raven-II system

The RAVEN is a proven, third generation surgical robotics testbed. Yet, it is not approved by the FDA and thus, is not used in public settings inside hospitals. This robotic system can perform autonomous surgery, assisted by machine learning (AI) which helps it collect data from each surgery performed, but still it can be used by surgeons. [5]Also, it is a teleoperated surgical system, which means that surgeons can utilize it remotely, no matter where they are.[6]

Cybersecurity

"Cybersecurity is the application of technologies, processes, and controls to protect systems, networks, programs, files, devices, and data from cyber-attacks." [7]

Data Privacy

"Data privacy involves the proper handling of sensitive data, including personal data but also financial and intellectual data, in order to satisfy regulatory requirements and protect privacy and immutability." [8]

---

[2] Contributor, Guest. "Investing into Health Care Infrastructure." Facility Executive Magazine, 21 June 2021, facilityexecutive.com/investing-into-health-care-infrastructure/. Accessed 10 Sept. 2023.
[3] "Robotic Surgery." Mayo Clinic, Mayo Foundation for Medical Education and Research, 6 May 2022, www.mayoclinic.org/tests-procedures/robotic-surgery/about/pac-20394974.
[4] "About Da Vinci Systems." Intuitive.Com, Intuitive, www.intuitive.com/en-us/patients/da-vinci-robotic-surgery/about-the-systems.
[5] "Robotic Database - Robotic Platform." TERRINet, Imperial College London, 10 Nov. 2022, www.terrinet.eu/robotic_database_show_platform/?id=92.
[6] Aliouche, Hidaya. "What Is Remote Surgery/Telesurgery?" News, University of Manchester, 11 Nov. 2021, www.news-medical.net/health/What-is-Remote-SurgeryTelesurgery.aspx.
[7] "Cyber Security." IT Governance, www.itgovernance.co.uk/what-is-cybersecurity.
[8] "What Is Data Privacy?" SNIA, www.snia.org/education/what-is-data-privacy.

Network Security

"Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft. It involves creating a secure infrastructure for devices, applications, and users to work in a secure manner." [9]

Malware

"Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems. Hostile, intrusive, and intentionally nasty, malware seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device's operations." [10]

Incident Response

"Incident response (IR) is the process by which an organization handles a data breach or cyberattack. It is an effort to quickly identify an attack, minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents."[11]

Cybersecurity Risk Assessment

"A cybersecurity risk assessment evaluates an organization's ability to protect its information and information systems from cyber threats. It identifies, assesses, and prioritizes cyber risks to information and systems that are in use by a company." [12]

Ransomware attack

"Ransomware is a type of malware that threatens to publish or block access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker." [13]

HIPAA

"The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge." [14]

Blockchain

"A blockchain is a distributed database that maintains a continuously growing list of ordered records, called blocks. These blocks are linked using cryptography. Each block contains a cryptographic record of the previous block, a timestamp, and transaction

---

[9] "What Is Network Security?" Cisco, 4 July 2023, www.cisco.com/c/en/us/products/security/what-is-network-security.html.

[10] "What Is Malware? Malware Definition, Types and Protection." Malwarebytes, www.malwarebytes.com/malware.

[11] "What Is Incident Response? Strategy, Process, Templates & More." Cynet, 20 Aug. 2023, www.cynet.com/incident-response/.

[12] "Cybersecurity Risk Assessment: Components + How to Perform." KnowledgeHut, www.knowledgehut.com/blog/security/cybersecurity-risk-assessment.

[13] "What Is Ransomware? - Definition, Prevention & Examples: Proofpoint Us." Proofpoint, 16 Aug. 2023, www.proofpoint.com/us/threat-reference/ransomware.

[14] "Health Insurance Portability and Accountability Act of 1996 (HIPAA)." Centers for Disease Control and Prevention, 27 June 2022, www.cdc.gov/phlp/publications/topic/hipaa.html.

data. A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network." [15]

Ethical Hacker

"An ethical hacker, also known as a 'white hat hacker', is employed to legally break into computers and networks to test an organization's overall security."[16]

BACKGROUND INFORMATION

Surgical Robots and robotic-assisted surgeries

"Robotic Surgery is the revolution of the 21st century, opening new horizons in the field of Medicine. Robotic assistance has made possible the removal of many constraints regarding operations in some difficult fields of surgery."[17]

This is how most people in our society view robotic surgeries. Without doubt, surgical robots have shown great importance in the field of medicine, with robotic assisted surgeries (RAS) gaining ground as the years pass, as seen in Figure 1. The most notable characteristic of RAS is the small incisions made, resulting in less pain and scarring, alongside multiple other advantages.[18]

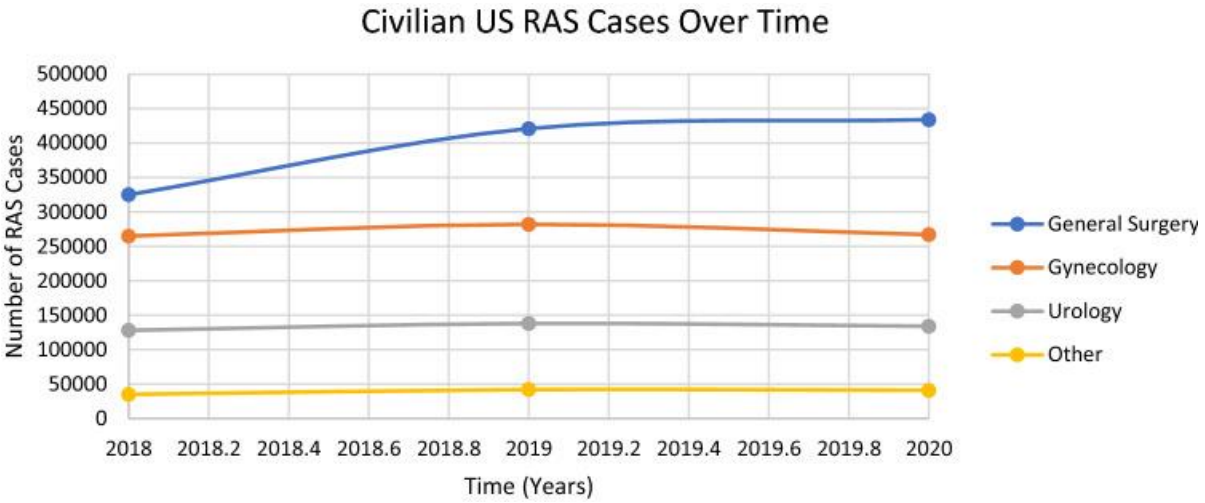

Figure 1: The upward trend in robot assisted surgeries (RAS) in the past years[19]

[15] "What Is Blockchain and How Does It Work?" Synopsys, www.synopsys.com/glossary/what-is-blockchain.html.
[16] "What Is an Ethical Hacker? And How to Become One - Crowdstrike." Crowdstrike.Com, 7 July 2023, www.crowdstrike.com/cybersecurity-101/ethical-hacker/.
[17] "Robotic Surgery." Our Services, athensmedicalgroup.com/critical-illness/robotic-surgery/.
[18] "Benefits of Robotic Surgery." UC Health, www.uchealth.com/services/robotic-surgery/patient-information/benefits/.
[19] Rizzo, Kayla R., et al. "Status of Robotic Assisted Surgery (RAS) and the Effects of Coronavirus (COVID-19) on Ras in the Department of Defense (DOD) - Journal of Robotic Surgery." SpringerLink, Springer London, 23 June 2022, link.springer.com/article/10.1007/s11701-022-01432-7.

