Sponsored by:

TRIMEDX℠

Cybersecurity in the COVID-19 era: Why it's time for health systems to formalize medical device cybersecurity

The world is becoming more interconnected, and the healthcare industry is no exception. Health systems are increasingly developing a connected infrastructure of medical devices and software that can generate and share valuable data. By 2025, 68 percent of medical devices will likely be connected, according to a survey of 237 medtech companies commissioned by Deloitte.

One of the main drivers fueling the growth of connected medical devices is the transition to outpatient care and the corresponding decentralization of these devices, according to Doug Folsom, CIO of TRIMEDX. He noted the COVID-19 pandemic has accelerated this expansion to alternate care sites.

"There is now forced reliance on connected devices whether it's for telehealth, monitoring patients at home or doing remote triaging," Mr. Folsom said.

This reliance on connected devices has underscored the risk of safety and privacy issues, especially since healthcare cybersecurity threats have significantly increased amid the pandemic. In late April, the World Health Organization reported a five-fold increase in cyberattacks since the pandemic started compared to the same period last year.

Cybersecurity attacks can cause significant financial and reputational consequences for healthcare organizations. If a hospital is unable to provide services due to a cybersecurity incident, patients will likely seek care elsewhere, which could mean both immediate and long-term revenue losses for the organization. In 2019, cybersecurity breaches cost healthcare organizations an average of $6.5 million, representing the highest cost among all industry sectors for the ninth consecutive year, according to a 2019 report from IBM Security.

"The reputational risks are also significant, especially if it's a data breach where you lost patients' health or payment information," Mr. Folsom said. "A lot of patients involved in a situation like that won't come back."

The rise in cybersecurity threats could also increase scrutiny among healthcare regulators and policymakers. Connected device inventories offer more convenience and access to information for both patients and hospitals. However, these stakeholders may begin to see them as a potential patient safety issue if a health system is targeted by a cybercriminal.

Full visibility is critical

To mitigate these risks, healthcare organizations must ensure they have full visibility into their medical device inventory. They must understand not only what devices they have, but the specific details of each to help identify any potential risk.

This visibility is especially important considering that medical devices today, with appropriate maintenance and servicing, can last well beyond predicted manufacturer life expectancy. As these devices age, they may no longer be supported, resulting in devices that may have vulnerabilities or require necessary updates or patches. Healthcare organizations need data on utilization, availability of medical devices and current cyber risk-scoring to help identify at-risk devices and know how to prioritize response activities.

"If there is an exploit that is impacting a certain operating system or device, you need to be able to quickly respond and understand what your exposure is and how to mitigate it," Mr. Folsom said.

To identify at-risk devices, organizations should know:

- Their complete device inventory across their organization
- What devices are already connected or capable of connecting to the network
- What operating systems and underlying software are on these devices

Organizations should then match this information up against what vulnerabilities or exposures exist from a cyber threat perspective, along with best practices for managing the threat to that type of device or operating system.

Based on these factors, healthcare organizations should consider creating a cyber risk score to help prioritize response activities. Responses may include re-placing at-risk devices with underutilized devices from other locations, or prioritizing an at-risk device for a replacement or upgrade.

Staying ahead of the curve

Cyberattacks are increasing in healthcare and pose serious threats to patient safety, patient experience and an organization's financial health. To mitigate these risks and stay ahead of the curve, health systems should consider putting a formal cybersecurity program in place now, according to Mr. Folsom.

"Cybersecurity in healthcare matters, and it is coming more to the forefront," he said. "Health systems need to stay ahead of those trends by making sure they are understanding and mitigating their risks way out in front."

He outlined four major components the program should entail:

1. Clearly outlined roles and responsibilities between the CIO, chief information security officer and other IT or clinical engineering team members.
2. A process to monitor and score cybersecurity risks.
3. A deep understanding of your medical device inventory to know how to manage those risks.
4. An active network monitoring solution that can look at your inventory in real-time and, in some cases, identify vulnerabilities or threats.

"These are really the key things health systems should be focused on during and certainly post-COVID-19," Mr. Folsom concluded. ■