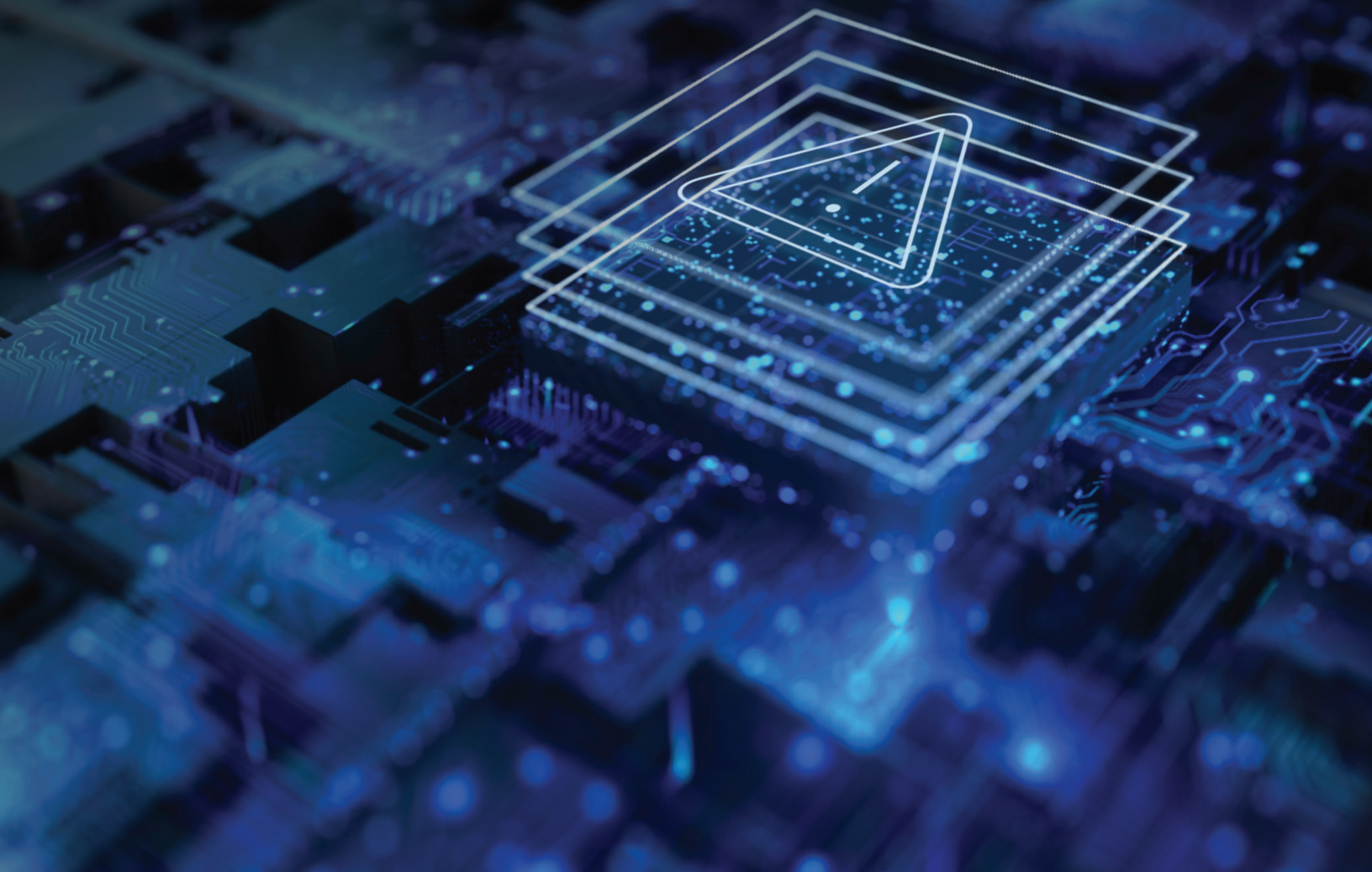
WHITE PAPER | MEDICAL DEVICE CYBERSECURITY

TRIMEDX℠

ASSESSING MEDICAL DEVICE CYBERSECURITY RISK

Reveal a more complete view of cybersecurity risk in health systems



ASSESSING MEDICAL DEVICE CYBERSECURITY RISK

Secure the technologies that collect, analyze, and communicate vital health data

Advancing healthcare technology has driven a great deal of innovation in patient care. Providers have the tools to collect, analyze, and communicate vital health data more efficiently than ever before. The growth of network connectivity has exciting potential to streamline care pathways and give patients greater agency over their health.