The process of reaching this stage, where millions of RAS are being performed every year, was not short. The idea of robots begun in 1920, when a Czech writer established the concept of robots, just not in the context that it is used today. In 1970, NASA and the USA military started experimenting with the idea of telesurgery for different purposes. NASA wanted to be able to support astronauts whilst the USA military wanted to provide help to the soldiers in the battlefield without risking the life of doctors. The first robotic surgery was performed in 1985, with a robot called PUMA 560, in a brain biopsy procedure. Its purpose was to just reduce movement of the surgeon's hand in order to minimize errors. With a series of advancements, we reach today, where we can perform surgeries without the doctor even being in the same room as the patient.[20]

Are robotic surgeries so safe though? Considering the aforementioned, someone would believe that throughout all these years, robotically assisted surgeries are error free. However, this is not the case. This will be analysed in the following sections.

Da Vinci system

The da Vinci Surgical System is an advanced robotic surgical system that utilizes a minimally invasive surgical technique. The system is produced by the company Intuitive Surgical, while the technology can be utilized in the context of prostatectomies, along with heart valve repair, kidney surgeries, and gynecologic procedures.

The da Vinci System comprises a surgeon's console, normally located within the same space as the patient, and a patient-side cart equipped with three to four interacting robotic arms (number of arms varies based on the model), which are operated from the console. The upper part of the body has the capacity to manipulate various items, serving as instruments such as scalpels, scissors, bovies, or graspers. The final limb handles the 3D cameras. The surgeon utilizes the controls of the console in order to manipulate the robotic arms of the patient-side cart. The operation of the system generally demands the presence of a human operator.

The da Vinci Surgical System was granted clearance by the Food and Drug Administration (FDA) in the year 2000 for utilization in various surgical procedures. These include urologic surgical procedures for both adults and pediatric patients, general laparoscopic surgical procedures, gynecologic laparoscopic surgical procedures, general non-cardiovascular thoracoscopic surgical procedures, and thoracoscopically assisted cardiotomy procedures.[21]

The da Vinci Surgical System offers a variety of advantages. Notably, it stands as a paragon of precision in surgical interventions, alleviating concerns related to human

[20] Tsclinic. "The History of Robot-Assisted Surgery." The Surgical Clinic, thesurgicalclinics.com/history-of-robot-assisted-surgery/.
[21] "Da Vinci Surgical System." Da Vinci Surgical System - an Overview | ScienceDirect Topics, www.sciencedirect.com/topics/medicine-and-dentistry/da-vinci-surgical-system.

hand tremors and enhancing the finesse required for intricate procedures. The system's remarkable imaging capabilities provide surgeons an immersive, high-definition 3D view of the surgical site, a feat especially invaluable in complex surgeries. Furthermore, its main attribute resides in enabling minimally invasive procedures, which helps to reduce incision sizes, mitigate scarring, and speed up patient recovery periods. With its ability to manage blood loss and accelerate hospital discharges, the da Vinci system constitutes significant progress in surgical care. The clinical value of this intervention is shown by its effectiveness in facilitating a quicker return of regular daily activities.

However, the da Vinci Surgical System does have certain limitations. One important consideration is to the significant financial commitment associated with it, which includes costs for acquisition, ongoing maintenance, and extensive training requirements. As a result, this may possibly restrict its availability inside healthcare organizations. The complex characteristics of this technology result in a steep learning curve, which can result in longer surgical durations during the early phases of its implementation. Furthermore, it is important to note that the system's inherent shortcoming is mostly associated with its reduced ability to provide sensory input, which is the ability of the machine to be used by the doctors in a way similar to that of their hands -by sensing the smallest hand movements of the doctor as responding appropriately. This deficiency results in surgeons being deprived of the tactile signals that are essential in traditional surgical procedures. In addition, the complex arrangement and calibration processes necessary prior to each surgical procedure have the potential to result in extended periods of time required. The suitability of the da Vinci system varies depending on the specific surgical treatment, as certain interventions may be more effectively performed using traditional techniques or alternative technologies. In conclusion, the possibility of technology malfunctions occurring during surgical procedures emphasises the need for robust backup plans and alternative manual procedures.[22]

RAVEN-II system

The core components of the Raven platform emerged in 2005 as a component of a DARPA (Defense Advanced Research Projects Agency) project focused on the prospective advancements in military medicine. The Raven system was developed by a group of academics, led by Professor Blake Hannaford, who specializes in robotics at the University of Washington in Seattle. This system was specifically created for laparoscopic surgery and is intended to be mobile in nature, meaning that anyone would be able to carry it with them to an expedition or a mission -when referring to the military. The objective was to improve the modularity of Raven and making it lighter in weight, with the aim of increasing its portability relative to the larger surgical robots commonly employed in hospital settings, hence enabling reassembly by a limited team of individuals. The development of the Raven II surgical robot was

[22] "Da Vinci Surgical System ." Intuitive.Com, www.intuitive.com/en-us/patients/da-vinci-robotic-surgery/about-the-systems.

undertaken as a joint research initiative funded by the National Science Foundation, with the aim of advancing the field of surgical robotics. The Raven II platform was utilized by a total of seven universities, including Harvard University, Johns Hopkins University, University of Nebraska, University of California, Santa Cruz, University of California, Berkeley, and University of Washington. The laboratories conducted investigations on various issues pertaining to surgical robots and associated technologies, and afterwards shared their experiences and advancements utilizing the Raven system as a shared platform. Telesurgery tests utilizing the Raven system have entailed the engagement of a surgeon situated remotely, who assumes control of the robot in challenging environments, such as underwater settings within a submarine pod or amongst high desert temperatures.[23]

The RAVEN-II surgical system has a large variety of advantages. Yet, we must keep in mind that this system was not created for usage in a hospital setting, but rather, in areas where high-end healthcare cannot reach and namely, the battlefields, under extreme conditions. This is believed to be one of the reasons why the FDA has yet to approve this system, because it has not been tested properly. And this is a main difference between the da Vinci and the RAVEN-II systems. One has been used extensively in the past decade with the FDA's approval, while the other has only been experimented with by research institutes. Another key difference is that the da Vinci system was created to be handled by specialists that are located in the same room as the patient who they operate on. The RAVEN-II system, on the other hand, was created for the purpose of specialists operating remotely on the patient, or under extreme conditions. Both could be used for teleoperated surgeries. This became a concern to some people, and the following question arose: could someone hack these systems and cause harm?

Robotic-Assisted surgeries

Teleoperated surgery, commonly known as telesurgery, is an advanced medical technique that enables surgeons to do surgical interventions on patients situated at a distant location. The application of sophisticated robotic systems and telecommunications infrastructure for the remote manipulation of surgical tools by a surgeon, ensuring a high level of precision and accuracy. Telesurgery commonly entails the utilization of a robotic surgical system by a surgeon who is situated in a distant location, while the patient is physically situated within the operating room. The actions performed by the surgeon are converted into equivalent motions of robotic arms, so enabling precise and least intrusive surgical procedures. Telesurgery exhibits potential in enhancing accessibility to specialist surgical proficiency, particularly in geographically isolated or inadequately served regions, as well as facilitating surgical interventions in emergency scenarios.

