ACCRUENT TMS

7 BEST PRACTICES FOR CYBERSECURITY IN THE HEALTHCARE ENVIRONMENT

Boosting Healthcare Cybersecurity to Combat Evolving Threats

ACCRUENT

TABLE OF CONTENTS

INTRODUCTION

Medical devices are more advanced, connected and ubiquitous than ever, to the point where the industry has spawned the IoT subset IoMT (Internet of Medical Things). These devices not only house sensitive patient data but also connect to broader systems as part of a fully developed network with features like two-way communications and wireless connectivity. As a result, they've become the targets of bad actors looking to exploit medical device vulnerabilities every chance they get.

At the same time, healthcare facilities themselves are more connected, with core infrastructure systems like security cameras, HVAC, power supplies, water, fire protection, elevators and other systems tied together through a building's IT infrastructure. These systems, too, are increasingly threatened by malicious actors going after not just patient data but endangering the physical health and safety of patients, employees and visitors as well. Cyberattacks pose significant threats to the healthcare sector, jeopardizing patient care and costing providers billions. It will take a concerted effort on the part of clinical engineering,

facilities management and IT to keep their organizations safe from cyberthreats. This eBook looks at the growing body of healthcare technology management (HTM) and healthcare facility management (HFM) attacks and how hospitals can boost their medical device and medical facility cybersecurity.

> ***"Medical devices are increasingly connected to the Internet, hospital networks, and other medical devices to provide features that improve health care and increase the ability of health care providers to treat patients. These same features also increase the risk of potential cybersecurity threats."***
>
> – U.S. Food and Drug Administration

WHY TODAY'S CYBERSECURITY APPROACH IS INSUFFICIENT

Until recently, keeping medical devices and facilities safe was a relatively straightforward task. Isolated devices and building systems could be protected discretely, with Clinical Engineering relying on vendors to build secure devices and Facilities Management focused on the maintenance and upkeep of non-networked building assets and systems. But connectivity changed the game. These days, ensuring a safe environment means safeguarding networks from malicious damage or disruption – and the attack surface is expanding:

- In 2024, the global devices market is worth an estimated $511 billion. The US takes the lead in revenue generation, with an estimated $182 billion.[1]
- A typical U.S. hospital has between 10 and 15 medical devices per bed. This means a 1,000-bed hospital could have around 15,000 medical devices.[2]
- There is an average of 6.2 vulnerabilities per medical device. Recalls have been issued for critical devices like pacemakers and insulin pumps, with known security issues.[3]
- 53% of connected medical devices and other IoT devices in hospitals had known critical vulnerabilities.[3]
- Going into 2024, expect medtech revenue growth to stabilize at 100 to 150 basis points above pre-pandemic rates.[4]

RECENT HIGH-PROFILE CYBER ATTACKS

$22 MILLION

The amount Change Healthcare paid for a ransomware attack that caused issues processing patient prescriptions.[5]

6 MILLION PEOPLE

Were affected by a large-scale hack on PharMerica, where sensitive patient data was leaked.[5]

30M HEALTHCARE PROVIDERS

Began to report data breaches after their medical records were breached at OneTouchPoint.[6]

[1]https://www.statista.com/outlook/hmo/medical-technology/medical-devices/worldwide#:~:text=The%20Medical%20Devices%20market%20market,bn%20in%20the%20same%20year.

[2]https://www.hipaajournal.com/63pc-known-exploited-vulnerabilities-hospital-networks/

[3]https://www.gao.gov/assets/d24106683.pdf

[4]https://www.mckinsey.com/industries/life-sciences/our-insights/what-to-expect-from-medtech-in-2024

[5]https://www.electric.ai/blog/recent-big-company-data-breaches

[6]https://www.upguard.com/blog/biggest-data-breaches-in-healthcare

UNDERSTANDING CYBERSECURITY VULNERABILITIES

The first step in securing your organization from cyberattack is understanding what the attackers are after – and how they might get there – so that you can take the appropriate security measures. Phishing scams that lead to ransomware attacks have gotten a great deal of press lately, but keep in mind that cyberattacks don't always happen in the most obvious way. There are many go-to vulnerabilities that attackers actively target because they're things that developers or hospitals may overlook. These first attempted points of entry include:

- **Unsecure firmware updates:** Many software updates are implemented incorrectly, making it easy for attackers to exploit vulnerabilities.
- **Physical attacks:** Physical attacks, where malware is installed through a physical point of entry, can be carried out through ports, flash drives and other points of entry.
- **Manufacturing support left enabled:** During manufacturing, the manufacturers have access to a lot of commands and functionalities that they use to test and calibrate devices. If these capabilities are left enabled, it can be easy for attackers to find the commands and gain access to functionality.
- **Points of communication:** Things that connect systems and devices, like Bluetooth low energy (BLE), are inherently insecure – and an unsecured pairing can open up your environment and devices to vulnerabilities. These pairings must be checked pre-emptively to confirm that the pairing is to the right place and that there are no security risks.
- **Personal devices:** The move to remote work means many doctors and medical professionals are working remotely – and most healthcare organizations haven't taken the necessary steps to secure personal devices or train employees on security measures. A report analyzed by Health IT revealed that nearly 24% of health employees in the U.S. hadn't received any cybersecurity training to help identify phishing scams, which can only make things worse.[7]

[7]https://www.getastra.com/blog/security-audit/healthcare-data-breach-statistics/

BEST PRACTICE #1: PERFORM INVENTORY CHECK FOR RISK ANALYSIS

You can't protect what you don't know about. With thousands or even tens of thousands of networked medical devices in your healthcare facility, making sure each device is accounted for is crucial so that you know what needs to be protected, what each device interacts with, and where to focus your energy. Untracked devices that fly under the radar are attractive points of entry for bad actors. The same is true for all your networked building systems, such as power supplies, lighting, water and sewer, security cameras, elevators, HVAC, access control systems and more. Each system could be tampered with, allowing hackers to disrupt service (e.g., turning off the power until a ransom is paid) or possibly access patient data in the organization's network. In addition to these individual components, however, be sure to take into account any building automation systems (BASs) and fire suppression monitoring systems. It's common for these systems to have a dedicated server and be managed outside of your IT team, so they may not follow the same security protocols.

Hospitals and other healthcare facilities usually rely on IT-based systems to manage attributes of network-connected devices. With a modern healthcare CMMS, you can add these attributes into your system and conduct comprehensive risk assessments, reconcile MDS2 data and other security attributes against inventory, remediate potential risks and vulnerabilities, and identify devices and systems affected by network outages or maintenance. You can even generate a report that lists all the devices that are targeted by a specific cybersecurity attack.

BEST PRACTICE #2: WORK WITH SUPPLIERS TO ENSURE DEVICES AND SYSTEMS ARE SECURE ON THEIR END

Remember that cybersecurity protection does not simply fall on the shoulders of your healthcare delivery organization; it's a multi-layered process that involves not only your facility but also the vendors and contractors who supply your devices and systems. On the medical device manufacturer (MDM) side, the MDMs should be proactively identifying and reducing risks when building devices. On the HFM side, it starts with making buildings more secure during planning, design and construction, and ensuring that embedded technologies are properly designed, installed and secured.

Be sure to ask vendors and suppliers:

- What vulnerabilities could have been introduced during development, and how did you address them?
- Do you offer a contract that guarantees the cybersecurity of the device or system?
- What installation services do you offer, and what security do they entail?
- What ongoing cybersecurity support do you offer, and do you conduct annual risk assessments?

Holding medical device manufacturers accountable for security risks has gotten easier as MDMs become more transparent. A number of high-profile companies, including Siemens, Philips and Boston Scientific, have announced they will share vulnerability information in cases of cybersecurity breaches on their devices. Meanwhile, the Healthcare and Public Sector Coordinating Council has proposed that any entity purchasing a connected medical device would have access to a list of all its underlying software via a Cybersecurity Bill of Materials (CBOM), which the FDA says "can be a critical element in identifying assets, threats, and vulnerabilities."

