SPONSORED

Privacy & Security

Protecting the endpoints

Survey finds gap in provider defenses.

By leidos | April 19, 2018 | 09:12 AM

The top-line finding in the *2018 HIMSS Cybersecurity Survey*, released in March, provided cold comfort to healthcare CIOs hoping for better news in the battle against breaches.

"Of the 239 respondents in this year's survey, 75 percent said that they had experienced a 'significant security incident' in the past 12 months," said Rod Piechowski, HIMSS senior director of health information systems. "It's a hard job to secure all of this."

One reason for the difficulty: The number of vulnerable targets at an organization is growing by leaps and bounds. The demand for real-time data is increasing the number of networked medical devices and mobile endpoints across healthcare organizations, and efforts to defend the edge is straining IT resources.

In fact, 28 percent of survey respondents listed "too many endpoints" as a significant barrier to remediating and mitigating cybersecurity incidents. Yet less than 5 percent included mobile devices in their penetration testing. And less than 4 percent included medical devices.

"As more devices come into an organization's network, adjusting a cybersecurity program to reflect the importance of endpoint security and security of mobile/medical devices is paramount," said Lee Kim, director of privacy and security for HIMSS North America.

The first point of adjustment comes at the very beginning – the procurement phase. Kim recommends that organizations conduct an initial assessment to make sure potential vendors and devices have a good cybersecurity track record, or to learn about any adverse findings relevant to security of the device.

"You need to put your security, clinical and legal teams together to vet these devices from the procurement phase," Kim said. "It's due diligence. That will help you establish a baseline from the get-go."

After procurement, good mobile-device-management software can track devices, remotely locate the devices and wipe data remotely if the device has been lost or stolen. At a bare minimum, organizations should keep an accurate inventory of devices and an accurate and thorough end-to-end risk assessment and management strategy.

But good security practices are more than just sound strategy concerning the procurement of devices. Appropriate implementation, configuration and use of such devices are also important. For instance, a wireless printer with an unchanged, default password that is exposed to the internet represents a gaping hole in a network's defenses. Securing printers and other devices may cause headaches for the staff, but this is critical for security.

Yet this vigilance may also lead to conflicts between users and IT staff.

"If end users are fighting against the security controls to get their work done, then these controls are being defeated and an organization has an inherently weaker security system," Kim said. "As another example, if a nurse is fighting with the technology instead of tending to that patient who is really suffering, there's a problem. At the end of the day, patient care needs to be the key priority for both clinician workflow and IT security."

With three-quarters of providers reporting incidents in the last 12 months, a cybersecurity incident is a question of when, not if. "The best thing an organization can do is to be prepared," Piechowski said. "The more-mature organizations have playbooks so that when an incident occurs, they know exactly what to do."

Since the *2018 HIMSS Cybersecurity Survey* also found that a lack of people (52 percent) and a lack of financial resources (47 percent) were also barriers to remediating and mitigating cybersecurity incidents, it may make sense to partner with an experienced cybersecurity team on issues such as endpoint security. A consultant with a strong client list provides economies of scale and is likely to bring both efficiency and best practices.

Bottom line: "Humans are your first line of defense ***and*** your biggest threat," Kim said. "So, it's important to educate your end users. It's important to encourage security awareness throughout your organization."

Topics:
Privacy & Security

More regional news

Q&A: Using AI to expand access to breast cancer screening
By Emily Olsen | August 26, 2022

Student loan forgiveness for healthcare IT workers
By Andrea Fox | August 26, 2022

One comprehensive system makes for a more efficient physician practice – and free evenings
By Bill Siwicki | August 26, 2022

By: leidos


Automating workflows to improve care coordination


Data analytics: Leveraging analytics and EHRs to power better healthcare


3 key questions for pop health success


Clinical optimization:

ADDITIONAL RESOURCES


Taking a Strategic Approach to Experience True Digital Transformation


Transforming Data into Actionable Information that Improves Performance


Best Practices for Go-Live Success


Automating workflows to improve care coordination


Data analytics: Leveraging analytics and EHRs to power better healthcare


3 key questions for pop health success


Clinical optimization: Liberating the data from EHRs


Beyond meaningful use: How enterprise IT modernization enables providers to focus on improving outcomes

ADDITIONAL RESOURCES


Taking a Strategic Approach to Experience True Digital Transformation


Transforming Data into Actionable Information that Improves Performance


Best Practices for Go-Live Success