Telesurgery presents a number of appealing advantages. Firstly, telemedicine has the potential to overcome geographical obstacles, thereby facilitating patients in distant

[23] Team, Robots. "Raven II." ROBOTS, 18 May 2018, robotsguide.com/robots/ravensurgical.

or underserved areas to avail themselves of proficient surgical care provided by skilled surgeons situated in urban hubs. This initiative enhances the availability of specialist medical knowledge and mitigates disparities in healthcare. Moreover, the implementation of telesurgery facilitates expedited reaction times in emergency situations since proficient surgeons are able to offer instructions and conduct surgical procedures from a remote location when necessary. In addition, the utilization of robotic surgical systems can significantly improve surgical outcomes and mitigate the potential for human errors by virtue of their enhanced precision and stability. Minimally invasive operations conducted via telesurgery frequently yield advantages such as diminished incisions, decreased scarring, and expedited patient recovery periods.[24]

Nevertheless, telesurgery is not devoid of its obstacles and drawbacks. Apart from the unreliability of the surgical systems that have not been tested to their limits, and the astronomical costs to acquire and maintain these machines, and train the professionals to use it, there is one very significant problem. Namely, the potential of cybersecurity breaches. The utilization of digital communication and robotic systems in telesurgery introduces a possible vulnerability where the system may be susceptible to unauthorized access or control, should it be compromised through hacking. The preservation of security and integrity within telesurgery systems is of paramount importance in order to mitigate potential dangers. However, studies show that these surgical systems have not yet been fully developed in order to be teleoperated.

In a study published by the University of Washington in 2015, researchers were able to hijack the RAVEN-II system with ease. The reason why they used this specific system was because the RAVEN-II has its servers public, and thus, an attack is more than possible to occur. The FDA-approved surgical systems -like the da Vinci- use private servers, which makes a cyberattack less luckily to happen, but still there is the possibility of an attack happening in the future. [25]

To this day, fortunately, we have not seen any cases of hacking surgical systems in hospitals. Nonetheless, this is a risk that we should not be taking, and it is very easy to ensure that an attack will not occur -which would make systems like RAVEN-II more likely to be approved by the FDA and thus, we would have a broader availability of robotic assisted surgeries (RAS). According to researchers from the University of Washington: “In the Raven II, we were able to breach several concerning elements of the system over a wide attack surface, and some extremely efficiently (with a single packet). Yet, some of these attacks could have easily been prevented by using well-

[24] Choi, Paul J, et al. “Telesurgery: Past, Present, and Future.” Cureus, U.S. National Library of Medicine, 31 May 2018, www.ncbi.nlm.nih.gov/pmc/articles/PMC6067812/.
[25] Langston, Jennifer. “UW Researchers Hack a Teleoperated Surgical Robot to Reveal Security Flaws.” UW News, 7 May 2015, www.washington.edu/news/2015/05/07/uw-researchers-hack-a-teleoperated-surgical-robot-to-reveal-security-flaws/.

established and readily available security mechanisms, including encryption and authentication."[26]

Medical/Healthcare Infrastructure

Healthcare stakeholders

Patients must be aware of secure communication methods with healthcare professionals. Also, patients must be aware of the confidentiality and safety policies and know how to protect their information if they interact virtually with their healthcare providers, whether through a telehealth platform, e-visits, encrypted messaging, or another method.

The workforce members are another type of stakeholder in this field that must be aware of the healthcare organization's privacy and security rules. For healthcare cybersecurity, regular security awareness training is crucial so that staff employees are informed about risks and know what to do in the event of actual security incidents. Additionally, employees must be aware of who to turn to with inquiries or issues. In essence, employees can serve as the cybersecurity team's eyes and ears. Understanding what is working and what is not working in the attempt to secure the information technology infrastructure and data can aid the cybersecurity team.[27]

Intangible facilities

Intangible facilities are essential in the modern healthcare scenario. These digital resources are crucial elements of the healthcare infrastructure, greatly enhancing patient care, facilitating communications, and maintaining the accuracy of vital healthcare data.[28]

Electronic Health Records (EHRs) stand out as a key component of these intangible services. EHRs act as sophisticated data warehouses for complete patient information, containing a wide range of information such as thorough medical histories, accurate diagnoses, prescription schedules, detailed treatment plans, and precise test findings. They essentially take the form of computerized collections of patients' medical histories. The digital form of EHRs, which grants improved care coordination capabilities and enhances patient safety, is a defining characteristic of these systems.[29] Notably, inside this electronic environment, healthcare practitioners may easily access and manage patient data, improving the continuum of care. This digital

[26] Bonaci, Tamara, et al. "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats against Teleoperated Surgical Robots." arXiv.Org, 12 May 2015, arxiv.org/abs/1504.04339.
[27] Epalm. "Cybersecurity in Healthcare." HIMSS, 16 Dec. 2021, www.himss.org/resources/cybersecurity-healthcare.
[28] Rider EA;Comeau M;Truog RD;Boyer K;Meyer EC; "Identifying Intangible Assets in Interprofessional Healthcare Organizations: Feasibility of an Asset Inventory." Journal of Interprofessional Care, U.S. National Library of Medicine, pubmed.ncbi.nlm.nih.gov/30415591/.
[29] "What Is an Electronic Health Record (EHR)?" What Is an Electronic Health Record (EHR)? | HealthIT.Gov, 10 Sept. 2019, www.healthit.gov/faq/what-electronic-health-record-ehr.

environment reflects a well-balanced healthcare symphony, orchestrating the collection and distribution of patient data, enabling well-informed decision-making, and ultimately raising healthcare standards.[30]

Effective communication is vital for all healthcare organizations, thus, email and other communication systems play an important role in this regard. The said systems contribute to the internal and external communications, supporting healthcare providers in caring out multiple processes such as scheduling appointments, communicating with patients, sharing critical medical information etc..[31]

Medical imaging has been transformed, with digital systems changing the way we store, manage, and interpret vital medical images such as X-rays, MRIs, and CT scans. Radiology departments in hospitals have been extremely benefited by the Picture Archiving and Communication Systems (PACS), which improved accessibility and aided in diagnosing patients.[32]

Pharmacy Information Systems (PIS) have a main goal of optimizing the drug dispensing system, enhancing inventory management inside healthcare organizations, and facilitating the monitoring of prescription data collected by physicians. Drug mistakes gets minimized and patient safety is ensured, in healthcare organizations that have the said systems in place.[33]

Clinical Decision Support Systems (CDSS) are pivotal tools that offer healthcare practitioners information that is based on evidence, alongside with recommendations to help in the process of decision-making. These systems greatly contribute to the improvement of diagnosing accurately and assists in the development of treatment programs.[34]

Telemedicine and telehealth platforms have been used by healthcare organizations for the past years, and more prominently in the context of delivering healthcare services to rural areas that are hard for doctors to approach in any other way. These areas vary from villages in eastern countries that are far away from big cities, to small communities in the western world where people may need specialized doctors that are not available in their area. Digital solutions facilitate remote meetings serving multiple purposes,

[31] "Communication Systems in Healthcare." HIPAA Journal, 14 Dec. 2022, www.hipaajournal.com/communication-systems-in-healthcare/.
[32] Charles, Megan, et al. "What Is PACS (Picture Archiving and Communication System)?: Definition from TechTarget." Health IT, TechTarget, 30 Aug. 2018, www.techtarget.com/searchhealthit/definition/picture-archiving-and-communication-system-PACS.
[33] "What Are PIS Systems?" What Are PIS Systems? | Nev's Ink, 3 Sept. 2020, nevsink.com/what-are-pis-systems-va-30.html.
[34] Sutton, Reed T., et al. "An Overview of Clinical Decision Support Systems: Benefits, Risks, and Strategies for Success." Npj Digital Medicine, vol. 3, no. 1, 2020, doi:10.1038/s41746-020-0221-y.

telemonitoring, and virtual care, providing patients the convenience of accessing healthcare services from their respective places.[35]

Finally, ensuring the protection of patient data is of utmost importance, hence necessitating the implementation of comprehensive data security and privacy measures within intangible infrastructures. The aforementioned elements consist of cybersecurity measures, encryption techniques, access restrictions, and detailed rules that are specifically devised to safeguard patient data from unwanted access or breaches.

