**Team Project**

**Medical devices and cybersecurity**

**Authors:**

**Nahuel Hernan Ramos**

**Jennifer Wakstein**

**Masha Zalivansky**

**ThriveDX**

**Israel, 2023**

**Table of Contents**

[**1.1 Introduction 3**](#_fvzpj6st47ms)

[**1.2 Relevance global cyber threat 4**](#_ucto4hbx6800)

[**1.3 Our goal 4**](#_yto8ljvkwtno)

[**2.1 Current situation in the healthcare industry 4**](#_i1dr2fylqv9b)

[**2.2 Cases 12**](#_gzyvek20h7mr)

[**3. Types of Attacks on Medical devices 14**](#_hw4b1ma2wtm3)

[**4.1 Solutions – General ideas 22**](#_t048jraaiae7)

[**4.2 Solution – attack mitigations 24**](#_k1i8va8o19mv)

[**4.3 New suggested solutions 30**](#_dzf6p14pi3)

[**5. Conclusion 32**](#_dd297dnsnojn)

[**6. Appendix 33**](#_tov78v6jnh09)

# 1.1 Introduction

In the world we live in now pretty much nothing can be done without an electronic device of some sort. We use technology in every part of your lives, and it’s helping us achieve our goals faster and better. But there is a downside – everything with an internet connection can be broken into and taken advantage of. This is also true for medical devices. Healthcare is one of the areas where technological progress has the most impact: we can see better, have artificial organs, monitor babies in utero, live longer and healthier lives. And the vulnerabilities in these kinds of devices can directly affect people’s lives. Lives can be endangered if someone with bad intentions can access the manipulation of critical devices.

The GHTF (Global Harmonization Task Force) definition states, in summary, that a medical device is any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article that does not achieve its primary intended action in or on the human body solely by pharmacological, immunological or metabolic means and that is intended for human beings for:

• the diagnosis, prevention, monitoring, treatment or alleviation of disease;

• the diagnosis, monitoring, treatment, alleviation of, or compensation for an injury;

• the investigation, replacement, modification, or support of the anatomy or of a physiological process;

• supporting or sustaining life;

• controlling conception;

• disinfecting medical devices; and

• providing information for medical or diagnostic purposes by means of in vitro examination of specimens derived from the human body.

Healthcare infrastructure relies heavily on the digital connectivity of medical devices. Connected medical devices are at high risk of cyberattacks, and the consequences of an attack can be more severe than with other connected systems.

Many connected devices store or transmit patient data, making it important to protect privacy and ensure the integrity of the data. A data breach could be used to damage the reputation of a patient or force a healthcare organization to pay a ransom to regain access to the data.

But the risk of cyberattacks on medical devices goes far beyond privacy concerns – they can threaten the safety of patients as well. Medical devices breached by attackers can cause physical harm to patients, disrupt medical care, and affect health outcomes.

Data shows that 53% of connected medical devices and other IoT devices in hospitals have a known critical vulnerability. Additionally, a third of bedside healthcare IoT devices – which patients most depend on for optimal health outcomes – have an identified critical risk. If attacked, these vulnerabilities could impact service availability, data confidentiality, or patient safety – with potentially [life-threatening consequences](https://www.businesswire.com/news/home/20210922005436/en/New-Ponemon-Institute-Research-Shows-Ransomware-Attacks-on-Healthcare-Delivery-Organizations-Can-Lead-to-Increased-Mortality-Rate) for patient care.

Today, there are an estimated 2 million different kinds of medical devices on the world market, categorized into more than 7000 generic devices groups.

Cybersecurity is becoming a critical aspect of the design, manufacturing, and operation for medical devices.

# 1.2 Relevance global cyber threat

Life sustaining medical devices, such as ventilators and infusion pumps, are now connected wirelessly to a variety of systems, networks and other tools within a hospital – ultimately contributing to the Internet of Medical Things (IoMT) and presenting potential points of breach as well as incremental costs and operating risk to providers.

Some of the common risks facing connected medical devices is that the medical devices last for a long time, so are not updated with the new manufacturing regulations.

* Devices with known security vulnerabilities but do not support software or firmware updates. (many critical devices run old Windows versions that no longer have security updates.)
* Devices that default credentials which can be easily discovered by attackers. In some cases the default credentials cannot be changed, and even if they can, hospital staff may not have visibility over the affected devices.
* Default Passwords Remain a Common Risk: The most common IoMT and IoT device risks are connected to default passwords and settings that attackers can often obtain easily from manuals posted online, with 21% of devices secured by weak or default credentials.
* Devices that do not support deployment of endpoint security technology, such as endpoint detection and response (EDR). Instead, they must rely on inadequate network and perimeter defenses. (It can be challenging and time consuming to obtain logs from these devices, and there is usually no solution for real-time alerting in case of anomalous events.)

Patient care disruptions and safety issues related to medical device security vulnerabilities are a critical concern as the number of IoMT medical devices is expected to skyrocket from 10 billion to 50 billion over the next decade. These cyberattacks not only threaten patient privacy and clinical safety and outcomes, but also a hospital’s financial resources

# 1.3 Our goal

In this paper we will explore the world of medical devices used in hospitals, analyze their vulnerabilities and the threats, explore the more recent attacks and will try to figure out what are the strategies to protect this precious equipment from the hand of wrongdoers.

# 2.1 Current situation in the healthcare industry

It’s impossible to talk about the MedDev cybersecurity without talking about the situation in the healthcare sector in general. And the situation is dire to say the least. Here are just a few facts and statistics.

In 2019 ECRI (global, independent authority on healthcare technology and safety) identified cyber security as a #1 health hazard.

After the beginning of the pandemic world saw the surge in cyber attacks. Healthcare providers saw a [42% increase](https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=68478cba5650) in data breaches in 2020, and a staggering [69% year-over-year increase](https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise) in the volume of cyber attacks from 2020 to 2021 (in this chapter the data is US-based).

Phishing attacks against healthcare organizations [increased by 220%](https://www.f5.com/company/news/features/phishing-attacks-soar-220--during-covid-19-peak-as-cybercriminal) during the COVID-19 pandemic. [81% of healthcare organizations](https://ironscales.com/blog/ironscales-releases-findings-from-state-of-cybersecurity-survey/) report experiencing an increase in phishing attacks since March 2020

According to the Ponemon Institute’s survey of 641 IT and IT security practitioners in healthcare organizations, 89 percent of these organizations experienced cyberattacks in 2022. For organizations in that group, the average number of attacks was 43. Based on the responses, the average total cost for the most expensive cyberattack experienced was $4.4 million.

In 2022 cyberattacks on healthcare services were on the rise. The first months of 2022 have exhibited a disproportionate number of cyberattacks against national healthcare systems.

According to the research, healthcare institutions are currently the main target for ransomware attacks. This is the most disruptive type of attack because it leads to the most operational delays. [66% of healthcare organizations](https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise) say they experienced a ransomware attack in 2021, an increase from 34% in 2020.

The average cost of remediating a single ransomware incident is [$1.27 million](https://www.chiefhealthcareexecutive.com/view/cyberattacks-in-healthcare-surged-last-year-and-2022-could-be-even-worse). Healthcare providers paid ransoms [61% of the time](https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise) in 2021.

Connected medical devices in the healthcare delivery system represent a significant potential entry point for cyberattacks, yet these devices are not always included in a hospital’s information technology structure and security planning. Today, they represent important clinical assets to be secured, as these and other connected medical devices in hospitals work within a single network and can be an access point for a breach.