BEST PRACTICE #3: SECURE ASSETS AND DEVICES THROUGHOUT THEIR LIFECYCLES

Aging devices and systems are not only at risk of failure as parts wear out and break; they're also at risk of breach. Take medical devices, for instance. 1 in 5 connected medical devices runs on unsupported operating systems, and nearly 40% of analyzed nurse call systems have critical, unpatched vulnerabilities.[8] This puts them well past Microsoft's end-of-life date, where the software is no longer serviced via upgrades, patches and overall maintenance, making them vulnerable to hackers. Updating operating systems is a vital step toward stronger cybersecurity.

Ensuring the software is up to date is just one piece of the bigger picture, however. Even up-to-date devices and systems can experience physical attacks, such as malware being installed through a port or flash drive. Creating and updating standard operating procedures (SOPs) around how teams secure devices and systems are key, but keep in mind that security measures may introduce friction into the employee experience, possibly leading to end users creating workarounds that put security at risk.

Healthcare Technology Management (HTM) and Healthcare Facilities Management (HFM) departments have long provided key post-acquisition support and management of medical equipment and facilities assets with planned and corrective maintenance throughout their useful life. A CMMS can help facilitate scheduling routine maintenance, tracking the repair history and organizing data for each asset, and automating workflows for your organization when security gaps or risks are found, as well as helping you retire outdated devices, identify remediation needs, and reduce systems outages. In addition, some vendors offer real-world work order and asset lifecycle data so you can gain insight into device history before purchase for improved capital planning decisions.

[8]https://healthitsecurity.com/news/1-in-5-connected-medical-devices-run-on-unsupported-operating-systems

BEST PRACTICE #4: MONITOR NETWORK TRAFFIC

What information is going to and from your devices and your systems? What networks are they interacting with? Who has access to these networks and what levels of authorization do they have?

Malicious network traffic is the number one cybersecurity risk for healthcare providers, according to security firm Wandera. Affecting nearly three quarters of organizations (72%), network access from an app to a web service that is known to demonstrate malicious behavior can include downloading unauthorized software to a device, disrupting normal operation, or gathering sensitive information.

Detecting threats alone is insufficient, however; an organization must be able to act quickly, before serious damage is done. A healthcare CMMS that integrates with network monitoring tools can trigger alerts and send automatic notifications when network traffic falls outside of normal traffic patterns so you can address potential issues the moment they happen. Real-time notification allows HTM and HFM resources to be disconnected from medical devices and systems to prevent or reduce the spread of cyberattacks, allowing you to swap out a device – in many cases even when it's currently being used on a patient.

Initial access brokers are targeting the healthcare industry. They compromise healthcare networks and then sell access to ransomware gangs. Network access from an app to a web service that is known to demonstrate malicious behavior can include downloading unauthorized software to a device, disrupting normal operation, or gathering sensitive information.

Failure to implement cybersecurity measures could lead to a higher risk of data breaches (96%), financial/legal penalties for hospitals (79%), and concerns about patient safety (65%).[9]

Accruent is partnered with discovery and monitoring tools organizations. These tools monitor the network traffic and the information going to and from devices. If an activity falls outside the normal traffic patterns, an alert is sent to the appropriate staff. This proactive approach ensures you are not just waiting for the next cyberattack to spread throughout your organization.

TALK TO AN EXPERT

A best practice is to have separate networks in use by various entities. For example, a guest network for patients and visitors allows for complete isolation from medical devices and systems, while an internal network for each major organizational group (administration, finance, pharmacy, utility systems, medical devices, etc.) gives an organization the means to harden each network, ensuring a cyberattack on one network does not affect the others.

[9]https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10642560/

BEST PRACTICE #5: ESTABLISH SAFE PRACTICES FOR PERSONAL DEVICES

Personal devices proliferate in hospitals, from phones to smart TVs. Healthcare organizations create avenues for hackers to infiltrate their network(s) when they allow access to network resources and do not have a protection plan that prevents access to infrastructure and business systems. Knowing how vendors, manufacturers and others will access medical devices and systems will provide a layer of security by ensuring those access points are secured.

