Building a Mature Medical Device Cybersecurity Program

Health systems are spending more than ever on cybersecurity, but they need to build the right processes for managing medical device technology to fully realize the benefits of their investments. Without the right processes in place to coordinate between people and technology, major gaps can remain in a healthcare organization's cybersecurity strategy.

Health systems increasingly rely on digital technology and networks to provide patient care, adding a complex new element to the efforts of protecting patient data and healthcare assets. Cybersecurity is one of the most prevalent challenges in healthcare, with attacks increasing each year. Each of these breaches cost health systems an average of $10 million.[1] The cost of cyberattacks, combined with operational disruption to vital medical equipment and patient care, put healthcare facilities' reputation and, most importantly, patient safety and outcomes at risk.

The proliferation of cyberattacks has driven health systems to focus greater effort on securing technology resources. Spending on cybersecurity initiatives continues to increase rapidly, with sustained double-digit annual growth projected through the end of the decade.[2,3] Yet, increased spending alone cannot guarantee the success of a cybersecurity program. Health systems need to establish the right processes to maximize the visibility of their cybersecurity risk and track the impact of their efforts to manage or reduce that risk.

One of the primary challenges to establishing a mature medical device cybersecurity program is misplaced investment in technology without establishing and applying the necessary people and processes to implement an effective solution that not only monitors and detects, but can interpret, recommend, and contribute to corrective action. In many health systems, medical equipment is a prime example of this problem.

As the number and complexity of medical devices connected to hospital networks steadily increases, so does the need for effective cybersecurity practices. Without a strong cybersecurity program in place, health systems are left vulnerable to cyberattacks and malicious intrusions. To achieve a sufficient level of cybersecurity maturity, healthcare organizations must strengthen their processes for managing medical devices, invest in recruiting and equipping the necessary staff to identify and understand risk, and invest in robust systems and tools to protect their networks.

Breaches can impede clinical operations to the point that facilities may have to reschedule patient appointments or even reroute emergency patients to different sites.

The Impacts of Cyberattacks Go Beyond Financial Loss

The disruptions that cyberattacks cause can threaten the core functions of healthcare facilities and often demonstrate the dangers of not having a standardized approach to data security. Identifying and containing cybersecurity breaches takes 277 days on average.[1]

Average time to identify and contain data breaches in 2022

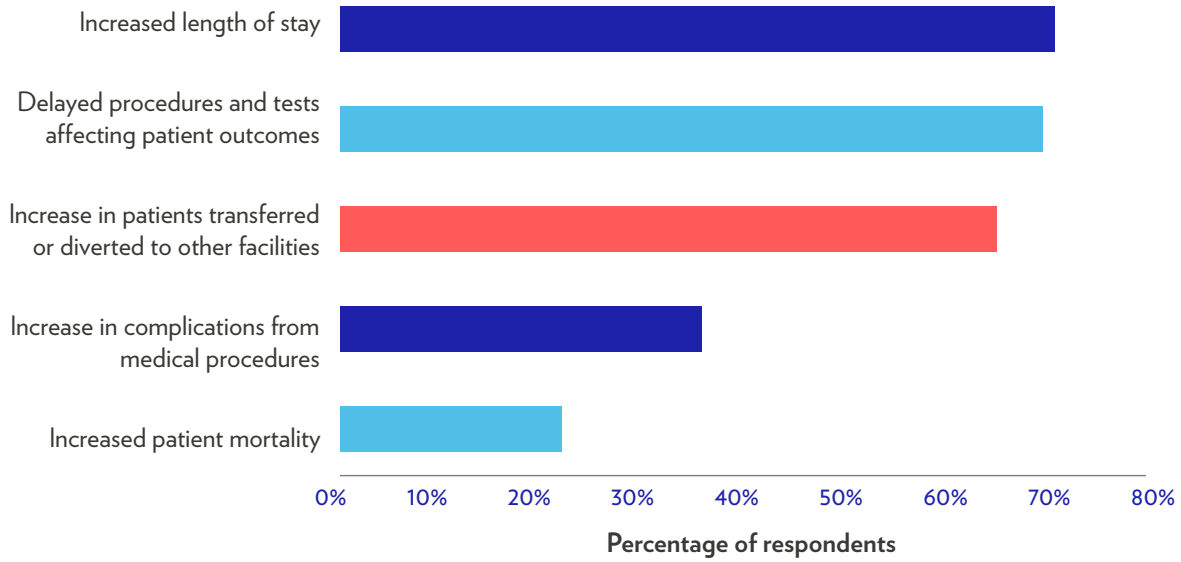
Cost of a Data Breach Report 2022, IBM Security