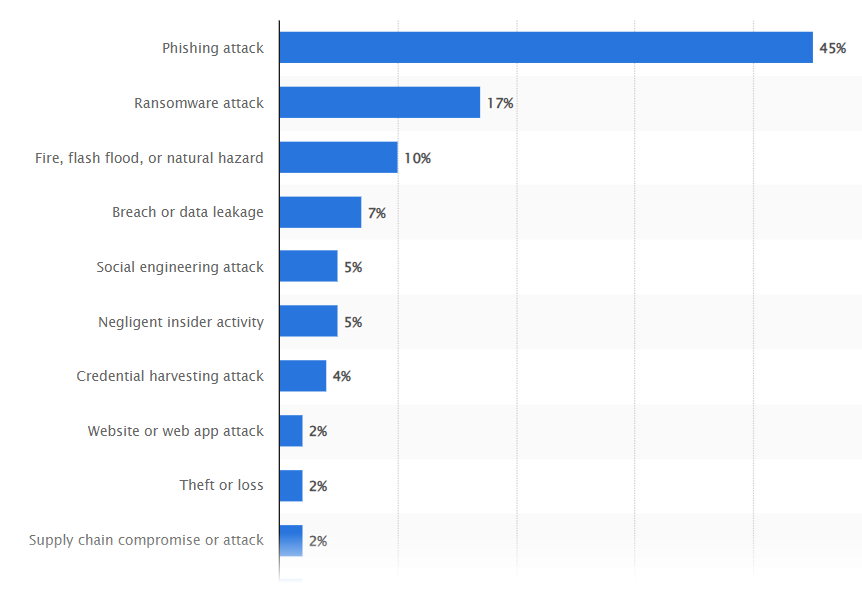
Medical devices are most commonly run on Linux-based medical software that cannot be protected by traditional cybersecurity like Windows-based software. They stay in operation despite outdated serviceability, which could create exploitable weaknesses for attackers. Some of the most vulnerable devices for a cyberattack are IV pumps, ultrasounds and cardiac monitoring systems.

It is important to note that even if medical devices are not the target of the attack they are a part of the medical institution’s network and also highly susceptible to the cyberattacks.

64% of organizations are concerned about device security.

64% of healthcare organizations report feeling at risk of business email compromise and spoofing phishing attacks, yet just [48% of those organizations](https://www.healthcareitnews.com/news/direct-line-between-hospital-cyberattacks-and-patient-mortality-report-shows) have a documented plan in place to address this threat.

**Significant cyber security incidents in healthcare organizations (USA, 2021)**



FBI Notice

In a September of 2022 notice from the FBI’s Internet Crime Complaint Center (IC3), the law enforcement agency said it has identified “an increasing number” of vulnerabilities posed by unpatched medical devices that run on outdated software and devices that lack adequate security features. “Medical device vulnerabilities predominantly stem from device hardware design and device software management. Routine challenges include the use of standardized configurations, specialized configurations, including a substantial number of managed devices on the network, lack of device embedded security features, and the inability to upgrade those features.”

The FBI noted that medical device hardware is often used for more than 30 years at some healthcare facilities, giving cybercriminals and state actors ample time to discover and exploit bugs.

The FBI specifically cited vulnerabilities found in insulin pumps, intracardiac defibrillators, mobile cardiac telemetry, pacemakers and intrathecal pain pumps, noting that malicious hackers could take over the devices and change readings, administer drug overdoses, or “otherwise endanger patient health.”

Top Five Cyber threats in the healthcare industry

**1. Ransomware**

Between July 1 and September 30, 2021, researchers found 68 healthcare ransomware attacks globally. The United States was home to 60 percent of those attacks, with France, Brazil, Thailand, Australia, and Italy following. Medical clinics are the most frequently attacked sub-industry for ransomware attacks, with ten ransomware gangs taking center stage.

**Examples**

In September 2021, the Hive gang was responsible for attacking four healthcare facilities in the United States. One of the facilities, a medical center in Missouri, was a victim of Hive and had patient information stolen from its servers. After stealing the information, the ransomware gang posted it online – including names, medical information, and Social Security numbers. Hive was also responsible for a ransomware attack against Memorial Health which resulted in emergency room diversions and appointment cancellations.

Hive uses phishing emails to gain access to networks and RDP to navigate the network. Fortunately, the attack didn’t cause care disruptions; however, other healthcare facilities, like Springhill Medical Center are not as fortunate.

In 2019, Springhill Medical Center was attacked by a ransomware gang and that attack led to a baby’s death. The baby was born with its umbilical cord wrapped around his neck, depriving him of oxygen during delivery. A heart rate monitor usually detects and informs hospital staff of life-threatening situations, but the monitor never alerted staff due to its system being compromised by a ransomware attack. The doctor delivering the baby stated that she would have delivered her via cesarean section had she been able to see the heart monitor’s readout. She stated that the situation was preventable. As a result, the baby was born with severe brain damage and died nine months later. The hospital had to defend themselves in a trial related to the attack in September 2021.

**2. Business email compromise**

The FBI calls business email compromise (BEC) the “Billion Dollar Scam”. The tactic involves attackers using spoofed emails (spear-phishing emails) or compromised accounts to persuade employees to transfer large sums of money to fraudulent accounts. Typically, the attacker pretends to be someone of authority or power within the medical facility, like the CEO or Vice President. Before sending the spoofed email pretending to be someone from the organization, attackers do thorough research on how the CEO might sound so that victims are more likely to believe their scam. In addition to spear-phishing emails, attackers will also spoof a website or use malware to infiltrate hospital networks to gain access to email chains about billing and invoices**.**

One of the most recent instances we have of a BEC attack is a California hospital that was attacked between December 2020 and April 2021. The attack happened when an employee clicked on a malicious link in their work email, thus opening the door for other email accounts to be compromised. The organization noticed suspicious activity in March 2021 and terminated authorized access to compromised email accounts.

The attackers allegedly accessed and exfiltrated claims information, dates of birth, lab results, addresses, and other private patient information. The hospital notified patients of the breach in September 2021, but one patient decided to sue the healthcare system for breach of contract, negligence, and violating California consumer privacy and medical confidentiality laws. The patient’s lawyer stated that the breach could have been preventable had the organization trained their employees on how to avoid becoming a victim of phishing attacks.

**3. Insider threats**

Sometimes, organizations are so enthralled with keeping track of outside threats, that they forget to be conscious of threats within their very own organization. Insiders often have access to systems and networks which puts them in the perfect position to compromise them. They may also have knowledge of vulnerabilities or of the network set up.

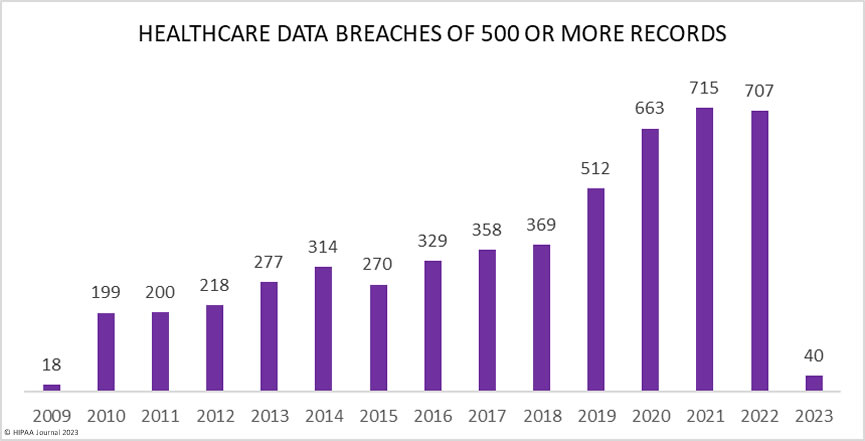
Some insiders are just careless, accidentally losing work devices with sensitive information, but others are malicious and intentionally cause devastation to an organization. According to HealthItSecurity.com, the healthcare industry isn’t proactive when it comes to stopping insider data breaches. In a report published by Verizon, researchers found that the healthcare industry was the only industry that had more inside threats(56%) than external threats (43%).

In 2011, a night security guard employed at a Texas hospital built a botnet using the hospital’s network. He recorded himself moving around the hospital, going from desk to desk using an Ophcrack CD and the botnet, which was on a USB flash drive. He used his credentials to gain access to different areas and showed the viewers of his YouTube channel how he removed the hospital’s antivirus software from the system to install the botnet.