All of these intangible assets are the ones at greatest risk of being hacked. As we discussed earlier, while there is the chance for surgical robots to be hacked, this has not happened yet. However, as we will see later on, there have been several instances of hacking this kind of healthcare/medical infrastructure, since many times, the security measures are out of date (Legacy systems).

Cybersecurity Practises in the field of healthcare

Key challenges and considerations in Healthcare Cybersecurity

The preservation of information and cybersecurity in the healthcare sector are of utmost importance in today's society, given the prevalence of digital systems. Such precautions are crucial for ensuring the smooth functioning of organizations. Many medical facilities possess a range of specialized hospital information systems, including electronic health record (EHR) systems, e-prescribing systems, practice management support systems, clinical decision support systems, radiology information systems, and computerized physician order input systems. Furthermore, it is important to ensure the protection of numerous devices that constitute the Internet of Things. These include smart elevators, smart heating, ventilation and air conditioning (HVAC) systems, infusion pumps, remote patient monitoring devices, and several more examples. The following examples illustrate other assets commonly found within medical enterprises, in addition to those already stated.

Email serves as a main mode of communication within healthcare companies. Various types of information are exchanged, generated, received, sent, and preserved within electronic mail networks. The storage capabilities of mailboxes typically increase as individuals save a wide range of valuable information, including intellectual property, financial data, patient records, and several other types of information. Consequently, ensuring the security of email communications holds significant importance within the field of healthcare cybersecurity.

[35] Lutkevich, Ben, et al. “What Is Telehealth (Telemedicine)?: Definition from TechTarget.” Health IT, TechTarget, 24 Feb. 2023, www.techtarget.com/searchhealthit/definition/telemedicine.

Hacking poses a significant concern. Hacking is the primary cause of a majority of noteworthy security-related incidents. Random users may inadvertently engage with a misleading hyperlink or access a fraudulent attachment embedded within a fraudulent email, so exposing their computer systems to the entry of malware. In specific cases, the propagation of malware over the computer network to additional computer systems may occur. The scam email has the potential to extract sensitive or confidential information from the recipient. Emails that are fraudulent have proven to be highly efficient in their ability to deceive patients, often leading them to engage in desired actions, such as disclosing sensitive or private information, interacting with dangerous links, or accessing unsafe attachments. Therefore, it is crucial to implement consistent security awareness training in order to successfully combat hacking efforts.

The damaging of a computer or device may occur as a result of unauthorized physical access as well. One typical example is the utilization of physical means to jeopardize a device's security. The act of physically exploiting a device has the potential for bypassing the technical controls that have been implemented. The physical security of a device is essential in order to protect its functionality, appropriate setup, and data integrity.

An illustration can be found in the act of leaving a laptop unsupervised during travel or when working in another location. Careless behaviours have the potential to result in the unauthorized acquisition or misplacement of the laptop. Another instance that can be cited is an "evil maid" assault, when a device undergoes subtle modifications, enabling subsequent unauthorized access by cybercriminals. This may involve the installation of a keylogger, which quietly extracts sensitive information, including credentials.

Legacy systems refer to systems that have ceased receiving support from the manufacturer. Legacy systems involve a variety of components, such as software and operating systems, among others. A notable obstacle encountered in the sector of healthcare cybersecurity is to the high prevalence of legacy systems inside numerous enterprises. One notable drawback of legacy systems is their lack of manufacturer support, resulting in a shortage of security patches and other updates.

Legacy systems are often found in organizations due to the high cost associated with upgrading them or the unavailability of an upgrade option. Operating system makers have the option to discontinue support for certain systems, while healthcare institutions may have limitations in their cybersecurity budget, hindering their ability to upgrade to currently supported

versions. Thus, it is common for medical devices to possess legacy operating systems.[36]

Cybersecurity in Healthcare, laws and regulations

The foundation of every healthcare cybersecurity program is risk assessment. Before taking any steps to assist manage risk, risk must first be evaluated. Risk assessment must take into account variables including likelihood of occurrence, impact on the organization, and risk priority. Regular risk assessments, at least once a year, should be carried out or reviewed.

Every healthcare institution should have both fundamental and sophisticated security measures in place. By doing this, defence-in-depth can be ensured, such that if one control fails, another will take its place. As an illustration, a virus might breach a company's firewall but be stopped by an anti-virus program. But not every security incident can be avoided, depending on the expertise of the person that is trying to harm that healthcare organization. Here, blocking and tackling become important. For healthcare cybersecurity, a strong incident response plan is essential so that any security issues are either prevented or dealt with quickly and effectively.

A few basic security controls include encryption at rest, email gateways, data loss prevention, backup and restoration of files and data, and antivirus software.

Furthermore, for covered entities and business associates, the Health Insurance Portability and Accountability Act (HIPAA) is a legal obligation in the United States. The HIPAA Privacy Rule, Security Rule, and Breach Notification Rule make up HIPAA. Health plans, healthcare clearinghouses, and healthcare providers that send any health information electronically in conjunction with transactions for which the US Department of Health and Human Services has developed guidelines are considered covered entities. Similarly, Canada has the Personal Information Protection and Electronic Documents Act (PIPEDA) which applies to private-sector organizations across Canada that collect, use or disclose personal information in the course of a commercial activity. Hospitals are generally governed by provincial laws in Canada, but PIPEDA may apply in certain instances.[37]

Case studies

One would expect that as years progress, our security systems would get enhanced as well, leading to fewer cyberattacks on the intangible facilities of the medical industry. However, that was not the case, mainly because whilst we are trying to develop and progress our knowledge on medicine, we forget that it is linked with other areas that

[36] Epalm. "Cybersecurity in Healthcare." HIMSS, 16 Dec. 2021, www.himss.org/resources/cybersecurity-healthcare.
[37] Epalm. "Cybersecurity in Healthcare." HIMSS, 16 Dec. 2021, www.himss.org/resources/cybersecurity-healthcare.

are essential for the smooth operation of hospitals. In fact, up until this year, we had an increasing trendline on the number of data breaches.