In cases involving attacks like ransomware, this can mean uncertain periods of limited or no access to health records and medical devices, and reduced capabilities to deliver reliable care. Breaches can impede clinical operations to the point that facilities may have to reschedule patient appointments or even reroute emergency patients to different sites. In cases where time is a factor in treatment, these breakdowns and delays can amplify the risk to patient safety and outcomes.

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.[4,5] Medical devices can be integral to procedures that, if interrupted by cyberattacks, could put patients in immediate danger. A report from the Ponemon Institute demonstrates that cybersecurity teams in hospitals have seen a clear impact to the technology resources that are essential to delivering consistent, timely and effective care for patients.[6]

IT professionals weigh in on the impacts of ransomware

A Ponemon Institute survey revealed that healthcare IT and cybersecurity professionals view cyberattacks as a major threat to patient safety and health outcomes.



The Impact of Ransomware on Healthcare During COVID-19 and Beyond, Ponemon Institute

Without a rigorous assessment of current clinical assets and an understanding of inventory accuracy, it can be difficult to know where the best starting point is for improving medical device cybersecurity.

Cyberattacks have an undeniable effect on patient privacy and confidence in healthcare providers. Attackers can steal electronic Protected Health Information (ePHI) or use ransomware to lock out health system staff to extort payments. Such cyberattacks may also compromise the integrity and availability of health records and medical devices, impeding patient care.

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 unring the bell. The damage that breaches patient confidence is hard to repair. As many as 67% of organizations hit by one cyberattack suffer a second.[7]

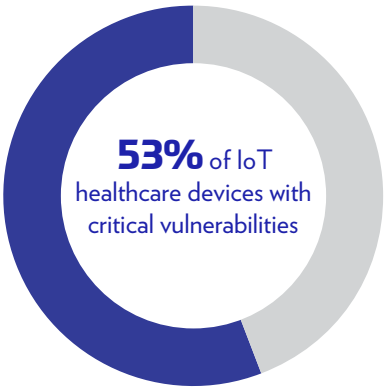
Starting with Inventory

Inventory accuracy builds the foundations of a reliable cybersecurity program, but it is often a major stumbling block for many health systems. Without a rigorous assessment of current clinical assets and an understanding of inventory accuracy, it can be difficult to know where the best starting point is for improving medical device cybersecurity.

Cybersecurity requires a foundation of visibility and reliable data. 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 for executing a medical device cybersecurity strategy. While this may sound intuitive, maintaining an accurate medical device inventory is often easier in theory than in practice due to the need of establishing and following set processes. Building an accurate inventory can be a major hurdle to improving the cybersecurity maturity for many health systems. The size of inventories and the geographic footprint of modern health systems make any sort of manual accounting far too cumbersome for teams juggling multiple responsibilities.

