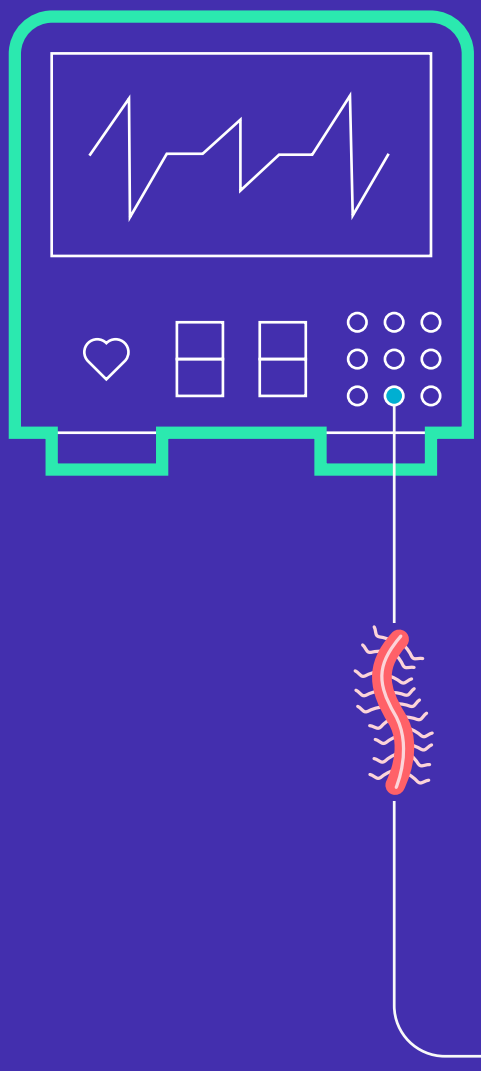
Cybersecurity Best Practices for Connected Medical Devices



CYBER MDX

Executive Summary

Would you leave your door unlocked so a stranger could enter your home?

Probably not.

Because you know the repercussions. Your safety would be put at risk, your money could be taken, and irreplaceable time and treasures would be stolen from you.

Now, think of connected medical devices as the unlocked back door to your medical facility. One that hackers can easily leverage to overtake an entire network. And, the same losses are incurred — but on a larger, more detrimental scale.

Learn what it takes to lock the back door in this guide.

Introduction

Medical devices and hospital networks are vulnerable to hackers. And, according to 30% of hospital IT and security professionals, identifying and mitigating risks in medical devices is a major problem. And for those who can identify risks, roughly one third of device makers and HDOs are aware of potential adverse effects to patients due to an insecure medical device, but despite the risk, only 17% of device makers and 15% of HDOs take steps to prevent attacks, according to Ponemon.

This means cyber attacks can go unnoticed. In fact, only about 56% of healthcare data breaches are discovered within several days and 39% of healthcare data breaches take months — or more — before being discovered, according to a Verizon study.

Not only are professional healthcare organizations starting to protect themselves, but in 2015, the FBI issued a warning to individual consumers of medical devices (the hospitals and healthcare providers).

Their recommendations to consumers included precautions like:

- Isolating IoT devices on their own protected networks
- Purchasing IoT devices from manufacturers with a track record of providing secure devices
- Updating devices with security patches when available
- Using strong passwords

For facilities and their IT personnel, cyber attacks mean patient data, patient safety, hospital security, and operations are compromised, halted, and manipulated.

The final outcome can mean disastrous health and financial consequences.

Hospital Operations Are Halted

After the 2017 WannaCry attack crippled facilities in 150 countries worldwide, the impact of cyber attacks on patient care became obvious. Hospital doctors and other practitioners were unable to perform simple tasks like accessing patients' medical records or appointment booking because their connected devices were unusable.

Even using pen and paper became difficult as paper templates needed to be printed and staff members were locked out of computers with access to printers. Without a functioning system, operations ceased. Patients who needed care had to wait for extended periods of time.

> nearly
> **20,000 hospital appointments were canceled**

Patient Safety is at Risk

When patient care is halted, health and safety risks increase.

The WannaCry breach, and the glaring vulnerabilities in NHS' system, meant nearly 20,000 hospital appointments were canceled. These appointments weren't all run of the mill checkups either, 139 were potential cancer referrals, and five hospitals had to divert ambulances carrying emergency patients to different locations at the peak of the crises.

Cyberattacks can cause issues to individual medical devices, too.

Successful exploitation of medical device vulnerabilities can allow a remote attacker to gain unauthorized access to common devices like cardiac defibrillators, pacemakers, or infusion pumps, and manipulate the intended operations. The outcome of this manipulation can be fatal.