After installing the botnet, he showed viewers how he accessed the infected machines remotely. The security guard was part of a hacking group that was using botnet machines to attack other hacking groups, including Anonymous. It wasn’t until an analyst from McGrew Security noticed screenshots of the hospital’s HVAC system online, that the FBI was notified, and the security guard was arrested.

Each year, insider threats are consistently named as the biggest risk to healthcare data. With remote work and telehealth becoming more available, it’s important for healthcare organizations to be proactive with training employees on best cyber security practices, as well as keeping a watchful eye on who they hire.

**4. Data breaches**



Healthcare related data breaches [cost a total of $21 billion in 2020](https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals). A recent report from [IBM](https://www.hipaajournal.com/average-cost-of-a-healthcare-data-breach-9-42-million-2021/) found that the average cost of a healthcare data breach was $9.23 million USD, an increase of $2 million USD from the previous year.

Unfortunately, data breaches are familiar territory for the healthcare industry and the sector experiences more data breaches than any other sector. There are several ways the breaches happen, with the most common being credential-stealing malware, employee negligence, and insider’s disclosing patient data.

Patient data is the most valuable data for attackers to steal. It’s more valuable than credit card information and social security numbers. Credit card information sells for about $1 to $2 on the dark web, while patient data can sell for as much as $363. Because the data is more valuable, cyber criminals have more incentive to attack medical databases. Another factor for cyber criminals looking to reap the rewards of stolen medical data is the weak and outdated systems of healthcare organizations. The industry has been slow to update their cybersecurity technology and they often times have substantial financial resources. Cyber criminals know this and assume money will be easy to collect.

**5. DDoS ATTACKS**

In our previous threat report, we discussed DDoS and how the Meris botnet is infecting systems on a global scale, primarily focusing on the technology industry. Did you know that DDoS attacks are popular within the healthcare industry as well? This technique is used by cyber criminals to overwhelm networks, causing a major problem for healthcare systems that need to access their network for proper patient care.

In 2018, Boston Children’s Hospital was attacked by hacktivist group, Anonymous. The group launched a massive DDoS attack against the hospital as retaliation for the hospital’s involvement in a child custody case. The attack disrupted the hospital’s network for two weeks, causing the hospital to lose over $300,000 trying to mitigate the attack. Not only did Anonymous disrupt the hospital’s network, but the attack also caused Harvard University and all of its hospitals to lose internet access as well. DDoS attacks can occur in a variety of ways, but this particular attack is the most common way a healthcare entity could be victimized.

Why is the healthcare industry consistently at risk?

The healthcare industry is two to three times more likely to be a target for cybercrime than any other industry. Cyber security firm, Herjavec Group, reported that healthcare accounts for 18% of the nation’s gross domestic product (about $3.5 trillion) and they expect it to soar over the next decade. They also predict that global healthcare spending will increase dramatically from $8 trillion in 2013 to more than $18 trillion in 2040.

Most attackers won’t consider patients or vulnerable people when they see an opportunity. As previously stated, healthcare information is the most profitable information to sell on the black market, but there are other reasons why the industry is a constant target for cyber criminals.

Medical devices that are on a network are an easy way for attackers to gain entry. Because the machines are constantly changing and newer version are created every year, those in charge of online security and patient data have a hard time keeping up. The devices are designed for medical reasons, but they aren’t made with security in mind. The devices don’t store data, but they can be used to launch attacks on servers that do store data due to their lack of security.

Remote work and inconvenience are additional reasons why the healthcare industry is at risk for attacks. Medical professionals are often overworked and on time constraints. They may not consider online security to be a priority when their primary role is to save lives. Lack of proper authentication measures for devices and lack of time to devote to ensuring security are issues in this sector that must be addressed. Not wanting to disrupt convenient working practices to implement new technology may end up costing the industry more than time.

# 2.2 Cases

First death by ransomware attack

In 2021, an Alabama mother sued her local hospital for the death of her baby who was born in 2019 with the umbilical cord wrapped around its neck, resulting in serious brain damage.

Teirrani Kidd gave birth to her son, Nicko Silar, at Springhill Memorial Hospital in Mobile in July 2019, and the boy died on April 16, 2020, according to the lawsuit she filed in Mobile Circuit Court.

Kidd claimed that, unknown to her at the time, the hospital was the target of a ransomware attack that prevented doctors from accessing information that would have detected Nicko’s umbilical cord was wrapped around his neck in the womb, which she said caused brain damage to her son and resulted in his death nine months later.

The mother said she would not have chosen to give birth to Nicko at Springhill had she known the hospital was the target of a cyberattack, the suit states.

Kidd’s lawsuit was described as “the first credible public claim that someone’s death was caused at least in part by hackers who remotely shut down hospital computers in an extortion attempt,” according to NBC News.

Proofpoint & Ponemon study

[A 2021 study from Proofpoint and the Ponemon Institute](https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf), which surveyed more than 600 health care facilities, found that mortality rates increased at a quarter of the facilities following a ransomware attack.

According to the study, 50% of respondents say their organizations had an attack against its supply chain. 70% of those respondents say it disrupted patient care. The consequences included the delay of procedures and tests that resulted in poor outcomes such as an increase in the severity of an illness (54%). Another consequence was a longer length of stay (51%).

Ransomware attacks are more likely than the other types of attacks to hurt patient safety and care delivery. 64% of respondents in organizations that experienced a ransomware attack say it caused delays in procedures and tests that resulted in poor outcomes. 59% of respondents say it resulted in longer lengths of stay, which strains resources.

Technologies such as cloud, mobile, big data and IoT increase the risks to patient information and safety, according to 67% of respondents.

Overdose due to cyberattack

In 2022 a 3-year-old got overdosed on pain medicine because the hospital was under attack which had taken down some of the hospital’s digital tools.

When Kelley Parsi took her 3-year-old son to a hospital in Des Moines, Iowa, after tonsil surgery. She expected doctors to quickly treat him for pain and dehydration and send him home. But the computer system that automatically calculated medicine doses wasn’t working, the resident doctor informed her, and he mistakenly “gave him five times what was prescribed,” Kelley said. She later learned a cyberattack had taken down some of the hospital’s digital tools.

Paralyzed hospital

In 2022 [the](https://www.rfi.fr/en/france/20220822-hackers-demand-10m-to-end-cyber-attack-on-paris-regional-hospital) Corbeil-Essonnes hospital southeast of Paris was crippled by a cyberattack that lasted many days and forced the institution to return to pre-digital workflows.

The attack has blocked access to all medical imaging storage and patient admissions systems, so that staff had to resort to burning data onto DVDs to share information. Plus it was taking five times as long as usual to fill a pharmacy prescription, which needs to be prepared by hand.

Some 500 patients, including 13 children, were transferred to other institutions.

# 3. Types of Attacks on Medical devices

1. DoS (Denial-of-Service)

**What does it affect:**

Servers

Workstation

Monitors

Pumps

Ventilator

Communications

Body Heater

**How is it conducted:**

An attacker can flood the workstation in the patient's room by sending multiple communication packets over the internet.

**Techniques:**

Social Engineering,

Insertion of infected USB,

Malicious email

Electromagnetic interference.

2. Man-in-the-Middle

**What does it affect:**

Servers

Workstation

Monitors

Pumps

Ventilator

Communications

Body Heater

**How is it conducted:**

The attacker can steal the data or change it, so the recipient doesn’t receive the original (intended) data.

**Techniques:**

Social Engineering

Insertion of infected USB

Malicious email

3. Spyware

**What does it affect:**

EHR Servers

Central Monitoring Station

Infusion Pump

Communication box

**How is it conducted:**

An attacker installs spyware on a system/server. Such spyware enables the attacker to steal medical and private information about the patient and his/her treatment.

**Techniques:**

Social Engineering

Insertion of infected USB

Malicious email

4. Alert Attack – Missing Alerts (devices)

**What does it affect:**

Infusion and Syringe Pumps

Body Heater

Medical Ventilator and Monitor

**How is it conducted:**

An attacker can cause the device to fail to issue alerts when needed. In this case, the medical team will be unaware of the patient's condition, preventing the patient from receiving proper treatment.