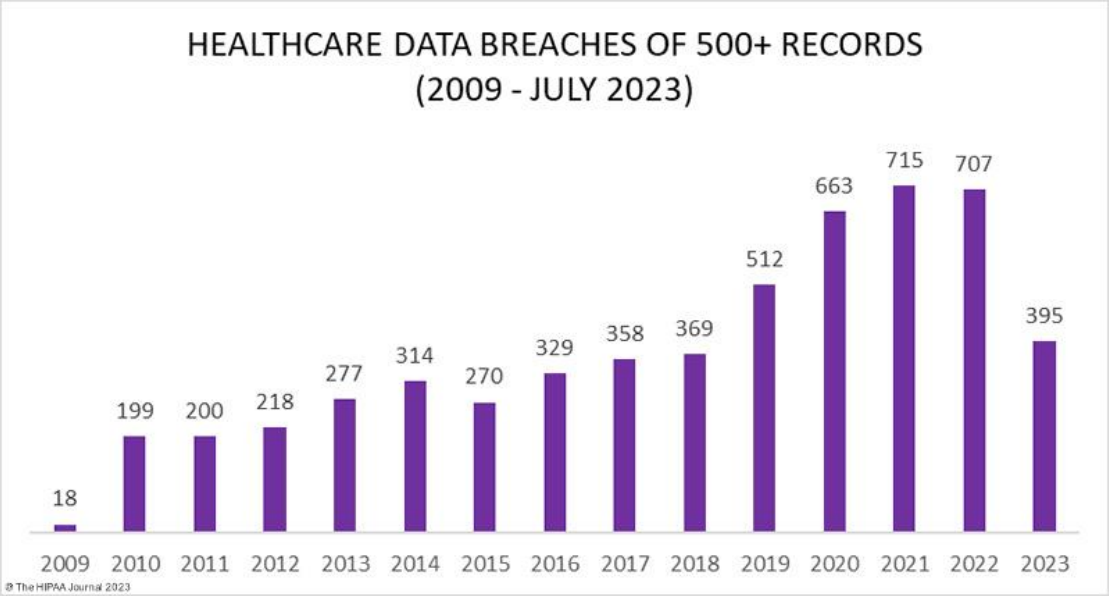

Figure 2: Number of data breaches in the past years[38]

WannaCry Ransomware Attack

The May 2017 occurrence of the WannaCry ransomware attack gained recognition due to its substantial effects on the EHRs and other intangible facilities of healthcare organizations, namely targeting the National Health Service (NHS) in the United Kingdom. The occurrence of this attack signified an important turning point in the convergence of cybersecurity and healthcare.

Even though the location of the group of hackers that attacked the NHS remains unknown, the healthcare industry globally was affected. WannaCry ransomware made patient files inaccessible to healthcare providers, and there was the potential risk of exposure of this sensitive medical information. Furthermore, the patient care was delayed, since the patient records were locked and healthcare providers needed to access crucial patient data, which impacted the timeliness and quality of care. Lastly, patients from all around the world lost their trust when it came to the confidentiality of their medical information, which had long-lasting effects, with elder people specifically not wanting to give their medical history to their new doctors/nurses.

This is the most well-known example of cyberattack/hacking of the medical infrastructure. Healthcare organizations after this attack, started slowly

[38]Murray-Watson, Author: Rebecca. “Healthcare Data Breach Statistics.” HIPAA Journal, 7 Sept. 2023, www.hipaajournal.com/healthcare-data-breach-statistics/.

renewing their cybersecurity capacities, but even today, we are a long way from being completely safe.[39]

SingHealth Data Breach

The summer of 2018 was a hard period for the nation of Singapore and its people. For about a week, from 27th June to 4th July, unidentified state actors were able to overcome all of the cybersecurity measures that had been taken by SingHealth, and as a result, they stole approximately 1.66 million patient records that had to do with their treatment, and on top of that, a large proportion of these stolen data was personal information of patients that visited outpatient clinics under the supervision of SingHealth, such as names, National Registration Identity Card (NRIC) numbers, addresses, date of births, race, gender etc.. [40] Singapore Health Services, commonly known as SingHealth, is Singapore's largest group of healthcare institutions. The group was formed in 2000 and consists of four public hospitals, three community hospitals, five national specialty centres and a network of eight polyclinics. The Singapore General Hospital is the largest hospital in the group and serves as the flagship hospital for the cluster.[41]

As SingHealth is the biggest healthcare organization of Singapore, many ministers and even the Prime minister of 2018 (Lee Hsien Loong) had their data stolen by this malicious attack. [42] Even an organization of this size did not have the right measures to defend against attackers, we can only imagine what can happen to smaller organizations around the world, if we do not take this topic seriously.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

United States of America

The US is the leading country in cybersecurity and healthcare industry at the moment. It has some of the best research facilities in the world in the field of biomedical engineering, whilst having state-of-the-art equipment for experts in software

[39] Kaspersky. "What Is WannaCry Ransomware?" Www.Kaspersky.Com, 6 July 2023, www.kaspersky.com/resource-center/threats/ransomware-wannacry.
[40] Auto, Hermes. "Personal Info of 1.5m SingHealth Patients, Including PM LEE, Stolen in Singapore's Worst Cyber Attack." The Straits Times, 1 Oct. 2021, www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most.
[41] "SingHealth." Ministry of Education (MOE), www.moe.gov.sg/sgis/sponsoring-organisations/industries/healthcare-administrators/singhealth.
[42] Tham, Irene. "Singapore's Most Serious Cyber Attack: How It Unfolded." The Straits Times, graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html.

engineering.[43] Apart from that, they have many laws and acts in order to tackle the issue discussed in this study guide, such as the HIPAA and the FDA postmarket cybersecurity guidance. Yet, many attacks have occurred, such as the cyberattack on Anthem Inc. in 2015, one of the largest and well-secured health insurance companies in the nation. In this attack, about 80 million patients' data were stolen. Anthem after the incident took several measures identity repair assistance -available to all those whose information was stolen in this breach, providing them with investigators to recover financial losses, restore and repair credit to pre-theft status.[44] This attack deeply affected the USA, which is evidence since HIPAA was modified afterwards, to make it more inclusive and enforce healthcare organizations to take all necessary steps to ensure patient confidentiality.

United Kingdom

Similarly to the US, the United Kingdom provides its people with world-class healthcare, having multiple research institutions and very advanced medical devices in its "medical arsenal". This makes the UK a "prime" target for cyberattacks. This has been seen in the past years, with the WannaCry ransomware attack for example, which, even though did not target specifically the UK, the country that was affected the most by it was the UK, due to the negligence of the National Health Service (NHS), which before that attack did not strive to ensure that healthcare organisations must be safe from cyberattacks. Whilst the United Kingdom might not have many actions or laws set for preventing cyberattacks on medical infrastructure, they have a body called the National Cyber Security Centre (NCSC) which deals with any possible problems that have to do with the digital safety of UK citizens, including patients in healthcare organisations.

China

The size of China's healthcare system and its substantial investment in medical infrastructure have created a strong incentive to prioritize cybersecurity when it comes to their healthcare system -and not only. China has not been impacted by any -known- cyber-attacks up to this date. [45] This could be the case for multiple reasons. Only a few Chinese get healthcare from hospitals due to the fact that they are not covered by insurance companies. The rest of the population relies on their traditional methods of medication, remedies. Most people are treated in places where

[43] Marks, Joseph. "The Cybersecurity 202: The United States Is Still Number One in Cyber Capabilities." Washington Post, 28 June 2021, www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities.

[44] California, State of. "Anthem Data Breach." CA Department of Insurance, www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm.

[45] Briefing, China. "Understanding China's Rapidly Growing Healthcare Market." China Briefing News, 12 June 2023, www.china-briefing.com/news/understanding-chinas-rapidly-growing-healthcare-market.

computers are not used, and traditional methods are still taking place.[46] Yet, the fact that some are treated in healthcare institutes of China is an indication of economic status, thus, making Chinese hospitals a target for hackers.

