COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 1. January 11, 2024 Security Checklist for 2024: Experts' Recommendations

By Jane Anderson

Health care covered entities (CEs) and business associates (BAs) should take several steps to better fortify their organizations against cybercrime, experts told *RPP.*

Ransomware will continue to proliferate in 2024, and it will evolve in the types of tactics being used, said Rebecca Herold, CEO and Privacy Professor of Privacy & Security Brainiacs. The health care industry could see more tactics "that will or could cause significant safety/physical harms to the associated patients," she said.

In addition, Herold said she expects that "new types of cybercrimes utilizing the data collected through tracking pixels on health care sites will emerge and quickly proliferate as cybercrooks realize how easy it is now to establish themselves as a legitimate third-party marketing or similar type of business, and then obtain access to a huge amount of PHI [protected health information] via those Meta Pixels and similar types of online tracking tech."

The HHS Office for Civil Rights (OCR) has been signaling via guidance documents, free tools and penalties applied that it will focus on full security and privacy program elements in the coming year, Herold said. Therefore, "it would behoove health care CEs and BAs to make time to review their own full security and privacy programs and identify where there are gaps," she said.

Review Government Publications

Health care entities should start the process by reviewing the newly published *Healthcare Sector Cybersecurity: Introduction to the Strategy of the U.S. Department of Health and Human Services,* Herold said.[1] That publication references various other documents that would be helpful, she said.

In addition, Herold noted that OCR has mentioned documents from the National Institute of Standards and Technology (NIST), specifically special publication SP 800-66r2, "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide"[2] and the NIST Cybersecurity Framework.[3] She said CEs and BAs should review those NIST documents and then take actions to fill any gaps.

Specifically, to address security threats that might be seen in 2024, Herold recommends that health care entities:

- Review the full security and privacy program components and identify and then close gaps with current requirements and HHS-stated expectations.
- Provide better, more comprehensive and frequent security and privacy training to all workers and ensure BAs are doing the same with their workers.
- Establish policies and procedures to monitor, be aware of and provide rules for implementing new technologies and associated activities within the organization's entire digital and physical data and IT business ecosystems, including onsite facilities and remote activities.

David Harlow, vice president and chief compliance and privacy officer of Insulet Corporation, backed a focus on staff, devices and networks and vendor management. (Harlow noted that the views he expressed were his own.) Harlow said organizations should:

- Improve staff training, in part by using "nano-learning" modules. "Training must be mandatory," he said, noting that some organizations cut off access to the network for people who have not completed security training in a timely manner, while other organizations dock pay or year-end bonuses. Organizations should assign training based on each employee's department and job function, use a "just in time" approach to assigning training, test practical knowledge and retrain as needed, Harlow said.

- Enforce a hardened perimeter with a "belt and suspenders" approach. "If your organization is not ready to end its 'bring your own device' policy, then access to your network and conduct of business using personal devices needs to be more tightly controlled: on [virtual private network] only, and with recurring log-in and [multi-factor authentication] requirements even on company devices, to the point of it being annoying to most users," Harlow said. "Do not expose yourself to any zero-day attacks—enforce a vigilant tracking and patching program. This can never eliminate all risk, but having such a program in place meant that many companies were spared the pain of the SolarWinds attack, for example."

- Bring a continuous improvement mindset to vendor management. "Most health care data breaches are engineered exploiting a vendor vulnerability," Harlow said. "Because the threats are dynamic, management of the threats must be dynamic." Every organization brings a different perspective to the effort, and that effort should be informed by a senior-management-level enterprise risk management exercise so that the data privacy and security efforts of the organization are clearly in alignment with organizational priorities, he said. "But the common thread is making the vendor management effort a living process."