**Techniques:**

Social Engineering

Insertion of infected USB

Malicious email

Firmware updates

5. Alert Attack – False Alerts (devices)

**What does it affect:**

Infusion and Syringe Pumps

Body Heater

Medical Ventilator and Monitor

**How is it conducted:**

An attacker can cause the device to fail to issue alerts when needed. The sound of the alarms may frustrate the medical team, and over time this may cause them to ignore the alarms (e.g., they may fail to respond to a patient's deteriorating condition).

**Techniques:**

Social Engineering

Insertion of infected USB

Malicious email

Firmware updates

6. Data Manipulation

**What does it affect:**

Servers

Workstation

Monitors

Pumps

Communications

Body Heater

**How is it conducted:**

An attacker can change existing data, so the patient's medical condition will be displayed incorrectly on the device.

**Techniques:**

Phishing

Insertion of infected USB

Firmware updates

7. Ransomware

**What does it affect:**

Servers

Workstations

**How is it conducted:**

An attacker can use ransomware for financial gain. The attacker may publish the patient's personal information, encrypt data, or prevent access to critical patient information.

**Techniques:**

Malicious email attachments and links, malicious USB device, insertion of infected USB and Firmware updates via Wi-Fi.

8. Delay Attacker

**What does it affect:**

Servers

Workstation

Monitors

Pumps

Ventilator

Communications

Body Heater

**How is it conducted:**

An attacker delays the transmission of data to medical devices or online displays. Most of the devices in the ICU require continuous and real-time data, so the medical team can monitor the patient's condition and provide him/her appropriate and timely treatment.

**Techniques:**

Malicious email attachments and links

Firmware updates

9. Session Hijacking

**What does it affect:**

Central Monitoring Station

Communication box

Infusion Pump

**How is it conducted:**

An attacker uses an existing session between devices in order to gain unauthorized access to information in a computer system. In this case, the attacker can send malicious commands, steal medical data, etc.

**Techniques:**

Malicious email attachments and links

Packet sniffing (cookie thefts)

10. Centralized Alert Attack – Missing Alerts (nurses’ station)

**What does it affect:**

Central Monitoring Station

Communication box

Infusion Pump

**How is it conducted:**

An attacker can cause the device to fail to issue alerts when needed. In this case, the medical team will be unaware of the patient's condition, preventing the patient from receiving proper treatment.

**Techniques:**

Social Engineering, Insertion of infected USB and Malicious email/phishing.

11. Centralized Alert Attack – False Alerts (nurses’ station)

**What does it affect:**

Central Monitoring Station

Communication box

Infusion Pump

**How is it conducted:**

An attacker can cause the device to fail to issue alerts when needed. In this case, the medical team will be unaware of the patient's condition, preventing the patient from receiving proper treatment.

**Techniques:**

Social Engineering

Insertion of infected USB

Malicious email/phishing

12. Malicious Firmware update

**What does it affect:**

Servers

Workstation

Monitors, Pumps

Ventilator

Communications

Body Heater

**How is it conducted:**

An attacker can install a malicious firmware update in order to change default commands or settings, so the devices will perform different actions than those required.

**Techniques:**

Social Engineering (the attacker impersonates the software company).

13. Cryptominer

**What does it affect:**

EHR Server

Infusion Pump

**How is it conducted:**

An attacker can use the server in order to mine cryptocurrency. The mining may impair system performance and cause high power consumption.

**Techniques:**

Social Engineering (penetration of malware crypto mining)

Cryptojacking (code hosted on Web Applications) .

14. Configuration manipulation

**What does it affect:**

Servers

Workstation

Monitors

Pumps

Ventilator

Communications

Body Heater

**How is it conducted:**

An attacker modifies/sets device settings without the medical team´s awareness, causing the device to operate differently than intended.

**Techniques:**

Social Engineering

Insertion of infected USB

Malicious email/with malicious file/link

Firmware Update

15. Abuse or Legitime Operations

**What does it affect:**

Monitors

**How is it conducted:**

An attacker obtains access to the device (e.g., by influencing a member of the medical team to insert an infected USB into the device), then the attacker can send commands to the device without the medical team's awareness.

**Techniques:**

Social Engineering

Insertion of infected USB

Malicious email/with malicious file/link

Firmware Update

# 4.1 Solutions – General ideas

Hardening the security on medical devices needs to start on the assembly line, and continue throughout the supply chain, from the processors and components inside the devices, to the software updated over the air.

Tips for the manufacturers

**1. Ensure that Medical devices are designed with security in mind**

From the very beginning, all medical devices need to have a clear, laid-out design that includes all of its features and cyber attack controls. One of the simplest ways to ensure that your medical device is designed with security in mind is to look at the company’s stakeholders; how data travels between them, who has access to certain data and who owns the data. A threat model can be produced and those who do not need access to the data can be locked out.

**2. Conduct a risk assessment**

One of the most effective ways to protect your medical devices from cyber attacks is through conducting a risk assessment on your current devices. This involves identifying any weak points, security threats and vulnerabilities that pose threats to your device’s security. The risk assessment can then work to improve on the areas that are vulnerable to cyber-attacks, as well as improve the overall security of your device.

**3. Consider a security alert**

A security alert is the simplest way to improve your medical devices from cyber-attacks. You simply review any breaches, viruses or threats to your medical device over the last year. You are then able to identify exactly how and where they are coming from. Once you have this information, you know exactly where to improve. The only downside to this technique is that you have to fall victim to a cyber attack first. Be sure to make use of an intrusion detection system that monitors your system and detects any malicious activity and reports it to you.

**4. Conduct penetration testing**

This is a method that is commonly used by institutions, such as banks and law firms. These institutions hire a professional ‘hacker’ to attempt to breach their security. Should medical device manufacturers make use of this service, the organization will be able to see just how easy it is for cyber-attackers to gain access to data and information, cause disruption to organizational processes and operations and, possibly, have a negative, or even tragic, impact on the patients health or recovery. Penetration testing has proven to be one of the best ways to identify the various weaknesses and vulnerabilities in your security system.

Best-practice technologies for connected device security

**1. Secure Boot**

Provides embedded software APIs that ensure software integrity from the initial ‘power on’ to application execution and enable developers to securely code sign boot loaders, microkernels, operating systems, application code, and data.

**2. Device Identity Certificates**

Injecting digital certificates into devices during manufacturing, enabling devices to be authenticated when installed on a network and before being able to communicate with other devices in the system. This ensures devices cannot be spoofed and provides protection from counterfeit devices being introduced into the network.

**3. Embedded Firewall**

Works with Real Time Operating Systems (RTOS) and Linux to configure and enforce filtering rules, preventing communication with unauthorized devices and blocking malicious messages.

**4. Secure Element Integration**

OEMs and medical device manufacturers should integrate a variety of Secure Elements, such as Trusted Platform Module (TPM) compliant secure elements to provide secure boot, PKI enrollment using key-pairs generated within the secure element, and device attestation.

**5. Secure Remote Updates**

Validate firmware is authenticated and unmodified before permitting installation of firmware updates, ensuring components have not been modified and are authenticated modules from the original equipment manufacturer (OEM).

# 4.2 Solution – attack mitigations

1. DoS (Denial-of-Service)

* Intercept the incoming traffic upstream to filter out the attack traffic from the legitimate traffic using an Internet Service Provider (ISP) or by a 3rd party such as a Content Delivery Network (CDN) or providers specializing in DoS mitigations.
* Depending on flood volume, on-premises filtering may be possible by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.
* Analyze the risk associated to critical resources being affected by Network DoS attacks and create a disaster recovery plan/business continuity plan to respond to incidents.