The cybersecurity vulnerabilities found across these dispersed inventories are plentiful. A 2022 report indicated that 53% of healthcare Internet of Things (IoT) devices, including medical equipment, have known critical vulnerabilities.[8] When numerous vulnerabilities are not carefully and accurately identified and matched to the relevant devices, the ability to generate actionable intelligence suffers. Cybersecurity professionals have reported that 20% to 40% of cybersecurity alerts of vulnerabilities and malicious behavior are false positives.[9] These false alerts can waste crucial resources and damage confidence in cybersecurity initiatives at a time when the healthcare industry is facing a shortage of over 300,000 cybersecurity professionals.[10]

Blind spots in managing healthcare cybersecurity risk



HealthITSecurity

Security Magazine

TRIMEDX internal data

The need for cybersecurity education does not end once a system is established. As hacking tools and methods continue to advance, it is important that health system personnel keep up with trends so they can remain alert.

Empowering Associates to Support Security

Healthcare personnel are one of the key ways in which ransomware attacks gain access to healthcare systems. Cybercriminals use carefully disguised emails, links and websites to steal sensitive information and credentials that cannot be retrieved once divulged. Many victims don't even realize they've been targeted until it is too late.

Precautions are the greatest defense for anyone wishing to avoid careless leakage of vital details. However, healthcare workers have been exhausted and overworked for the past two years due to the global pandemic and staff shortages, which have put immense pressure on care providers and medical device maintainers. As a result, ransomware attacks have had an easier time infiltrating health systems, as overburdened staff are more inclined to overlook email and online communications.

Part of these problems are systemic, but health systems can provide extra resources and training to their members to make them more aware. Training must include common tactics used by hackers, like almost identical email addresses, dubious URLs, suspicious formatting and urgent text messages. In addition, by providing different members with the right areas to investigate, they will be better able to keep track of sensitive data and systems.

The need for cybersecurity education does not end once a system is established. As hacking tools and methods continue to advance, it is important that health system personnel keep up with trends so they can remain alert. One way of doing this is enabling information technology (IT) teams to actively engage with other members of the organization. It is recommended to connect with an external third-party organization that is well-versed in cybersecurity, particularly for medical device cybersecurity instruction for clinical engineering teams.

Removing Organizational Siloes between IT and Healthcare Technology Management Teams

Organizational silos can create major gaps in cybersecurity coverage. Health systems must leverage all human resources, including the biomedical engineering teams that maintain medical devices, to close the loop on cybersecurity initiatives.

Typically, 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 often lack IT and cybersecurity skills and training.
- Core network and cybersecurity attributes are not maintained in the computerized maintenance management system (CMMS). Only general attributes from medical devices are captured and documented in the CMMS.
- Clinical engineering policies, procedures and processes are not aligned to manage cybersecurity risks.
- Lack of coordination andsiloed structure between IT and clinical engineering.
- Every original equipment manufacturer (OEM) has disparate methods of sharing the availability of a validated or approved mitigation for medical devices impacted by a vulnerability, and there are no industry-wide standards 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.

Health systems can minimize these types of inefficiencies and inaccuracies by adopting tools and processes that make vital information more accessible to both IT and clinical engineering. Passive monitoring and identification tools can promptly detect vulnerabilities in network-connected medical devices and make

it easier for IT to develop remediation strategies, and for clinical engineering to implement patches and other compensating controls. 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 network signature. Up-to-date automated discovery in real-time combined with device profiling enables health systems to confidently identify authorized assets within their fleet.

Standardize Risk Assessment and Empower Continuous Improvement

Health systems must monitor and assess cybersecurity risk in medical devices in a way that aligns with the distinct functions these technologies serve in clinical environments. Knowledge, resources and frameworks tailored to medical device technology can support more accurate and proactive preventative measures against cyberattacks.

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. Tracking key characteristics of medical devices can help to establish a common understanding of risk and how to prioritize it.

Network connectivity: Can a device connect to the facility's networks, and is it currently connected? This narrows down and brings attention to devices that could be at risk for cyberattacks.

Protected Health Information (PHI) storage: Can a device electronically store identifying patient data, and does it currently do so? 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.

Food and Drug Administration (FDA) alerts and manufacturer recalls: 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 and cybersecurity, and partnerships in place to identify and address these urgent situations. Cybersecurity teams can take advantage of that efficiency when alerts and recalls are issued regarding medical devices.