Ransomware Attacks Cause Financial Loss

The WannaCry ransomware attack was costly for medical facilities.

Attackers were charging $300 per locked device to regain access to files. Hospitals lost money on patient care, HIPAA violations, overtime for IT staff, and repair costs.

The total loss, according to cyber risk modeling firm, Cyence, was around $4 Billion.

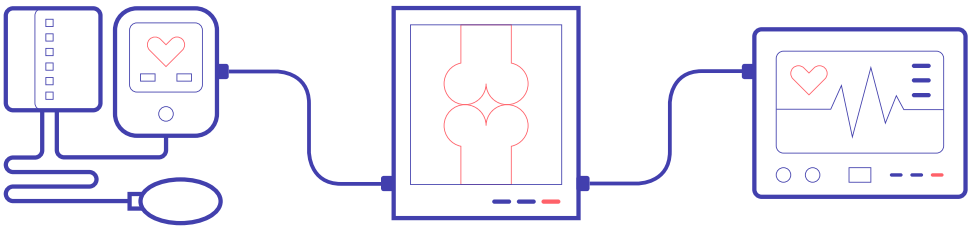
> The total loss, according to cyber risk modeling firm, Cyence, was **around $4 Billion**.

A Few More Frightening Statistics to Consider

- A new survey from software company Nuix found that 38% of 112 surveyed hackers said they could find the healthcare data they sought in less than one hour
- According to the Ponemon Institute, 89% of studied healthcare organizations have experienced a data breach
- According to Financial Times, US hospitals currently average between 10 and 15 connected devices per bed, each of which is a potential "backdoor" for hackers if it isn't secured properly
- According to Trend Micro, more than 36,000 healthcare-related devices in the U.S. are discoverable on Shodan, the search engine for connected devices.

Why Does Cybersecurity Matter?

There are many high-liability assets at stake when you battle cybercrime.



Priceless Data Has a Price

Your devices contain information that hackers and other criminals would love to have, and to sell on the black market. Their attempts at breaching your system are relentless and sophisticated. What's worth big bucks to a hacker on the black market (according to Experian, it's worth up to $1,000 per health record) is invaluable to your patients.

Medical identity theft can be expensive and time-consuming to repair. When cyber criminals sell medical information, the victims have a long, uphill battle to redeem their independence. By obtaining someone's medical records, criminals are able to:

- Steal personal information like a social security number or health ID, to obtain medical services or goods, illegally
- Obtain money by falsifying claims for medical services
- Falsify health records to support medical claims

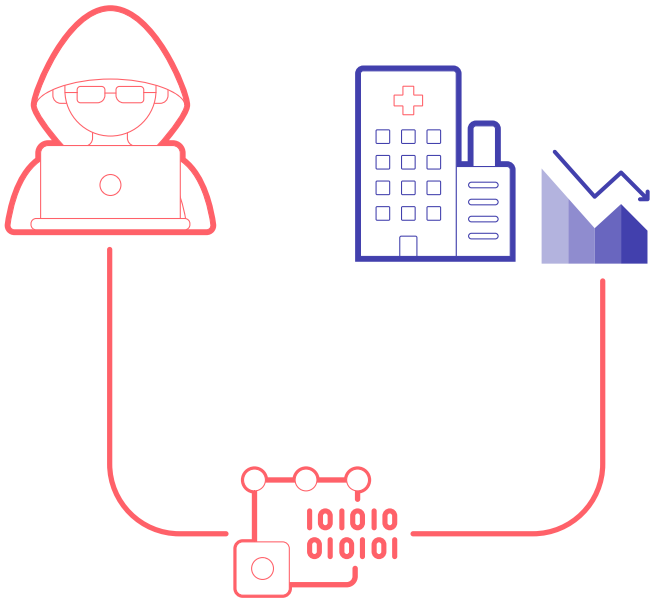
In some cases, medical information can be used to perpetuate other financial crimes, like opening credit cards. It can take years to sort out the effect of the crime.

You're One Breach Away from Financial Hardship

Cyber attacks can cause medical facilities significant financial losses.

In 2017, when the Petya attack hit Princeton Community Hospital in West Virginia, the hospital spun into crisis mode. All but four computers were affected by the attack leaving most doctors and nurses operating with pen and paper. Surgeries had to be rescheduled which sparked financial loss.

Worse still, the attack was so expensive and detrimental, the hospital was forced to replace their entire fleet of computers rather than repair them.