2. Man-in-the-Middle

* Disable legacy network protocols.
* Ensure that all wired and/or wireless traffic is encrypted appropriately. Use Kerberos and ensure web traffic that may contain credentials is protected by SSL/TLS.
* Use network appliances and host-based security software to block network traffic that is not necessary within the environment.
* Limit access to network infrastructure and resources that can be used to reshape traffic.
* Network intrusion detection and prevention systems that can identify traffic patterns indicative of a suspicious activity.
* Network segmentation can be used to isolate infrastructure components that do not require broad network access.
* Train users to be suspicious about certificate errors. Adversaries may use their own certificates in an attempt to intercept HTTPS traffic.

3. Spyware

* Use trusted antivirus software with anti-spyware and anti-malware features.
* Don’t download suspicious-looking email attachments.
* Don’t click on online pop-ups (or block them entirely with a secure browser).
* Don’t open links received in text messages from unknown numbers.
* Avoid chatting with strangers in messaging apps.
* Keep your computer and mobile operating systems up-to-date.

4. Alert Attack – Missing Alerts (devices)

* Fine tuning of monitoring rules helps to reduce them.
* Use a CSPM(Cloud Security Posture Management) and other monitoring tools
* Provide easy one-click remediation so security staff can quickly and easily mitigate common threats or even provide step-by-step instructions on how to remediate these threats.
* With CSPM you can: contextualize alerts, provide actionable insights, custom rules and threat level flagging, and quick remediation of threats and vulnerabilities.

5. Alert Attack – False Alerts (devices)

* Fine tuning of monitoring rules help to reduce them.
* Use a CSPM (Cloud Security Posture Management) and other monitoring tools
* Provide easy one-click remediation so security staff can quickly and easily mitigate common threats or even provide step-by-step instructions on how to remediate these threats.
* With CSPM you can: contextualize alerts, provide actionable insights, custom rules and threat level flagging, and quick remediation of threats and vulnerabilities.

6. Data Manipulation

* Encrypt Sensitive Information: Consider encrypting important information to reduce an adversary’s ability to perform tailored data modifications.
* Network Segmentation: Identify critical business and system processes that may be targeted by adversaries and work to isolate and secure those systems against unauthorized access and tampering.
* Remote Data Storage: Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.
* Restrict File and Directory Permissions: Ensure least privilege principles are applied to important information resources to reduce exposure to data manipulation risk.

7. Ransomware

* Antivirus/Antimalware: Anti-virus can also automatically quarantine suspicious files.
* Network Intrusion Prevention: Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.
* Restrict Web-Based Content: Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments.
* Software Configuration: Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.
* User training: Users can be trained to identify social engineering techniques and spear phishing emails.

8. Delay Attacker

* Antivirus/Antimalware: Anti-virus can also automatically quarantine suspicious files.
* Network Intrusion Prevention: Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.
* Restrict Web-Based Content: Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments.
* Software Configuration: Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.
* User training: Users can be trained to identify social engineering techniques and spear phishing emails.

9. Session Hijacking

* Use strong passwords and multifactor authentication. These techniques protect accounts from being accessed by hackers if they manage to steal a user’s session ID.
* Only share session IDs with trusted sources. Be careful when sharing links or sending requests to websites, as these may include session IDs.
* Use a VPN. A VPN helps prevent attackers from intercepting traffic, making it more difficult for them to steal session IDs (McCann & Hardy, 2022).
* Keep software up to date. Make sure to keep operating systems and software up to date with the latest security patches to prevent attackers from exploiting vulnerabilities to access users’ sessions.
* Take cybersecurity training. Cybersecurity threats are constantly evolving, so it’s essential to stay informed on the latest attack techniques and how to prevent them. Consider getting certified in various cybersecurity domains, including ethical hacking, incident handling, and penetration testing.

10. Centralized Alert Attack – Missing Alerts (nurses’ station)

* Fine tuning of monitoring rules help to reduce them.
* Use a CSPM (Cloud Security Posture Management) and other monitoring tools
* Provide easy one-click remediation so security staff can quickly and easily mitigate common threats or even provide step-by-step instructions on how to remediate these threats.
* With CSPM you can: contextualize alerts, provide actionable insights, custom rules and threat level flagging, and quick remediation of threats and vulnerabilities.

11. Centralized Alert Attack – False Alerts (nurses’ station)

* Fine tuning of monitoring rules help to reduce them.
* Use a CSPM (Cloud Security Posture Management) and other monitoring tools
* Provide easy one-click remediation so security staff can quickly and easily mitigate common threats or even provide step-by-step instructions on how to remediate these threats.
* With CSPM you can: contextualize alerts, provide actionable insights, custom rules and threat level flagging, and quick remediation of threats and vulnerabilities.

12. Malicious Firmware update

* Access Management: All devices or systems changes, including all administrative functions, should require authentication.
* Audit: Perform integrity checks of firmware before uploading it on a device. Utilize cryptographic hashes to verify the firmware has not been tampered with by comparing it to a trusted hash of the firmware.
* Boot Integrity: Check the integrity of the existing BIOS or EFI to determine if it is vulnerable to modification. Use Trusted Platform Module technology. Move system's root of trust to hardware to prevent tampering with the SPI flash memory. Technologies such as Intel Boot Guard can assist with this.
* Code Signing: Devices should verify that firmware has been properly signed by the vendor before allowing installation.
* Communication Authenticity: Protocols used for device management should authenticate all network messages to prevent unauthorized system changes.
* Encrypt Network Traffic: The encryption of firmware should be considered to prevent adversaries from identifying possible vulnerabilities within the firmware.
* Encrypt Sensitive Information: The encryption of firmware should be considered to prevent adversaries from identifying possible vulnerabilities within the firmware.
* Filter Network Traffic: Filter for protocols and payloads associated with firmware activation or updating activity.
* Human User Authentication: Devices that allow remote management of firmware should require authentication before allowing any changes. The authentication mechanisms should also support Account Use Policies, Password Policies, and User Account Management.
* Network Allowlists: Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations.
* Network Segmentation: Segment operational network and systems to restrict access to critical system functions to predetermined management systems.
* Software Process and Device Authentication: Authenticate connections from software and devices to prevent unauthorized systems from accessing protected management functions.
* Update Software: Patch the BIOS and EFI as necessary.

13. Cryptominer

* Practice strong security hygiene. IT hygiene is foundational to security. Regularly patching vulnerable applications and operating systems, and protecting privileged user accounts, are essential practices for optimal security posture.
* Educate your employees. Ensure all employees complete comprehensive training on the importance of keeping sensitive data safe, best practices to prevent crypto jacking, and a thorough understanding on the different ways cyber attacks can happen.
* Deploy a true next-generation endpoint protection platform (EPP). Organizations must be prepared to prevent and detect all threats, including known and unknown malware, as well as identifying in-memory attacks. This requires a solution that includes next-gen AV protection, as well as endpoint detection and response (EDR), to prevent attacks and gain full visibility throughout the environment.

14. Configuration manipulation

* Encrypt Sensitive Information: Consider encrypting important information to reduce an adversary’s ability to perform tailored data modifications.
* Network Segmentation: Identify critical business and system processes that may be targeted by adversaries and work to isolate and secure those systems against unauthorized access and tampering.
* Remote Data Storage: Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.
* Restrict File and Directory Permissions: Ensure least privilege principles are applied to important information resources to reduce exposure to data manipulation risk.

15. Abuse or Legitime Operations

* Encrypt Sensitive Information: Consider encrypting important information to reduce an adversary’s ability to perform tailored data modifications.
* Network Segmentation: Identify critical business and system processes that may be targeted by adversaries and work to isolate and secure those systems against unauthorized access and tampering.
* Remote Data Storage: Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.
* Restrict File and Directory Permissions: Ensure least privilege principles are applied to important information resources to reduce exposure to data manipulation risk.

# 4.3 New suggested solutions

New regulations concerning cybersecurity

As recent as December 29, 2022, the Consolidated Appropriations Act, 2023 ("Omnibus") was signed into law. Section 3305 of the Omnibus — "Ensuring Cybersecurity of Medical Devices" —amended the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding section 524B, Ensuring Cybersecurity of Devices.