Singapore

Singapore is a nation that has suffered the consequences of hacking medical infrastructure. One of the biggest cyber-attacks was recorded in that country, the SingHealth data breach, which is in depth discussed in the *Background Information: Case studies*. This makes Singapore a country with deep care about the cybersecurity of its country, with multiple revision of the laws concerning the topic, especially after that attack, so as to ensure that nothing like this would occur in the future. Up until now and since then, there have been no cases of cyber-attacks in Singapore, proving that they handled the consequences of that attack efficiently.[47]

World Health Organization (WHO)

The WHO oversees and monitors healthcare systems and infrastructure in member states, as well as providing guidance and setting standards for healthcare worldwide. The WHO also plays a critical role in global health emergency response, as it was shown to all of us in the COVID-19 pandemic. The WHO itself cannot do much for the problem at hand. However, with the cooperation of other organizations, it can efficiently transfer to them its knowledge on how to respond to emergencies, making the tackling of the issue much smoother and quicker.

Cybersecurity and Infrastructure Security Agency (CICA)

CISA is a US federal agency dedicated to cybersecurity safety. It works as the central hub of cybersecurity in the United States. CISA as an agency has done extensive research in cyber threats, thus, it provides vital information that help us stay up to date with the cyber attackers. On top of that, as a federal organization, it has contributed economically to the distribution of information about the cyber world, specifically to young people that are interested in pursuing careers regarding the topic. The most recent case where CISA donated money for this purpose was on the 3rd of November 2023, when they awarded 3 million dollars (USD) in funding for cyber education and training of next generation's cyber leaders.[48]

[46] AsiaNews.it. "Only Those with Money Can Afford Health Care in China." CHINA, www.asianews.it/news-en/Only-those-with-money-can-afford-health-care-in-China-4263.html.
[47] Auto, Hermes. "Personal Info of 1.5m SingHealth Patients, Including PM LEE, Stolen in Singapore's Worst Cyber Attack." The Straits Times, 1 Oct. 2021, www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most.
[48] "CISA Awards $3M in Funding for Cyber Education and Training of Next-Gen Cyber Leaders: CISA." Cybersecurity and Infrastructure Security Agency CISA, 7 Nov. 2023, www.cisa.gov/news-events/news/cisa-awards-3m-funding-cyber-education-and-training-next-gen-cyber-leaders.

TIMELINE OF EVENTS

DATE	DESCRIPTION OF EVENT
21 August 1996	"The Health Insurance Portability and Accountability Act (HIPAA) is passed on, with the dual goals of making healthcare delivery more efficient and increasing the number of Americans with health insurance coverage."[49]
2000	The FDA approves the Da Vinci surgical system for use in hospitals.[50]
13 April 2000	"PIPEDA becomes a law, to promote consumer trust in electronic commerce. The act is also intended to reassure the EU that the Canadian privacy law is adequate to protect the personal information of European citizens."[51]
2005	The RAVE-II surgical system is developed, as a part of a project on the future of battlefield medicine.[52]
4 February 2015	One of the biggest cyberattacks to a US company in the healthcare sector takes place, specifically, the cyberattack on Anthem Inc.
December 2016	The FDA issues guidance to inform the industry about managing postmarket cybersecurity vulnerabilities for medical devices, which brings us a step closer to solving the issue discussed.[53]
May 2017	The WannaCry ransomware attack takes place, which strains the healthcare system of the UK and other countries. Maybe the biggest cyberattack that affected healthcare in history.
26 May 2018	The 71st World Health Assembly is closed, with many topics covered, and for the case of this study guide, a resolution on "Digital Health" is voted for, which urges the member states to prioritize development and greater use of digital technologies in health.[54]

[49] Introduction - beyond the HIPAA Privacy Rule - NCBI Bookshelf, www.ncbi.nlm.nih.gov/books/NBK9576/.

[50] "Da Vinci Surgical System." Da Vinci Surgical System - an Overview | ScienceDirect Topics, www.sciencedirect.com/topics/medicine-and-dentistry/da-vinci-surgical-system. Accessed 10 Nov. 2023.

[51] Branch, Legislative Services. "Consolidated Federal Laws of Canada, Personal Information Protection and Electronic Documents Act." Personal Information Protection and Electronic Documents Act, 10 Nov. 2023, laws-lois.justice.gc.ca/eng/acts/p-8.6/.

[52] Team, Robots. "Raven II." ROBOTS, 18 May 2018, robotsguide.com/robots/ravensurgical.

[53] Center for Devices and Radiological Health. "Postmarket Management of Cybersecurity in Medical Devices - Guidance." U.S. Food and Drug Administration, FDA, www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices.

[54] Mitchell, Cristina. "Paho/WHO: 71st World Health Assembly Wraps up with Adoption of Resolutions on Wide-Ranging Topics." Pan American Health Organization / World Health Organization, 26 May 2018, www3.paho.org/hq/index.php?option=com_content&view=article&id=14391%3A71st-world-health-assembly-wraps-up-with-adoption-of-resolutions-on-wide-ranging-topics&Itemid=0&lang=en#gsc.tab=0.

27 June – 4 July 2018	Sensitive information of millions of patients in Singapore is stolen, in an attack called SingHealth cyberattack.
5 December 2018	The UN General Assembly Resolution A/RES/73/27 is passed, having to do with the field of information and telecommunications in the context of international security.[55]
September 2020	National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 5 provides a catalogue of security and privacy controls for information systems and organizations, to protect against a wide variety of threats.[56]
26 May 2021	EU Medical Device Regulation establishes a regulatory framework for medical devices that safeguard public information.[57]
29 March 2022	The FDA issues a guidance for immediate application of cybersecurity in medical devices.[58]
3 November 2023	CISA donated 3 million US dollars for funding cyber education and training of the next generation's cyber leaders [59]

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

UN General Assembly Resolution A/RES/73/27

This resolution, adopted by the United Nations General Assembly in December 2018, outlines the significance of digital health technology in the progression of global health. While its primary focus is not only on cybersecurity, the aforementioned program also underlines the importance of enhancing the resilience of health systems, which include the implementation of cybersecurity measures to safeguard medical infrastructure. In the said resolution, the focus is on future meeting and negotiations regarding the topic, meetings that never occurred however, due to the pandemic and

[55] A/RES/73/27, undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F73%2F27&Language=E&DeviceType=Desktop&LangRequested=False.
[56] Force, Joint Task. "Security and Privacy Controls for Information Systems and Organizations." CSRC, 10 Dec. 2020, csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.
[57] "What Is the European Union Medical Device Regulation?" Assent, 18 Jan. 2023, www.assent.com/resources/knowledge-article/what-is-the-european-union-medical-device-regulation/.
[58] Center for Devices and Radiological Health. "Cybersecurity." U.S. Food and Drug Administration, FDA, www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.
[59] "CISA Awards $3M in Funding for Cyber Education and Training of Next-Gen Cyber Leaders: CISA." Cybersecurity and Infrastructure Security Agency CISA, 7 Nov. 2023, www.cisa.gov/news-events/news/cisa-awards-3m-funding-cyber-education-and-training-next-gen-cyber-leaders.

then the wars that broke out in eastern Europe and in the middle east. Thus, solutions were not developed by the General Assembly, making this resolution ineffective.[60]

USA FDA's postmarket cybersecurity guidance

In December 2016, the US Food and Drug Administration (FDA) released guidelines on the topic of "Postmarket Management of Cybersecurity in Medical Devices" and it was targeted specifically towards manufacturers of such devices. This document provides a comprehensive set of guidelines for addressing cybersecurity vulnerabilities in existing medical equipment. The recommendations encompass various measures such as software updates, continuous monitoring for emerging vulnerabilities, and the establishment of a robust incident response strategy.[61]

European Union Medical Device Regulation (MDR)

The MDR was adopted in 2017 but applied in May of 2021, and it includes specific measures targeting medical device cybersecurity. For example, it established on-site assessment activities of medical devices that would be led by a designated authority, in order to ensure that all safety measures are in place and hospitals do not skip over important steps that would compromise the safety of the patients' data. It also obligated medical device manufacturers to implement appropriate cybersecurity measures and risk management strategies, as well as to monitor and report all cybersecurity incidents.[62]

National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 5

In September 2020, NIST released the fifth revision of SP 800-53, "Security and Privacy Controls for Information Systems and Organizations." While not exclusive to medical infrastructure, this comprehensive publication provides a catalogue of security controls that can be adopted by healthcare institutions to protect their systems, including surgical robots, such as a series of safety tests that can be performed by informed personnel of the hospital.[63]

---

[60] A/RES/73/27, undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F73%2F27&Language=E&DeviceType=Desktop&LangRequested=False.