Role in clinical care: Beyond the technical attributes of a device, it's important to understand how a device is used on a regular basis and the potential immediate safety risk of failure. 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: What is the potential risk of a device failure to organizational operations? These impacts could include disruption to the ability to deliver healthcare services or potential lost revenue centers. For example, the failure of a Compter Tomography (CT) scanner in an Emergency Room (ER) due to a cyberattack could force the healthcare organization to divert patients to other healthcare organizations which may result in significant lost revenue.

Once a health system understands the characteristics of risk, it is essential to apply that knowledge in a standardized method for prioritizing cybersecurity projects. Cybersecurity maturity is built on consistent approaches remediation, as well as data and knowledge resources. To ensure this standardization is achieved, there are key steps that must be taken. This includes accurately inventorying assets, assessing known threats, understanding the implications of device failure, gauging the risk of failure, evaluating the potential impact to patients and operations, prioritizing risks based on health system needs, and taking prompt action on identified priority projects. This ensures that all cybersecurity projects are properly prioritized to secure all the organization's assets.

Establishing a governance council can foster communication and accountability between all stakeholders involved in driving action that remediates known vulnerabilities and reduces overall risk. The groups that can contribute to a proactive approach for managing medical device security include IT, clinical engineering, operations, facilities and C-suite executives.

A centralized team managing intelligence streams is essential to ensure that organizational-specific mitigations and remediations align with an organization's risk appetite and posture. The governance council, working in tandem with clinical engineering and IT teams, should be plugged into all medical device technology integrations and related work processes. A properly enabled team should be able to monitor, detect and respond to cybersecurity threats more quickly when granted the appropriate training, coordination and improved visibility across organizational processes. Improved readiness is not just about shortening the response time when a breach occurs. It's also about increasing the ability to prevent attackers from gaining access in the first place.

Conclusion

Cybersecurity is one of the most pressing threats to healthcare, and the urgency will only increase going forward. Health systems understandably want to rise to the challenge quickly to protect their patients and the infrastructure that makes high-quality care possible. However, a thorough approach is needed to build sustainable security practices that address technology assets across the healthcare ecosystem, including medical devices. That approach requires comprehensive data, collaboration and established processes.

Health systems can start on the path to cybersecurity maturity by gaining accurate inventory visibility, breaking down organizational silos, and standardizing how their organization evaluates and addresses risk. Medical device technology and cyber threats will continue to evolve, but an organization with a strong, process-oriented foundation will be prepared to evolve with them. 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.

References

1. IBM Security. (2022). Cost of a Data Breach Report 2022.
2. https://www.globenewswire.com/news-release/2022/11/17/2557911/0/en/Healthcare-Cyber-Security-Market-to-Hit-70-55-Bn-by-2030-says-The-Brainy-Insights.html
3. https://www.grandviewresearch.com/industry-analysis/healthcare-cyber-security-market
4. Associated Press. (2021). Suit blames baby's death on cyberattack at Alabama hospital. https://apnews.com/article/technology-business-health-alabama-lawsuits-68c78e9d6af359842c0e9645b4577b50
5. 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
6. Ponemon Institute. (2021). The Impact of Ransomware on Healthcare During COVID-19 and Beyond. https://www.censinet.com/wp-content/uploads/2021/09/Ponemon-Research-Report-The-Impact-of-Ransomware-on-Healthcare-During-COVID-19-and-Beyond-sept2021-1.pdf
7. 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/
8. Health IT Security. (2022). 53% of Connected Medical Devices Contain Critical Vulnerabilities. https://healthitsecurity.com/news/53-of-connected-medical-devices-contain-critical-vulnerabilities
9. 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
10. Healthcare IT News. (2020). Cyber-talent shortage can put healthcare organizations at risk. https://www.healthcareitnews.com/news/cyber-talent-shortage-can-put-healthcare-organizations-risk