HealthManagement.org
Promoting Management and Leadership

Too confident about your cybersecurity?

Despite budget constraints, the majority of healthcare IT professionals remain confident that their connected medical devices are protected from a cyberattack, according to Zingbox's 2018 healthcare security survey.

The survey, which included 400 U.S.-based healthcare IT decision-makers and clinical engineers, found that 41 percent of these IT executives do not have a separate or sufficient budget for connected medical device security. This lack of resources however should not be cause for alarm, as 87 percent of respondents are confident about the security of their connected medical devices. This is down slightly from the 90 percent of respondents who were confident about their devices' security in Zingbox's 2017 survey.

Researchers pointed out though such confidence could stem from misperception about securing connected medical devices. They found that more than two-thirds of respondents believe that traditional security solutions designed for laptops and PCs can secure connected medical devices. This result was down slightly from the 2017 survey, which found that 72 percent of respondents had this belief about traditional security solutions.

“Much of the healthcare professionals’ confidence on the device protection and real-time device vulnerability in this survey is based on the use of traditional IT security solutions. The false sense of security can be disastrous for healthcare organisations who will be caught unprepared for the next round of ransomware/malware attacks,” the Zingbox report opined. For the first time, clinical and biomedical engineers were included in Zingbox’s healthcare security survey.

See also: **How to build a secure cyber-security dashboard**

The report includes these other findings:

- 85 percent of clinical/biomed engineers are confident that they have an accurate inventory of their connected medical devices, although close to two-thirds of them rely on manual processes to inventory devices.
- Room-to-room audit is the most common manual process used to inventory devices, the report said, noting this method, aside from being resource-intensive, is "susceptible to human error, and is certain to be outdated by the time it’s completed.”
- The second most common manual process, static asset management, is “only as accurate as the manual entry into the system,” the report added.

A recent article in HealthcareITSecurity.com highlights the importance of industry-wide collaboration

and proactive preparation in maintaining the security of medical devices that directly support quality patient care.

The article found that experts across the healthcare industry agree that organisations can stay ahead of malicious actors by engaging with longer-term industry efforts to improve security while taking immediate steps to close gaps in the medical device ecosystem.

“When it comes down to it, everybody really does want the patients to be treated safely and securely,” said MITRE IT and Cybersecurity Integrator Penny Chase. “But there’s a lot of work to be done, and the bad guys are always ahead of us. We really need to figure out how we can come together and better protect ourselves.”

Chase recommended that healthcare providers add procurement language in contracts with security requirements for device manufacturers, such as requiring devices to run antivirus software and be upgradable.

Source: HealthITSecurity.com
Image source: Pixabay

Published on : Tue, 13 Nov 2018