[61] Center for Devices and Radiological Health. "Postmarket Management of Cybersecurity in Medical Devices - Guidance." U.S. Food and Drug Administration, FDA, www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices. Accessed 13 Sept. 2023.

[62] "What Is the European Union Medical Device Regulation?" Assent, 18 Jan. 2023, www.assent.com/resources/knowledge-article/what-is-the-european-union-medical-device-regulation/.

[63] Force, Joint Task. "Security and Privacy Controls for Information Systems and Organizations." CSRC, 10 Dec. 2020, csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

POSSIBLE SOLUTIONS

Cybersecurity Bug Bounties

The establishment of bug bounties will be a measure that will drastically change the amount of cyberattacks in medical infrastructure and also, minimize the chances for a potential hijacking of surgical robots. Ethical hackers and researchers, along with the healthcare companies and patients could be benefited from it financially by assisting healthcare organizations in ensuring that no cyberattacks occur. Knowledgeable hackers can try to take over medical infrastructure and surgical robot -in a controlled situation of course- so that vulnerabilities in the systems can be brought up. Thus, the healthcare sector in cooperation with cybersecurity experts can take measures that "fix" these vulnerabilities, making it seemingly impossible for hackers to do any harm to patients, which is the number one priority of any healthcare organization.

To sum up, these bug bounty programs could incentivize individuals to actively participate in securing medical technology and uncovering potential weaknesses that may otherwise go unnoticed.

Blockchain for Medical Data Security

We have seen from the case studies and other attacks in medical infrastructure that the most common type of attack is stealing the sensitive data of patients. This is solely due to the fact that it is extremely easy to access the servers in which hospitals and other organizations of the same field, store the data of their patients, no matter the status of the server -whether they are public or private servers.

Exploiting the use of blockchain technology will enhance medical data security, since the blockchain's decentralized and temper-resistant nature can help protect patient records, ensure data integrity, and prevent unauthorized access to sensitive information, since changes in the blocks of the blockchain are almost impossible to happen. Furthermore, blocks cannot all be hacked at once, and hackers would have to put in the effort for tens of thousands of blocks. After the first block would have been hacked, the hospital would get informed about that, thus taking the measures necessary to tackle that problem. Even if the hacker is able to bypass the notifying system of the blockchain, if we were to establish weekly check-ups for this system, then, this threat would get completely resolved.

Basically, the implementation of blockchain-based solution can add an extra layer of protection to medical infrastructure.

Medical device Vulnerability Reporting Database

On a similar note to the first solution, the creation of a centralized vulnerability reporting database can help manufacturers, researchers, and medical professionals to

share information on the topic. Basically, it will serve as a repository for sharing information about known vulnerabilities and their mitigations.

This platform will only be accessible to healthcare organizations and not individuals. That way we ensure that no one else can publicise false information there, since individuals will not have access. In the case of a cyberattack to the systems of a hospital/healthcare organization and the hijacking of the passwords to access the platform, the organization can contact in any way possible the creators of that platform, to let them know what happened. In this way, even in the case were someone has unauthorized access to the platform through the account of an organization, the platform developers will know, and immediately ban that account temporarily, so no misinformation can be spread.

BIBLIOGRAPHY

Contributor, Guest. "Investing into Health Care Infrastructure." *Facility Executive Magazine*, 21 June 2021, facilityexecutive.com/investing-into-health-care-infrastructure/. Accessed 10 Sept. 2023.

"Robotic Surgery." *Mayo Clinic*, Mayo Foundation for Medical Education and Research, 6 May 2022, www.mayoclinic.org/tests-procedures/robotic-surgery/about/pac-20394974.

"About Da Vinci Systems." *Intuitive.Com*, Intuitive, www.intuitive.com/en-us/patients/da-vinci-robotic-surgery/about-the-systems.

"Robotic Database - Robotic Platform." *TERRINet*, Imperial College London, 10 Nov. 2022, www.terrinet.eu/robotic_database_show_platform/?id=92.

Aliouche, Hidaya. "What Is Remote Surgery/Telesurgery?" *News*, University of Manchester, 11 Nov. 2021, www.news-medical.net/health/What-is-Remote-SurgeryTelesurgery.aspx.

"Cyber Security." *IT Governance*, www.itgovernance.co.uk/what-is-cybersecurity.

"What Is Data Privacy?" *SNIA*, www.snia.org/education/what-is-data-privacy.

"What Is Network Security?" *Cisco*, 4 July 2023, www.cisco.com/c/en/us/products/security/what-is-network-security.html.

"What Is Malware? Malware Definition, Types and Protection." *Malwarebytes*, www.malwarebytes.com/malware.

"What Is Incident Response? Strategy, Process, Templates & More." *Cynet*, 20 Aug. 2023, www.cynet.com/incident-response/.

"Cybersecurity Risk Assessment: Components + How to Perform." *KnowledgeHut*, www.knowledgehut.com/blog/security/cybersecurity-risk-assessment.

"What Is Ransomware? - Definition, Prevention & Examples: Proofpoint Us." *Proofpoint*, 16 Aug. 2023, www.proofpoint.com/us/threat-reference/ransomware.

"Health Insurance Portability and Accountability Act of 1996 (HIPAA)." *Centers for Disease Control and Prevention*, 27 June 2022, www.cdc.gov/phlp/publications/topic/hipaa.html.

"What Is Blockchain and How Does It Work?" *Synopsys*, www.synopsys.com/glossary/what-is-blockchain.html.

Epalm. "Cybersecurity in Healthcare." *HIMSS*, 16 Dec. 2021, www.himss.org/resources/cybersecurity-healthcare.

Rider EA;Comeau M;Truog RD;Boyer K;Meyer EC; "Identifying Intangible Assets in Interprofessional Healthcare Organizations: Feasibility of an Asset Inventory." *Journal of Interprofessional Care*, U.S. National Library of Medicine, pubmed.ncbi.nlm.nih.gov/30415591/.

"What Is an Electronic Health Record (EHR)?" *What Is an Electronic Health Record (EHR)? | HealthIT.Gov*, 10 Sept. 2019, www.healthit.gov/faq/what-electronic-health-record-ehr.

"Communication Systems in Healthcare." *HIPAA Journal*, 14 Dec. 2022, www.hipaajournal.com/communication-systems-in-healthcare/.