> ***"IoT devices can range from the 3.7 million clinical devices that collect and transmit data via online networks to devices like iPads and wearables, which may not be critical to care but have increasing access to patient data. In July, the National Institute of Standards and Technology (NIST) issued a report indicating that clinicians are increasingly bringing their own smartphones and other devices to use at work, which necessitates protection against both privacy violations and cybersecurity vulnerabilities."***
>
> – The Healthcare Financial Management Association

BEST PRACTICE #6: TRAIN HTM & HFM END USERS

When we think about cybersecurity training in healthcare organizations, often the first thing that comes to mind is protecting against ransomware attacks, which are often spread by phishing emails that contain malicious attachments or fool users into giving attackers information. As a result, hospitals have beefed up their cybersecurity training around educating users how to recognize social engineering and how to employ safe password practices.

But equally important is for healthcare organizations to focus on training users in HTM and HFM departments on how to prevent and recognize possible attacks. Both technical and non-technical employees can be trained in areas such as policies, procedures, procurement, vendor relationships, clinical user training, network architecture, threat management, lifecycle and change management, event documentation and more.

By visibly showing network attributes on repair screens, a CMMS can ensure technicians are aware of devices and systems are connected along with potential security concerns based on accessibility. Connecting network attributes to work events allows healthcare organizations to track and analyze potential breach events, activities on connected devices, and remediation efforts.

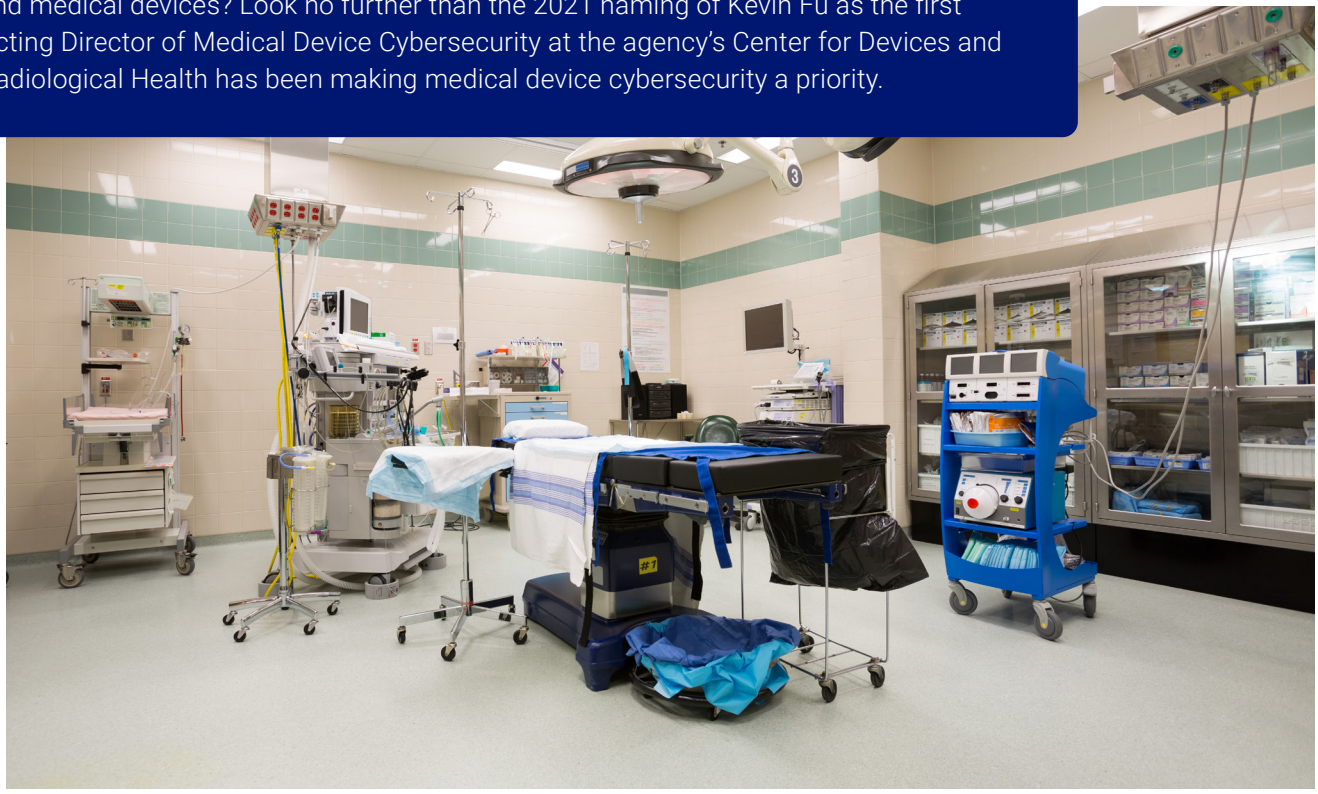
> ***"One way for organizations to offset at least part of the problem is to train other technical professionals in cybersecurity. Although dedicated experts remain sorely needed, by training their colleagues, we can distribute the workload more effectively and better prevent security crises from occurring."***
>
> – Axel Wirth, distinguished technical architect at Symantec