As part of the new law, all new medical device applicants must now submit a plan on how to "monitor, identify, and address" cybersecurity issues, as well as create a process that provides "reasonable assurance" that the device in question is protected. Applicants will also need to make security updates and patches available on a regular schedule and in critical situations, and provide the FDA with "a software bill of materials," including any open-source or other software their devices use.

At the same time, the FDA must also update its medical device cybersecurity guidance at least every two years.

As a regulator, the FDA has a leadership role in creating expectations that manufacturers will proactively minimize risk by building cybersecurity into products by design, providing security tools to health systems, and updating and patching devices as new intelligence and threats emerge.

Coordinated cooperation

Greater collaboration among healthcare providers, medical device manufacturers, and lawmakers and regulators will lead to predictability and consistency in cybersecurity management.

It’s vital that manufacturers incorporate and sustain industry-identified cybersecurity best practices and data management controls over the reasonable economic life of IoMT devices and equipment. Hospitals today are taking critical security steps to safeguard clinical technologies, information systems and their network environment(s) while enhancing data protection capabilities – but cooperative and accountable action with manufacturers is necessary to further reduce cyber vulnerabilities and the unsustainable costs they drive.

Specific cybersecurity technical writing in contracts helps mitigate risk and keeps device manufacturers accountable for their role in the security management process.

Manufacturers must share with health systems the responsibility for safeguarding the confidentiality of patient data, maintaining data integrity, and ensuring the continued availability and functionality of the device system itself.

Regulators should also consider revisiting the landscape for security breach penalties, they should be proportionally applied to the product manufacturer and the health system experiencing the breach based on their relative contribution to the breach’s root cause and using objective industry best-practices as the standard.

Incorporating cybersecurity in academic programs

Add cybersecurity courses to the curriculum to the Universities and colleges existing computer science, engineering, or business programs, covering topics such as network security, digital forensics, cryptography, and ethical hacking. The curriculum can also include hands-on labs and practical exercises to give students real-world experience in addressing cybersecurity challenges.

Incorporating cybersecurity academic programs can bring many benefits, enhancing their critical thinking and problem-solving skills, and promoting cyber awareness and safety in the professionals involved in the design and development of Medical Devices.

Establish cybersecurity certificates or minors: Schools can offer cybersecurity certificates or minors that allow students to specialize in cybersecurity while completing their major and start navigating in the different related industries. These programs can be designed to provide students with a broad understanding of cybersecurity concepts, as well as specialized knowledge in specific areas of cybersecurity.

Encourage research in cybersecurity: Universities can encourage students to pursue cybersecurity research through student projects, capstone courses, or internships. This can help students to develop critical thinking and problem-solving skills and contribute to the advancement of cybersecurity knowledge.

Promote cybersecurity awareness and safety: Universities can also promote cybersecurity awareness and safety by providing training to students, faculty, and staff on how to protect their digital assets and personal information. This can include educating students on the risks of social engineering, phishing, and other cyber threats, and providing guidance on how to create strong passwords and secure their devices.

Incorporating cybersecurity into academic programs can help prepare the next generation of cybersecurity professionals and enhance the security of digital assets. By promoting cyber awareness and safety, universities can also contribute to a safer and more secure digital world.

# 5. Conclusion

As we could see, medical devices are often at a great risk of being compromised. Often not as a direct attack, but as a collateral damage from a big-scale attack on a hospital or a healthcare facility. We reviewed the current situation in this field, compiled a list of the most common attacks and the ways to mitigate them and also proposed some new ones.

The increasing use of medical devices and technology in healthcare has brought about significant benefits in terms of improved patient outcomes and increased efficiency. However, it has also brought about new cybersecurity challenges and risks, which cannot be ignored.

Therefore, it is critical to prioritize cybersecurity measures in medical devices and healthcare systems to ensure patient safety and confidentiality. This can be achieved through increased awareness, education, increase and enforce regulations in the whole manufacturing process and life cycle of the medical devices, and collaboration among healthcare providers, manufacturers, regulators, and cybersecurity experts.

By taking a proactive approach towards cybersecurity in healthcare, we can ensure the benefits of technology are maximized while mitigating the associated risks.