Charles, Megan, et al. "What Is PACS (Picture Archiving and Communication System)?: Definition from TechTarget." *Health IT*, TechTarget, 30 Aug. 2018, www.techtarget.com/searchhealthit/definition/picture-archiving-and-communication-system-PACS.

"What Are PIS Systems?" *What Are PIS Systems? | Nev's Ink*, 3 Sept. 2020, nevsink.com/what-are-pis-systems-va-30.html.

Sutton, Reed T., et al. "An Overview of Clinical Decision Support Systems: Benefits, Risks, and Strategies for Success." *Npj Digital Medicine*, vol. 3, no. 1, 2020, doi:10.1038/s41746-020-0221-y.

Lutkevich, Ben, et al. "What Is Telehealth (Telemedicine)?: Definition from TechTarget." *Health IT*, TechTarget, 24 Feb. 2023, www.techtarget.com/searchhealthit/definition/telemedicine.

"Robotic Surgery." *Our Services*, athensmedicalgroup.com/critical-illness/robotic-surgery/.

Rizzo, Kayla R, et al. "Status of Robotic Assisted Surgery (RAS) and the Effects of Coronavirus (COVID-19) on Ras in the Department of Defense (DOD)." *Journal of Robotic Surgery*, U.S. National Library of Medicine, Apr. 2023, www.ncbi.nlm.nih.gov/pmc/articles/PMC9225798/.

"Da Vinci Surgical System ." *Intuitive.Com*, www.intuitive.com/en-us/patients/da-vinci-robotic-surgery/about-the-systems.

Choi, Paul J, et al. "Telesurgery: Past, Present, and Future." *Cureus*, U.S. National Library of Medicine, 31 May 2018, www.ncbi.nlm.nih.gov/pmc/articles/PMC6067812/.

Team, Robots. "Raven II." *ROBOTS*, 18 May 2018, robotsguide.com/robots/ravensurgical.

Langston, Jennifer. "UW Researchers Hack a Teleoperated Surgical Robot to Reveal Security Flaws." *UW News*, 7 May 2015, www.washington.edu/news/2015/05/07/uw-researchers-hack-a-teleoperated-surgical-robot-to-reveal-security-flaws/.

Bonaci, Tamara, et al. "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats against Teleoperated Surgical Robots." *arXiv.Org*, 12 May 2015, arxiv.org/abs/1504.04339.

Kaspersky. "What Is WannaCry Ransomware?" *Www.Kaspersky.Com*, 6 July 2023, www.kaspersky.com/resource-center/threats/ransomware-wannacry.

"SingHealth." *Ministry of Education (MOE)*, www.moe.gov.sg/sgis/sponsoring-organisations/industries/healthcare-administrators/singhealth.

Tham, Irene. "Singapore's Most Serious Cyber Attack: How It Unfolded." *The Straits Times*, graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html.

Auto, Hermes. "Personal Info of 1.5m SingHealth Patients, Including PM LEE, Stolen in Singapore's Worst Cyber Attack." *The Straits Times*, 1 Oct. 2021, www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most.

Marks, Joseph. "The Cybersecurity 202: The United States Is Still Number One in Cyber Capabilities." *Washington Post*, 28 June 2021, www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities.

Briefing, China. "Understanding China's Rapidly Growing Healthcare Market." *China Briefing News*, 12 June 2023, www.china-briefing.com/news/understanding-chinas-rapidly-growing-healthcare-market.

"Cyber Security Strategy for Germany 2021." *Bundesportal*, Germany, Federal Ministry of the Interior, Building and Community, Aug. 2021, www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf?__blob=publicationFile&v=4.

"Israel International Cyber Strategy." *Www.Gov.Il*, www.gov.il/BlobFolder/news/international_strategy/en/Israel%20International%20Cyber%20Strategy.pdf.

Introduction - beyond the HIPAA Privacy Rule - NCBI Bookshelf, www.ncbi.nlm.nih.gov/books/NBK9576/.

"Da Vinci Surgical System." *Da Vinci Surgical System - an Overview | ScienceDirect Topics*, www.sciencedirect.com/topics/medicine-and-dentistry/da-vinci-surgical-system. Accessed 10 Nov. 2023.

"Personal Information Protection and Electronic Documents Act." *Wikipedia*, Wikimedia Foundation, 18 July 2023, en.wikipedia.org/wiki/Personal_Information_Protection_and_Electronic_Documents_Act.

Mitchell, Cristina. "Paho/WHO: 71st World Health Assembly Wraps up with Adoption of Resolutions on Wide-Ranging Topics." *Pan American Health Organization / World Health Organization*, 26 May 2018, www3.paho.org/hq/index.php?option=com_content&view=article&id=14391%3A71st-world-health-assembly-wraps-up-with-adoption-of-resolutions-on-wide-ranging-topics&Itemid=0&lang=en#gsc.tab=0.

Center for Devices and Radiological Health. "Postmarket Management of Cybersecurity in Medical Devices - Guidance." *U.S. Food and Drug Administration*, FDA, www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices. Accessed 13 Sept. 2023.

Force, Joint Task. "Security and Privacy Controls for Information Systems and Organizations." *CSRC*, 10 Dec. 2020, csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

A/RES/73/27, undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F73%2F27&Language=E&DeviceType=Desktop&LangRequested=False.

"What Is the European Union Medical Device Regulation?" *Assent*, 18 Jan. 2023, www.assent.com/resources/knowledge-article/what-is-the-european-union-medical-device-regulation/.

"Food and Drug Administration (FDA): Usagov." *Food and Drug Administration (FDA) | USAGov*, www.usa.gov/agencies/food-and-drug-administration.

"What Is an Ethical Hacker? And How to Become One - Crowdstrike." *Crowdstrike.Com*, 7 July 2023, www.crowdstrike.com/cybersecurity-101/ethical-hacker/.

"About the CSTD." *UNCTAD*, unctad.org/topic/commission-on-science-and-technology-for-development/about. Accessed 09 Nov. 2023.

Tsclinic. "The History of Robot-Assisted Surgery." *The Surgical Clinic*, thesurgicalclinics.com/history-of-robot-assisted-surgery/.

"Benefits of Robotic Surgery." *UC Health*, www.uchealth.com/services/robotic-surgery/patient-information/benefits/.

California, State of. "Anthem Data Breach." *CA Department of Insurance*, www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm.

"CISA Awards $3M in Funding for Cyber Education and Training of Next-Gen Cyber Leaders: CISA." *Cybersecurity and Infrastructure Security Agency CISA*, 7 Nov. 2023, www.cisa.gov/news-events/news/cisa-awards-3m-funding-cyber-education-and-training-next-gen-cyber-leaders.

Branch, Legislative Services. "Consolidated Federal Laws of Canada, Personal Information Protection and Electronic Documents Act." *Personal Information Protection and Electronic Documents Act*, 10 Nov. 2023, laws-lois.justice.gc.ca/eng/acts/p-8.6/.

MULTIMEDIA RESOURCES

Murray-Watson, Author: Rebecca. "Healthcare Data Breach Statistics." *HIPAA Journal*, 7 Sept. 2023, www.hipaajournal.com/healthcare-data-breach-statistics/.

Rizzo, Kayla R., et al. "Status of Robotic Assisted Surgery (RAS) and the Effects of Coronavirus (COVID-19) on Ras in the Department of Defense (DOD) - Journal of Robotic Surgery." *SpringerLink*, Springer London, 23 June 2022, link.springer.com/article/10.1007/s11701-022-01432-7.