BEST PRACTICE #7: SHORE UP COMPLIANCE WITH FDA AND OTHER REGULATIONS

One of the most important responsibilities of an HTM or an HFM department is to ensure the hospital is compliant with all laws and regulations, as violations lead to negative outcomes such as federal fines and a less-than-optimal environment of care. Since issuing its first major recommendation in 2013 that medical device manufacturers and health care facilities take steps to ensure that appropriate safeguards are in place to reduce the risk of device failure due to cyberattack, the FDA has continued to update its guidance with pre-market and post-market recommendations. For medical devices and utility systems, compliance standards require a 100% completion rate for scheduled maintenance activities – whether the device is "high risk" or "non-high risk." Healthcare facilities managers must follow government regulations to ensure facilities comply with laws such as the Americans with Disabilities Act, and they must manage the continual upkeep of certifications and accreditations, like those issued by The Joint Commission. Recently, the HHS Office of Inspector General made recommendations that prompted CMS to consider adding new medical device cybersecurity requirements for hospitals participating in Medicare. And even HFM departments are seeing continued growth of connected devices and systems, from vibration and flow sensors to fully automated emergency support systems, requiring compliance with IT and regulatory requirements in those systems.

HTM and HFM departments use their CMMS as the primary tool to document regulatory compliance. But since CMS, the Joint Commission, and other regulatory bodies change their standards often, these teams need a modern solution, as legacy CMMS are not able to keep up with the changes. A modern healthcare CMMS aids in round-the-clock compliance, helping ensure healthcare organizations maintain certification, building and device compliance.

Just how important an issue has cybersecurity become for the FDA, a body that ensures the safety of a wide range of the nation's goods, including its food supply, cosmetics, radiation-emitting products, human and veterinary drugs, biological products and medical devices? Look no further than the 2021 naming of Kevin Fu as the first Acting Director of Medical Device Cybersecurity at the agency's Center for Devices and Radiological Health has been making medical device cybersecurity a priority.



CONCLUSION

As cyberattacks evolve, one thing remains clear: hospitals and other healthcare organizations will need to continue to focus on identifying and resolving cybersecurity risks – throughout the entire environment, including HTM and HFM departments.

A modern healthcare computerized maintenance management system can help. To mitigate cybersecurity risks, a modern CMMS aids in the management and control of the entire asset lifecycle, improving visibility and availability while ensuring compliance with government regulations.

Learn more at https://www.accruent.com/solutions/facility-management-software/facility-asset-management-tms

ABOUT ACCRUENT

At Accruent, we're building a more connected future where manufacturers' people, systems, and data work synergistically to drive informed decision-making, operational excellence, and business growth. As the world's leading provider of workplace and asset management software for unifying the built environment, our solutions deliver not only the promised results but also illuminate possibilities manufacturers couldn't see before. Coupled with our deep industry expertise and world-class professional services, healthcare professionals can depend on us to help maximize their investments in people, assets, and facilities.

Get in touch today to learn more about Accruent or how our industry-leading solutions can help transform your organization.

SPEAK TO A SPECIALIST

ACCRUENT TMS

Accruent, LLC

512-861-0726 | www.accruent.com