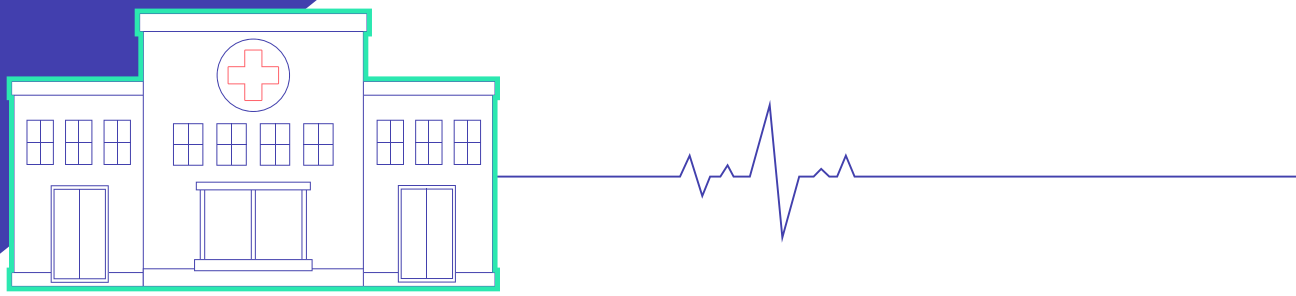


Your Patients' Lives Are on the Line

In the event of a cyber attack, patient care is halted and/or manipulated, which puts patients' safety at risk. At present, most data protection solutions that medical facilities have implemented are ill-suited to protect human life, which is becoming increasingly obvious.

In one terrifying example, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), released a warning in 2017 about problems with syringe infusion pumps by the manufacturer Smiths Medical.

A security flaw created vulnerabilities which were easily exploited by hackers. The device, designed to dispense small doses of medication, could be accessed by remote attackers who could take control of a pump and manipulate the quantities of medication administered to a patient. If the attackers wanted to, they could administer fatal doses.



5 Cybersecurity Best Practices for Connected Medical Devices

To mitigate risk, and protect your connected medical devices, it's imperative to implement a strong cybersecurity protocol.

Best Practice 1: Risk Assessment

Hospitals should assess the risk of new medical devices, legacy devices, as well as the vendors in the supply chain. Many hospitals even lack the visibility needed to identify and assess the number of devices they have in their network.

It's also important to ask if your vendors support the devices for the planned lifetime of the system. As medical devices age, vulnerabilities can occur. And, only 9 percent of manufacturers and 5 percent of users say they test medical devices at least annually, reports Healthcare IT News.

Best Practice 2: Encryption and De-identification

By encrypting and de-identifying data, you're implementing a backup measure in the event your devices are hacked. Encrypted data, or de-identified data, is rendered useless for hackers. If they steal data they cannot "unlock," it reduces the black market value of the data. This can protect your medical facility from potential HIPAA violations or exposing your patients' data in the dark web should a breach occur.

According to Synopsys, only a third of device makers say their organizations encrypt traffic among IoT devices and 29 percent of HDOs deploy encryption to protect data transmitted from medical devices. [c]

Best Practice #3: Protection by Software

IoT communication largely occurs without human interaction. That means your software needs to act as the eyes of your operation - you need something that can spot cybercrime in real-time.

Implement a procedure, or software, that constantly scans for threats. Early detection and action is the best way to mitigate risk.

Best Practice #4: Multiple Lines of Defense

Remember the basics of an IT toolbox. Every device should be up-to-date with its malware protection, antivirus software, firewalls and other authentication mechanisms to keep the hackers at bay.

If you're an administrator or CEO, ask your CISO the difficult questions.

Best Practice #5: Security Education

And, while your CISO and IT department have best practices to adhere to, that doesn't mean you can't train your staff to understand the basics of cybersecurity as well.

According to a Verizon report, 63% of confirmed breaches involved leveraging weak, default, or stolen passwords and over 30% involved an email phishing scheme. Both of these vulnerabilities relate directly to your staff, those who are using medical devices on a daily basis.

Teach your team about the importance of password security — especially for medical device access — and what to look for in suspicious emails.

How to Get Started: Assess and Protect Your Connected Medical Devices

Are you ready to start protecting your most critical assets?

- See how CyberMDX can help your medical facility stay ahead of the attack.
- Continuous in-depth discovery of medical devices and clinical network assets
- Concise risk assessment and security insights tailored to each medical device
- Automatic Smart Isolation, reducing the attack surface, hence dramatically decreasing the chances of an attack

AI-based attack detection on top of prevention, resulting in concise alerting, containment and response when a concrete threat appears

You can prevent, prepare and repair from cyber attacks with sophistication.

Get started with CyberMDX

Contact us today for more information:

CyberMDX
44 W 28 Street
8th Floor
New York, NY 10001

info@cybermdx.com

646-794-4160