Research:

CDOTrends.

Statistics:

- According to a recent study by healthcare cybersecurity provider Cynerio, 56% of hospitals have had their IoT/IoMT devices attacked in the past two years.
- 88% of data breaches involved IoT devices.
- An alarming figure is that 53% of medical IoT devices have at least one critical vulnerability.
- 47% of attacked hospitals pay the ransom when victimized by ransomware.
- More alarming is that 24% of hospitals reported increased mortality rates after a cyberattack.

Background:

- The capabilities of IoT devices have become indispensable in so many ways. They lower costs, deliver vital data and reduce the workload on humans. In terms of uptake, the healthcare industry will only use more IoT devices.
- IV pumps are the most common healthcare IoT device and make up 38% of an average hospital's IoT footprint.
    - Unfortunately, more than 70% of those pumps have a vulnerability that would jeopardize patient safety, data confidentiality, or service availability "if it were to be exploited by an adversary."
- Healthcare providers typically maintain spreadsheets of their connected IoT devices, which can be scanned, and some technology companies offer these services. The problem is that not every hospital maintains an accurate list; some devices defy scanning and require further investigation.
- The most common device risk remains insecure passwords, and some hospitals find that an audit will reveal that many of their older devices do not even have passwords set

Fierce Healthcare

Statistics:

- There are 10 million to 15 million medical devices in U.S. hospitals today with an average of 10 to 15 connected medical devices per patient bed
- Healthcare security leaders ranked compromised customer data as their top concern as a result of a cyberattack (39%), followed by patient safety (20%) and stolen intellectual property (12%)
- Device manufacturers are aware of these security gaps, as 82% of IoT device makers say they are concerned the devices are not adequately secured from a cyberattack
- An alarming number of devices in healthcare organizations, about 70%, will be running unsupported Windows operating systems by January 2020

International Electrotechnical Commission.

Statistics:

- Cyber attacks against healthcare organizations across the world increased by 74% in 2022, according to Check Point Research

- In a 2021 study, they found that mortality rates increased at a quarter of the hospitals surveyed following a ransomware attack
- According to CyberPeace Institute their data says that an average cyber attack on a health care system leads to 19 days of disruption in patient care

Background:

- IEC develops cyber security standards that can help to ensure the cyber security of medical devices and protect patient safety
- IEC TR 60601-4-5: provides security specifications for medical electrical equipment and systems connected to hospital IT networks
    - 7 foundational requirements: authentication control, use control, system integrity, data confidentiality, restricted data flow, timely response to events, and resource availability
- IEC 80001 is recommended for healthcare organizations and medical device manufacturers that use networked medical devices. It can also help organizations meet regulatory requirements related to medical device safety and security.

Business News Daily

Background:

- Even though medical devices don't always store significant amounts of patient data, they can be valuable entry points for attackers to access data-rich servers
    - Keeping these entry points updated and secure must remain a priority for the healthcare industry to reduce the costs and damage of unauthorized access
- The healthcare industry is vulnerable to cyberattacks, including ransomware, malware, data breaches, DDoS and cryptojacking.
- Patient care and safety, data loss, and damage to a healthcare provider's reputation are among the consequences of networks being breached.
- On average, a room contains 15 to 20 connected medical devices.
    - A large hospital would have as much as 85,000 connected devices
    - Each of these devices has a significant role in the delivery of care and operational efficiency, each connected device can also open the door to a malicious cyberattack

REAL EVENTS:

78 yo Women in Germany

- Location: Dusseldorf, Germany
- September 11
- 78 year old women will be suffering from an aortic aneurysm
- When the local hospital was called they were told that they are unavailable, which means that they have to go to a different hospital.
    - The other hospital was 32 km away which delayed the patients treatment by an hour
- She was not able to make it, and passed shortly after
- This was caused by a ransomware attack where the hackers encrypt data and then demand payment to unlock it, which forced the ambulance to turn away

- This would greatly affect the digital infrastructure that the hospital relies since it keeps tracks of the beds, doctors, and treatments
    - And how an attack can force a cancellation of as much as a 100 operations and procedures
- When the hospital was trying to find out who were the ones who were the hackers, they were not able to find out
    - This brings up the question, even though ransomware is taking place, can they be blamed for the death of a patient?
        - Not really.

[Women Sued Alabama Hospital for the Death of Her Daughter]

- Location: Alabama
- In 2020
- A woman (Ms. Kidd) sued an Alabama hospital for the death of her newborn baby, after the doctors failed to carry out a critical pre-birth testing due to a cyberattack
- The hospital have been experiencing computers being disabled on each floor,
    - which means that the health record were not accessible
    - and medical staff did not have access to medical equipment that could not track fetal heartbeats in 12 delivery rooms
- Ms.Kidd's daughter was born with the umbilical cord wrapped around their neck
    - This condition would have triggered warning signs on the heart monitor since the cords would cut off the fetus's oxygen and blood supply
    - The baby was diagnosed with brain damage and passed nine months later

[Son Almost Overdoses Due to Cyberattack]

- Location: Des Moines, Iowa
- Kelley Parsi took her son (3 yo) to the hospital to get a tonsil surgery
- The hospital was going through ransomware which meant that any of the hospital digital tools were not working at all or properly
- The computer system would automatically calculate medicine doses but since it was not working it gave the amount that was five times the normal amount
    - The son took the medicine and his body later was processing overdose, but luckily are able to recover

Real Event Presentation Script:
The first event that I will be talking about took place in Iowa where Kelley Parsi took her 3 year old son to the hospital to have tonsil surgery. Since the hospital was going through tonsil surgery, more specifically ransomware, it meant that their digital devices and computer systems were not working properly. So when it came time for the computer system to calculate the amount of medicine Parsi's son is supposed to take, it actually calculated 5 times the actual amount. This put the son's body to go through overdose. Fortunately, he was able to recover.

Unfortunately these next two events do not have a happy ending like the event I mentioned.

This next event takes place in Alabama, this is fairly recent, it happened in 2020. Ms. Kidd was pregnant and went to the hospital to have her baby. The hospital, like in the previous event, was dealing with a cyberattack where their medical devices were not working properly or not working at all. The problem that the fetus was having was that the umbilical cord was wrapped round their neck. Since the heart monitor, which would usually track the fetus's oxygen and heart beat, was not working so did not notify the doctors that the fetus was dealing with this, until later. Because the umbilical cord was wrapped around the fetus's neck for a long period of time, it caused brain damage. Though Ms. Kidd's baby survived, but she sadly passed nine months later.

This last event takes place in Germany, where a 78 year old woman was having an aortic aneurysm and called an ambulance. The ambulance then calls the local hospital to let them know that there is a woman who needs urgent care and is in critical condition. Due to the cyberattack that the hospital had, the system showed that they were unable to treat the woman since they were unavailable. This means that the ambulance had to find the next nearest hospital which was 32 km away (which was around an hour away). Even though the woman was able to make it to the hospital, she was not able to make it.

There are many other stories, where these cyberattacks have put many people's lives at risk and even death. It is not just stealing patient data but it is also affecting people's lives.