# 6. Appendix

The Great Table of Attacks and mitigations

| **Attack** | **Description** | **Attacked Devices** | **Mitigations** |
| --- | --- | --- | --- |
| **DoS**  **(Denial-of- Service)** | An attacker can flood the workstation in the patient's room by sending multiple communication packets over the internet;this might prevent the medical team from accessing the EHR, interfering with patient care, the medical team would have to revert to using paperwork which will be inefficient.  **Vector:**   * Social Engineering Techniques * Insertion of infected USB. * Malicious email * Electromagnetic interference | * EHR Server * Central Monitoring Station * Communication box * Workstation * Infusion Pump * Syringe Pump * Body heater * Medical Ventilator * Feeding Pump * Monitor | When flood volumes exceed the capacity of the network connection being targeted, it is typically necessary to intercept the incoming traffic upstream to filter out the attack traffic from the legitimate traffic. Such defenses can be provided by the hosting Internet Service Provider (ISP) or by a 3rd party such as a Content Delivery Network (CDN) or providers specializing in DoS mitigations.  Depending on flood volume, on-premises filtering may be possible by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.  As immediate response may require rapid engagement of 3rd parties, analyze the risk associated to critical resources being affected by Network DoS attacks and create a disaster recovery plan/business continuity plan to respond to incidents. |
| **Electromagnetic interference** | An attacker emits disruptive radiation near a device which affects the availability or activity of the device. For example the Syringe Pump which operates based on infrared radiation technology.   **Vector:**   * Disruptive radiation near the device | * Infusion Pump * Syringe Pump |  |
| **Man-in-the-**  **Middle** | The attacker can steal the data or change it, so the recipient doesn’t receive the original (intended)data. In this case, the patient may not receive the proper treatment, since the medical information shared between devices is incorrect.  **Vector:**   * Social Engineering Techniques * Insertion of infected USB * Malicious email | * EHR Server * Central Monitoring Station * Communication box * Workstation * Infusion Pump * Syringe Pump * Body heater * Medical Ventilator * Monitor | Disable legacy network protocols that may be used to intercept network traffic if applicable, especially those that are not needed within an environment.  Ensure that all wired and/or wireless traffic is encrypted appropriately. Use best practices for authentication protocols, such as Kerberos, and ensure web traffic that may contain credentials is protected by SSL/TLS.  Use network appliances and host-based security software to block network traffic that is not necessary within the environment, such as legacy protocols that may be leveraged for AiTM conditions.  Limit access to network infrastructure and resources that can be used to reshape traffic or otherwise produce AiTM conditions.  Network intrusion detection and prevention systems that can identify traffic patterns indicative of AiTM activity can be used to mitigate activity at the network level.  Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of AiTM activity.  Train users to be suspicious about certificate errors. Adversaries may use their own certificates in an attempt to intercept HTTPS traffic. Certificate errors may arise when the application’s certificate does not match the one expected by the host. |
| **Spyware** | An attacker installs spyware on a system/server. Such spyware enables the attacker to steal medical and private information about the patient and his/her treatment.  **Vector:**   * Social Engineering Techniques * Insertion of infected USB * Malicious email | * EHR Server * Central Monitoring Station * Communication box * Infusion Pump | Use trusted antivirus software with anti-spyware and anti-malware features  Don’t download suspicious-looking email attachments  Don’t click on online pop-ups (or block them entirely with a secure browser)  Don’t open links received in text messages from unknown numbers  Avoid chatting with strangers in messaging apps  Keep your computer and mobile operating systems up-to-date |
| **Alert Attack – Missing Alerts**  **(devices)** | An attacker can cause the device to fail to issue alerts when they are needed. In this case, the medical team will be unaware of the patient's condition, preventing the patient from receiving proper treatment. For example, an attacker can insert an infected USB(such as a keyboard) into the server of the central monitoring station in order to disable the monitor´s alerts remotely.  **Vector:**   * Social Engineering Techniques * Insertion of infected USB * Malicious email * Firmware updates | * Infusion Pump * Syringe Pump * Body heater * Medical Ventilator * Monitor | You can’t eradicate false alerts, unfortunately. Fine Tuning monitoring rules help reduce them, but the reduction is insignificant at best. However, using a CSPM and other monitoring tools can help cybersecurity professionals contextualize the alerts or provide sufficient information for factual investigation and threat mitigation. Another possible countermeasure is to provide easy one-click remediation so security staff can quickly and easily mitigate common threats or even provide step-by-step instructions on how to remediate these threats.  Below are some features to consider in a CPSM tool to help reduce alert fatigue for your security staff.  **1. Contextualize alerts:**  A Cloud Security Posture Management (CSPM) should allow you to quickly identify and zoom in on suspected assets to understand the context of the threat in light of configuration and activity perspectives associated with event severities.  This significantly reduces the time required to investigate each alert. You can quickly identify and dismiss a false alert, take immediate action to mitigate the threat, or remediate the vulnerability.  **2. Provide actionable insights**  Prevention is always better than cure. Why wait for the alerts to come through? Imagine seeing a history of all changes made to your multi-cloud environment, each accompanied by an actionable insight that helps you know of potential threats to your cloud infrastructure and even guides you on taking proactive action to mitigate the potential threats.  Having such a feature will also allow your organization to stay audit-ready for international standards such as ISO 27001, SOC 2, industry-specific and territorial standards such as PCI DSS for the payments industry, Singapore's MAS TRM, Indonesia’s POJK 38, Australia’s APRA, and the Thai PDPA.  **3. Custom rules and threat level flagging**  Every organization has unique security and business needs; yours is no different. You may have some in-house security rules to monitor. Some organizations also have cloud assets more important than others compared to their industry peers.  You can reduce alert fatigue by monitoring these in-house rules and assets, setting the right criticality flags for each, and prioritizing them. For example, you may want to get alerts whenever there’s any change on an AWS S3 bucket containing Personal Identifiable Information (PII) data.  Going further, a CSPM should allow you to create monitoring groups where you can specify the criticality level and automatically apply it to other flagged critical assets in your organization. This will help you reduce alert fatigue.  **4. Quick remediation of threats and vulnerabilities**  Your security staff should also be able to quickly and easily remediate common and minor vulnerabilities and threats and receive step-by-step instructions on mitigating specific vulnerabilities.  In fact, selecting all common and minor vulnerabilities and then bulk-remediating them with a single click of the mouse will significantly reduce the time your security staff spends on remediation.  Another way you can help your security staff stave off alert fatigue and upskill simultaneously is by ensuring that the CSPM tool offers step-by-step instructions for remediating vulnerabilities. For example, your security staff may choose to remediate common and minor vulnerabilities with the one-click option while using the step-by-step playbook for more complex remediations and learn from that. |
| **Alert Attack – False Alerts**  **(devices)** | An attacker can cause a device to issue an alert when it is not needed. The sound of the alarms may frustrate the medical team, and over time this may cause them to ignore the alarms(e.g., they may fail to respond to a patient's deteriorating condition). For example , an attacker can utilize social engineering techniques in order to encourage someone to insert an infected USB(such as keyboard) into the server of the central monitoring station; this will enable the attacker to change the required threshold for alerts, so the monitor´s alerts are triggered frequently.  **Vector:**   * Social Engineering Techniques * Insertion of infected USB * Malicious email * Firmware updates | * Infusion Pump * Syringe Pump * Body heater * Medical Ventilator * Monitor | You can apply the same mitigations of **Alert Attack -- Missing Alerts (devices).** |
| **Data Manipulation** | An attacker can change existing data, so the patient's medical condition will be displayed incorrectly on the device.  **Vector:**   * Email/phishing * Firmware updates * Insertion of infected USB | * EHR Server * Central Monitoring Station * Communication box * Infusion Pump * Syringe Pump * Body heater * Monitor | **Encrypt Sensitive Information:**  Consider encrypting important information to reduce an adversary’s ability to perform tailored data modifications.  **Network Segmentation:**  Identify critical business and system processes that may be targeted by adversaries and work to isolate and secure those systems against unauthorized access and tampering.  **Remote Data Storage:**  Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data. Ensure backups are stored off system and are protected from common methods adversaries may use to gain access and manipulate backups.  **Restrict File and Directory Permissions:**  Ensure least privilege principles are applied to important information resources to reduce exposure to data manipulation risk. |
| **Ransomware** | An attacker can use ransomware for financial gain. The attacker may publish the patient's personal information, encrypt data, or prevent access to critical patient information.  **Vector:**   * Malicious email attachments and links * Malicious USB device * Firmware update via Wi-Fi | * EHR Server * Workstation | **Antivirus/Antimalware:**  Anti-virus can also automatically quarantine suspicious files.  **Network Intrusion Prevention:**  Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.  **Restrict Web-Based Content:**  Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments.  **Software Configuration:**  Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.  **User Training:**  Users can be trained to identify social engineering techniques and spear phishing emails. |
| **Delay Attack** | An attacker delays the transmission of data to medical devices or online displays. Most of the devices in the ICU require continuous and real-time data, so the medical team can monitor the patient's condition and provide him/her appropriate and timely treatment.  **Vector:**   * Malicious email attachments and links * Firmware update | * EHR Server * Central Monitoring Station * Communication box * Workstation * Infusion Pump * Syringe Pump * Body heater * Medical Ventilator * Feeding Pump * Monitor | You can apply the same mitigations as **Ransomware**. |
| **Session Hijacking** | An attacker uses an existing session between devices in order to gain unauthorized access to information in a computer system. In this case, the attacker can send malicious commands, steal medical data, etc.  **Vector:**   * Malicious email (with malicious files/links). * Packet sniffing (cookie thefts) | * Central Monitoring Station * Communication box * Infusion Pump | **Use strong passwords and multifactor authentication:** These techniques protect accounts from being accessed by hackers if they manage to steal a user’s session ID.  **Only share session IDs with trusted sources:** Be careful when sharing links or sending requests to websites, as these may include session IDs.  **Use a VPN:**  A VPN helps prevent attackers from intercepting traffic, making it more difficult for them to steal session IDs.  **Keep software up to date:**  Make sure to keep operating systems and software up to date with the latest security patches to prevent attackers from exploiting vulnerabilities to access users’ sessions.  **Take cybersecurity training:** Cybersecurity threats are constantly evolving, so it’s essential to stay informed on the latest attack techniques and how to prevent them. Consider getting certified in various cybersecurity domains, including ethical hacking, incident handling, and penetration testing. |
| **Centralized Alert Attack – Missing Alerts (nurses’ station)** | Similar to **Alert Attack – Missing Alerts (devices)**  **Vector:**   * Social Engineering Techniques * Insertion of infected USB * Malicious email/phishing | * Central Monitoring Station * Communication box * Infusion Pump | You can apply the same mitigations of **Alert Attack – Missing Alerts (devices**). |
| **Centralized Alert Attack -- False Alerts (nurses’ station)** | Similar to **Alert Attack – False Alerts (devices)**  **Vector:**   * Social Engineering Techniques * Insertion of infected USB * Malicious email/phishing | * Central Monitoring Station * Communication box * Infusion Pump | You can apply the same mitigations of **Alert Attack -- Missing Alerts (devices).** |
| **Malicious Firmware Update** | An attacker can install a malicious firmware update in order to change default commands or settings, so the devices will perform different actions than those required.  **Vector:**   * Social engineering (the attacker impersonates the software company) | * EHR Server * Central Monitoring Station * Communication box * Syringe Pump * Body heater * Medical Ventilator * Feeding Pump * Monitor | **Access Management:**  All devices or systems changes, including all administrative functions, should require authentication. Consider using access management technologies to enforce authorization on all management interface access attempts, especially when the device does not inherently provide strong authentication and authorization functions.  **Audit:**  Perform integrity checks of firmware before uploading it on a device. Utilize cryptographic hashes to verify the firmware has not been tampered with by comparing it to a trusted hash of the firmware. This could be from trusted data sources (e.g., vendor site) or through a third-party verification service.  **Boot Integrity:**  Check the integrity of the existing BIOS or EFI to determine if it is vulnerable to modification. Use Trusted Platform Module technology. Move system's root of trust to hardware to prevent tampering with the SPI flash memory. Technologies such as Intel Boot Guard can assist with this.    **Code Signing:**  Devices should verify that firmware has been properly signed by the vendor before allowing installation.  **Communication Authenticity:**  Protocols used for device management should authenticate all network messages to prevent unauthorized system changes.  **Encrypt Network Traffic:**  The encryption of firmware should be considered to prevent adversaries from identifying possible vulnerabilities within the firmware.  **Encrypt Sensitive Information:**  The encryption of firmware should be considered to prevent adversaries from identifying possible vulnerabilities within the firmware.  **Filter Network Traffic:**  Filter for protocols and payloads associated with firmware activation or updating activity.  **Human User Authentication:**  Devices that allow remote management of firmware should require authentication before allowing any changes. The authentication mechanisms should also support Account Use Policies, Password Policies, and User Account Management.  **Network Allowlists:**  Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations.  **Network Segmentation:**  Segment operational network and systems to restrict access to critical system functions to predetermined management systems.  **Software Process and Device Authentication:**  Authenticate connections from software and devices to prevent unauthorized systems from accessing protected management functions.  **Update Software:**  Patch the BIOS and EFI as necessary. |
| **Cryptominer** | An attacker can use the server in order to mine cryptocurrency. The mining may impair system performance and cause high power consumption.  **Vector:**   * Cryptojacking (code hosted on Web Applications) * Social engineering (penetration of malware crypto mining) | * EHR Server * Infusion Pump | **Practice strong security hygiene:**  IT hygiene is foundational to security. Regularly patching vulnerable applications and operating systems, and protecting privileged user accounts, are essential practices for optimal security posture.  **Educate your employees:** Ensure all employees complete comprehensive training on the importance of keeping sensitive data safe, best practices to prevent crypto jacking, and a thorough understanding on the different ways cyber attacks can happen.  **Deploy a true next-generation endpoint protection platform (EPP):**  Organizations must be prepared to prevent and detect all threats, including known and unknown malware, as well as identifying in-memory attacks. This requires a solution that includes next-gen AV protection, as well as endpoint detection and response (EDR), to prevent attacks and gain full visibility throughout the environment. |
| **Configuration manipulation** | An attacker modifies/sets device settings without the medical team´s awareness, causing the device to operate differently than intended.  **Vector**:   * Social Engineering Techniques * Insertion of infected USB * Malicious email/with malicious file/link * Firmware update | * EHR Server * Central Monitoring Station * Communication box * Workstation * Infusion Pump * Syringe Pump * Body heater * Medical Ventilator * Feeding Pump * Monitor | You can apply the same mitigations as **Data Manipulation**. |
| **Abuse or Legitime Operations** | An attacker obtains access to the device (e.g., by influencing a member of the medical team to insert an infected USB into the device), then the attacker can send commands to the device without the medical team's awareness.  **Vector:**   * Social Engineering Techniques * Insertion of infected USB * Malicious email/with malicious file/link. * Firmware update | * Monitor | You can apply the same mitigations as **Data Manipulation**. |

