Three key steps to securing clinical assets

By John W. Mitchell

45 million malware attacks cost healthcare organizations more than $20 billion in 2021, according to the U.S. Department of Health and Human Resources.

"Beyond the financial implications, a hospital cybersecurity breach can disrupt workflow and have dire consequences if patient care is brought to a standstill," **David Phillips**, service marketing leader for customer services at Philips Healthcare North America, told HCB News.

"There are very scary attacks occurring now against hospital medical devices," Phillips said. "Such threats can disrupt clinical workflow and patient care — and severely damage a provider's brand image — and bottom line."

The intersection of devices, health apps and platforms creates an unprecedented potential to transform healthcare and enable better health and care at lower costs. However, this intersection also means that data security for clinical assets is an imperative.

As health systems and hospitals are under unprecedented stress from the COVID-19 pandemic, their IT departments also are facing critical skills and staffing shortages as they strive to prevent cyberattacks. Risk mitigation is reaching a new degree of urgency in 2022.

Taking action to reduce risk

In his work helping health systems and hospitals protect medical devices and patients from cyber threats, David Phillips recommends three best practice security actions every chief information officer (CIO) should take immediately:

1. Take the time to familiarize yourself with how original equipment manufacturers (OEMs) design clinical assets for cybersecurity, and plan a sustainable life cycle management strategy.

2. Maintaining upgrade and patch level is critical for medical asset protection, and it is one part of a multilayered cybersecurity strategy. With each vendor/asset combination, first identify vulnerabilities, then prioritize remediation, and finally, determine the mitigation plan for each asset and track status.

3. Build a strong business case to help the board understand the sense of urgency about cyberattacks.This enables them to make informed investment decisions about medical device cybersecurity and budget accordingly. Medical device software maintenance drives compliance, similar to software maintenance in EMR systems and PACS.

"Philips Healthcare's experience as a medical technology OEM, as well as Philips' 25 year history as a multi-vendor service provider, gives it unique value as a cybersecurity partner," he explained. "By bringing all of our security expertise under one vendor-neutral umbrella and leveraging an industry-leading OEM footprint, Philips Healthcare aims to protect the entire medical equipment ecosystem."

As an example of that high-level security, Phillips pointed to a recent project undertaken for a large southeast medical center with a Level I Trauma program. As part of a comprehensive cybersecurity program initiative, the organization deployed Philips' asset management software InfoView, which identified and tracked over 12,000 connected medical solutions. The software analyzed important security governance parameters such as operating system, the network's capability to store/transmit PHI, networking capability type, and securing IP address and MAC addresses for better management of potential threats. These key metrics provided the organization the access to clear, actionable data that enabled confident decision-making from comprehensive insights gained with InfoView's real-time business intelligence reporting.

An end-to-end cyber solution

For true cybersecurity, Phillips stressed that OEM research and development must continually monitor systems and evaluate vulnerabilities and risk control. Protection from those threats should be factored into the capital acquisition decision process and revisited throughout the asset life-cycle.

"This systemic approach begins with product design features — like operating system hardening and use of operating system security features — and is carried through testing and deployment to robust policies and procedures for vulnerability management throughout the product life cycle," he said.

Through its partnership with healthcare cybersecurity company CyberMDX, Philips Healthcare offers its clients a level of protection that goes well beyond managing exposure through patches. The solution identifies and prioritizes actionable alerts for the entire inventory of connected medical devices. The alerts identify critical vulnerabilities and the overall solution streamlines vulnerability remediation and mitigation from patches and upgrades to more extensive compensating controls, like firewalls or segmentation.

To help healthcare provider organizations identify and address their cybersecurity concerns, Philips Healthcare offers a 30-day connected medical device risk assessment.

Providers need confidence that their cybersecurity service provider has customizable solutions to meet the unique needs of diverse medical facilities with all types of medical equipment, regardless of vendor.

To that end, Philips Healthcare offers a full range of connected medical device cybersecurity services. Cybersecurity related services include risk assessment, risk management, upgrade, detection and recovery, access management, audit and consulting.

Share this story: dotmed.com/news/57735

This article was sponsored by Philips.