But network connectivity also comes with the risk of exposure to cyberattacks. This has contributed to cybersecurity becoming one of the biggest challenges facing the healthcare industry.

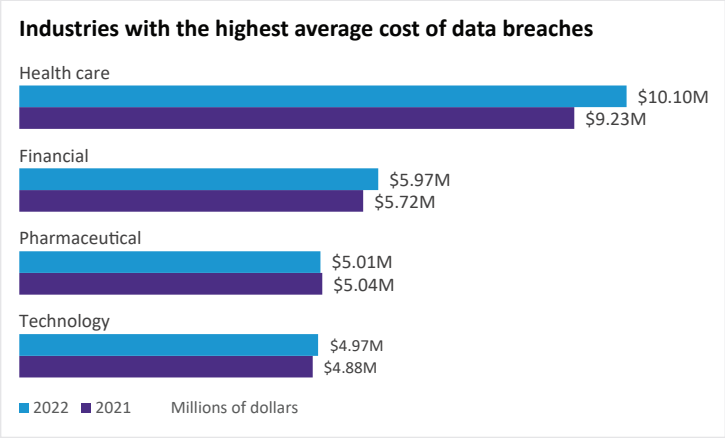
This risk extends to network-connected medical devices, which number 10 to 15 per patient bed in U.S. hospitals.[1] What sets medical devices apart from other healthcare technologies is their proximity and criticality to patient care as well as how they are maintained. Since medical devices fall under regulations, they are unable to utilize the standard IT tools and processes for the management of cybersecurity risks. The unique role of medical devices carries unique cybersecurity risk factors that must be well understood and actively monitored to support patient care.

MEASURING THE DAMAGE OF CYBERSECURITY RISK

Predicting the likelihood of a potential cybersecurity breach may not be possible, but we can see the real-world impact of the dramatic rise in cyberattacks against healthcare organizations. Just as the technologies used by attackers are varied and complex, so are the damaging effects on health systems and the communities they serve.

Financial

The average cost of healthcare data breaches is over $10 million, more than double the average cost of other critical infrastructure industries.[2]



Operational

Identifying and containing cybersecurity breaches takes over 300 days on average.[2] In cases involving attacks like ransomware, this can mean uncertain periods of limited or no access to health records and medical devices.

Cost of a Data Breach Report 2022, IBM Security

Patient safety
While it is difficult to know with certainty what impact many cyberattacks have on patient outcomes, some recent attacks have been followed by allegations or legal action against health systems' liability in patient deaths.[3,4] Medical devices, in particular, can be integral to procedures that, if interrupted by cyberattacks, could put patients in immediate danger.

Patient privacy
Cyberattacks do have a very tangible effect on patient privacy. Attacks like ransomware can be used to steal electronic Protected Health Information (ePHI), oftentimes to sell it to other bad actors or on the dark web. Such cyberattacks may also compromise the integrity and availability of health records and medical devices, impeding patient care.

Reputation
Health systems that are victims of cyberattacks work hard to limit damage, restore functionality, and protect patients. But no matter how successful their efforts are, they cannot un-ring the bell. The damage that breaches patients' confidence is hard to repair. As many as 67% of organizations hit by one cyberattack suffer a second.[5]

ARE MEDICAL DEVICES A BLIND SPOT FOR HEALTHCARE CYBERSECURITY?

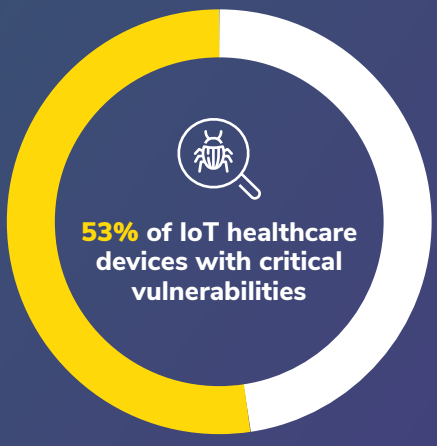
Often, the management of medical device cybersecurity is not a primary concern of a clinical engineering team in a healthcare organization due to the following factors:

- Clinical engineering teams are primarily focused on scheduled maintenance and bench repairs.
- Clinical engineering professionals may lack IT and cybersecurity skills.
- Only general attributes from medical devices are captured and documented in the Computerized Maintenance Management System (CMMS). Core network and cybersecurity attributes are not maintained in the CMMS.
- Clinical engineering policies, procedures, and processes are not aligned to manage cybersecurity risks.
- Lack of coordination and/or siloed structure between IT and clinical engineering.
- Original Equipment Manufacturers (OEMs) have unique methods of sharing the availability of a validated or approved mitigation for medical devices impacted by a vulnerability, plus there is no industry-wide standard or regulations for releasing validated patches in a reasonable time. This creates a unique challenge for healthcare organizations to track the timely availability of a patch or other mitigations

The advancement in healthcare technology has not only increased the dependency of integrated medical devices on the network but also provided bad actors with other entry points for cyberattacks due to weak security controls or unpatched vulnerabilities on medical devices.

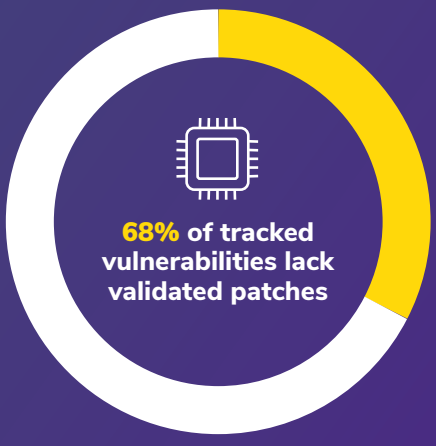
Traditionally, clinical engineering teams have reported to facilities engineering or other support services, but this reporting structure is changing as healthcare organizations are aligning clinical engineering services under IT to address the issues mentioned above. This trend shows a growing awareness among healthcare leadership that medical devices have a critical impact on cybersecurity, and it can be addressed by bridging the gap between IT and clinical engineering services.

BLIND SPOTS IN MANAGING HEALTHCARE CYBERSECURITY RISK



Health IT Security

Security Magazine



TRIMEDX internal data

APPLYING IT KNOWLEDGE TO CLINICAL ASSETS

Developing a strong understanding of what resources/assets a health system has, where they are, and how they are used in a clinical environment is crucial context for executing a medical device cybersecurity strategy. While it may sound intuitive, maintaining an accurate medical device inventory is easier said than done. The size of inventories and the geographic footprint of modern health systems make any sort of manual accounting far too cumbersome for any team.

The cybersecurity vulnerabilities found across these dispersed inventories are also plentiful. A 2022 report indicated that 53% of healthcare IoT devices, including medical equipment, have known critical vulnerabilities.[6]

When numerous vulnerabilities and devices are not carefully and accurately identified & matched, the ability to generate actionable intelligence suffers. Cybersecurity professionals have reported that 20–40% of cybersecurity alerts of vulnerabilities and malicious behavior are false positives.[7] These false alerts can waste crucial resources and damage confidence in cybersecurity initiatives.

Health systems can minimize these types of inefficiencies and inaccuracies by deploying passive monitoring and identification tools on the network. Tools that monitor IoT devices for suspicious behavior in real-time take advantage of deep packet inspection to increase the visibility of network traffic originating from devices scattered across care sites as well as profile them based on their signature on the network. Up-to-date automated discovery in real-time combined with device profiling enables health systems to confidently identify authorized assets within their fleet.

Health systems must carefully examine what strategies are available to them to remediate cybersecurity risks and vulnerabilities. Are validated or approved OEM patches available for medical devices? Does the manufacturer consider a device to be end-of-life? Is available mitigation compatible with how a device is used for patient care? Analyzing these questions will help health systems understand risk and also confidently identify paths for mitigation.

EXPANDING CYBERSECURITY PERSPECTIVES WITH CLINICAL ENGINEERING EXPERTISE

Understanding how medical devices function in a clinical environment is just as important for assessing cybersecurity risk as identifying and monitoring vulnerabilities. It is as important to bring the subject matter expertise of clinical engineering along with cybersecurity to perform the risk assessment, and bridging this gap between both teams provides a better assessment of where significant risks lie in a health system's inventory.

First and foremost, it needs to be determined whether a device is connected to a network or capable of being connected. This narrows down and brings attention to devices that could be at risk for cyberattacks.