Largest Healthcare Data Breaches in the USA (2009-2023)

| **Rank** | **Name of Covered Entity** | **Year** | **Covered Entity Type** | **Individuals Affected** | **Type of Breach** |
| --- | --- | --- | --- | --- | --- |
| 1 | Anthem Inc. | 2015 | Health Plan | 78,800,000 | Hacking/IT Incident |
| 2 | American Medical Collection Agency | 2019 | Business Associate | 26,059,725 | Hacking/IT Incident |
| 3 | Premera Blue Cross | 2015 | Health Plan | 11,000,000 | Hacking/IT Incident |
| 4 | Excellus Health Plan, Inc. | 2015 | Health Plan | 10,000,000 | Hacking/IT Incident |
| 5 | Science Applications International Corporation | 2011 | Business Associate | 4,900,000 | Loss |
| 6 | University of California, Los Angeles Health | 2015 | Healthcare Provider | 4,500,000 | Hacking/IT Incident |
| 7 | Community Health Systems Professional Services Corporations | 2014 | Business Associate | 4,500,000 | Hacking/IT Incident |
| 8 | Advocate Health and Hospitals Corporation, d/b/a Advocate Medical Group | 2013 | Healthcare Provider | 4,029,530 | Theft |
| 9 | OneTouchPoint | 2022 | Business Associate | 4,112,892 | Ransomware attack |
| 10 | Medical Informatics Engineering | 2015 | Business Associate | 3,900,000 | Hacking/IT Incident |

Links

1. <https://attack.mitre.org/mitigations/M1037/>
2. <https://attack.mitre.org/techniques/T0857/>
3. <https://attack.mitre.org/techniques/T1557/>
4. <https://attack.mitre.org/techniques/T1565/>
5. <https://attack.mitre.org/techniques/T1566/001/>
6. <https://expertinsights.com/insights/healthcare-cyber-attack-statistics/>
7. <https://explore.avertium.com/resource/cyber-threats-in-the-healthcare-industry>
8. <https://healthitsecurity.com/features/the-threat-of-distributed-denial-of-service-attacks-in-healthcare>
9. <https://ironscales.com/blog/ironscales-releases-findings-from-state-of-cybersecurity-survey/>
10. <https://learn.g2.com/alert-fatigue>
11. <https://therecord.media/fbi-warns-of-vulnerabilities-in-medical-devices-following-several-cisa-alerts/>
12. https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals
13. https://www.al.com/news/2021/10/alabama-mom-claims-baby-died-because-of-undisclosed-cyberattack-fights-for-hospital-records.html
14. <https://www.avast.com/c-spyware>
15. <https://www.cisecurity.org/insights/blog/ddos-attacks-in-the-healthcare-sector>
16. <https://www.crowdstrike.com/cybersecurity-101/cryptojacking/>
17. <https://www.cynerio.com/blog/cynerio-research-finds-critical-medical-device-risks-continue-to-threaten-hospital-security-and-patient-safety>
18. <https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/how-to-prevent-session-hijacking-attacks/>
19. <https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/how-to-prevent-session-hijacking-attacks/>
20. <https://www.f5.com/company/news/features/phishing-attacks-soar-220--during-covid-19-peak-as-cybercriminal>
21. <https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=68478cba5650>
22. <https://www.g2.com/categories/cloud-security-posture-management-cspm>
23. <https://www.healthcareitnews.com/news/direct-line-between-hospital-cyberattacks-and-patient-mortality-report-shows>
24. <https://www.hipaajournal.com/average-cost-of-a-healthcare-data-breach-9-42-million-2021/>
25. <https://www.hipaajournal.com/healthcare-data-breach-statistics/>
26. <https://www.jpost.com/cybertech/cyber-attacks-on-hospitals-can-kill-heres-why-682057>
27. <https://www.nbcnews.com/tech/security/ransomware-attacks-hospitals-take-toll-patients-rcna54090>
28. <https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf>
29. <https://www.proofpoint.com/us/cyber-insecurity-in-healthcare>
30. <https://www.researchgate.net/publication/340326809_SEC-C-U_The_Security_of_Intensive_Care_Unit_Medical_Devices_and_Their_Ecosystems>
31. https://www.rfi.fr/en/france/20220902-paralysed-french-hospital-fights-cyber-attack-as-hackers-lower-ransom-demand
32. <https://www.statista.com/statistics/1237131/cybersecurity-incidents-in-healthcare-organizations-us/>
33. [https://www.tausight.com/healthcare-and-cybersecurity-key-statistics](https://www.tausight.com/healthcare-and-cybersecurity-key-statistics/)
34. <https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise>