COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 11. November 09, 2023 Security Checklist: Use Existing Assets to Manage Medical Device Risk

By Jane Anderson

Most health care institutions can improve the security of medical devices by extending existing technology, educating personnel and introducing cybersecurity best practices to the organization, according to a recent white paper.[1]

The white paper from security firm Cynerio noted that hospitals traditionally have adopted new technologies while underinvesting in cybersecurity protections. In addition, Cynerio pointed out that health care is a profitable sector for cybercriminals.

“With these challenges, there is one fortunate situation often overlooked—the foundation for medical device security is already in place at most institutions,” the white paper said. “By automating inventory and visibility, building on existing processes and technologies, prioritizing vulnerability remediation, and ensuring that basic cyber hygiene is in place, organizations can greatly reduce the risks posed by their growing inventory of medical devices.”

The white paper offered a series of steps organizations can take to improve their medical device security:

- **Get on top of inventory and visibility**. To secure a device, Cynerio said, an organization must know its existence and see where it interacts with the network. “Unfortunately, many hospitals still have not completed the basic step of delivering an accurate, up-to-date inventory of their medical devices,” the report said.

  A manually populated spreadsheet or a computerized maintenance management system (CMMS) will not work for this task, the report said. “The only way to have a point-in-time view of the entire inventory is to automate the process through continual scanning of the network to discern what is connected, and where. This gives a hospital visibility into not only what is connected, but also where each device is located.”

  Still, while inventory and visibility are “absolutely necessary first steps,” the white paper said, “institutions should not mistakenly believe that the job of securing devices is finished when all devices are visible. Visibility does not secure devices; it simply makes it possible to secure them.”

- **Clarify organizational roles**. Ownership of device security at some hospitals falls under the chief information security officer, while other organizations house the function in other teams, Cynerio said. While there’s no one correct approach, it’s key to clarify roles in advance to ensure that the groups are not working in parallel or at cross purposes, the white paper said.

- **Build on existing processes**. This approach helps organizations deal with the challenge of having inadequate staff, the white paper said. Rather than disrupting operations to launch a new medical device security program, organizations can attach security components to existing processes, such as new device setup, maintenance of existing devices and updates to networking infrastructure.

"For example, it is significantly more efficient to patch devices in batch efforts during setup and routine maintenance than to reactively address time sensitive issues," the authors wrote. "More broadly, it is far more efficient to segment a network and properly onboard devices than to launch inherently insecure devices into a flat network, a combination known to exacerbate most healthcare cyberattacks."

- **Build on existing CMMS technology**. Almost every hospital has a CMMS system, but the white paper authors contend that few hospitals use their systems to their full potential. "Such tools provide a foundation for growth when it comes to medical device security," they said.

  When an inventory and visibility tool is integrated with an existing CMMS, "the two solutions work together to automate inventory, enhance data, provide workflow functionality, and provide a holistic view of the inventory from a single pane of glass," Cynerio said. "When risk reduction and incident response solutions are added, organizations can work through the CMMS to prioritize and execute on."

  In addition, the authors wrote that many institutions will benefit from seeking out expertise on device security from their in-house or outsourced security operations center, a managed security services provider, providers of device security technology solutions and experts from other industries "who can bring a fresh set of eyes to the challenges faced in healthcare."

- **Mitigate risk with informed prioritization**. According to the white paper, hospitals need two kinds of information about each known vulnerability found in a medical device. The Common Vulnerability Scoring System measures the severity of each vulnerability, while the Exploit Prediction Scoring System measures the likelihood of a vulnerability being exploited.

  "Both measures are critical to effective prioritization of remediation, as a vulnerability that has almost no likelihood of being exploited is a low-priority fix, regardless of severity," the authors wrote. "Risk reduction tools that take both scores into account enable hospitals to systematically and effectively reduce risk."

- **Integrate cybersecurity best practices to medical device security**. "One of the best ways to protect medical devices is to align security practices with the best practices that are likely already being practiced in other parts of the network," the authors wrote, noting that "There are any number of guides and checklists that can help institutions confirm that their processes are adequate."

- **Adopt medical device best practices from other industries**. Health care does not need to invent best practices for medical devices since other industries already have done so, the white paper said. "Many of the steps needed to secure a hospital (efficient device patching, microsegmentation, incident detection, etc.) have been developed and perfected by the financial, insurance, and commercial industries over the last decade. Adopting these proven approaches will help avoid the time, effort, and investments already invested by more forward thinking industries."