HEALTHCARE CYBERSECURITY RISK CHECKLIST

- ❑ Accurate device location and inventory tracking
- ❑ Network-connected or connectable
- ❑ Known vulnerabilities
- ❑ Real-time digital behavior monitoring
- ❑ Manufacturer-validated patching
- ❑ ePHI storage capability
- ❑ Active FDA alerts or manufacturer recalls
- ❑ Mission-critical role in patient care
- ❑ Patient safety risk of equipment failure
- ❑ Operational consequences of equipment failure

Likewise, it is imperative to evaluate and document if a device is capable of or is currently storing/transmitting ePHI. This step is crucial for responsible stewardship of patient privacy, and it helps to paint a clearer picture of what information could be at stake in the event of a successful attack or an incident.

As medical device technology rapidly evolves, new concerns and challenges are bound to emerge. FDA alerts and manufacturer recalls should be carefully monitored, as they present various risks—cybersecurity included. A proactive clinical engineering service has the processes, subject matter expertise in clinical engineering & cybersecurity, and partnerships in place to identify & address these urgent situations. Cybersecurity teams can take advantage of that efficiency when alerts and recalls are issued regarding medical devices.

Beyond the technical attributes of a device, one of the most important things to understand is the patient safety risk and the specific role it plays in patient care. Some equipment is integral to treatments and procedures for the most vulnerable patients. This level of criticality helps determine the potential risk to patient safety and provides valuable context for setting cybersecurity priorities.

Mission criticality also helps to determine the potential risk of a device failure to organizational operations that may lead to lost revenue. For example, the failure of a CT scanner in an ER due to a cyberattack could force the healthcare organization to divert patients to other healthcare organizations which may result in significant lost revenue.

CONCLUSION

Assessment of medical device cybersecurity requires a strong collaboration between IT and clinical engineering. By working together, both departments can develop a cybersecurity strategy and improve the lifecycle management of medical devices. This joint effort can empower healthcare organizations to protect against cyberattacks while contributing to its primary mission: safe and reliable patient care.

SOURCES

1. *FierceHealthcare. (2019). 82% of healthcare organizations have experienced an IoT-focused cyberattack, survey finds. https://www.fiercehealthcare.com/tech/82-healthcare-organizations-have-experienced-iot-focused-cyber-attack-survey-finds*
2. *IBM Security. (2022). Cost of a Data Breach Report 2022.*
3. *Associated Press. (2021). Suit blames baby's death on cyberattack at Alabama hospital. https://apnews.com/article/technology-business-health-alabama-lawsuits-68c78e9d6af359842c0e9645b4577b50*
4. *National Law Review. (2020). First Reported Death Connected to Misfired Ransomware Attack on German Hospital. https://www.natlawreview.com/article/first-reported-death-connected-to-misfired-ransomware-attack-german-hospital*
5. *CPO Magazine. (2022). 67% Of Businesses Suffer Repeat Cyber Attacks Within 12 Months After the First Data Breach. https://www.cpomagazine.com/cyber-security/67-of-businesses-suffer-repeat-cyber-attacks-within-12-months-after-the-first-data-breach/*
6. *Health IT Security. (2022). 53% of Connected Medical Devices Contain Critical Vulnerabilities. https://healthitsecurity.com/news/53-of-connected-medical-devices-contain-critical-vulnerabilities*
7. *Security Magazine. (2022). One-fifth of cybersecurity alerts are false positives. https://www.securitymagazine.com/articles/97260-one-fifth-of-cybersecurity-alerts-are-false-positives*

UNLOCK THE **FULL POTENTIAL** OF YOUR CLINICAL ASSETS

TRIMEDX is an industry-leading, independent clinical asset management company delivering comprehensive clinical engineering services, clinical asset informatics, and medical device cybersecurity. We help healthcare providers transform their clinical assets into strategic tools, driving reductions in operational expenses, optimizing clinical asset capital spend, maximizing resources for patient care, and delivering improved safety and protection. TRIMEDX was built by providers, for providers, and leverages a history of expert clinical engineering with data on 92% of all active medical device models.

Learn how TRIMEDX can help improve your medical device security posture.

trimedx.com or 877-TRIMEDX

TRIMEDX℠

 5451 Lakeview Pkwy S Drive Indianapolis, IN 46268

info@trimedx.com

921361-122022