Report on Patient Privacy Volume 21, Number 1. January 07, 2021 Health Care Cybersecurity Checklist for 2021

By Jane Anderson

Experts interviewed by *RPP* recommended a variety of strategies to stay ahead of evolving security threats this year, particularly as the COVID-19 pandemic winds down and threats from highly capable bad actors ramp up.

The best approach to cybersecurity now is a more agile approach, said David Harlow, chief compliance officer at Insulet Corporation. “One way of framing this is ‘design thinking’—delving into the need in front of us at the moment, engaging in rapid prototyping and creative idea generation.”

To explain this, Harlow said he uses an analogy that’s been used in communicating how to protect against COVID-19: the Swiss cheese approach. “What does this mean? It means that we need many layers of protection (many slices of cheese),” he said. “Each slice may have a hole or two in it, but the holes don’t line up, so the effect of all the slices stacked up together is that there are no holes that run from the top of the stack through to the bottom. More concisely: The perfect is the enemy of the good. Each slice needs only to be good. If we wait for each slice to be perfect, we’ll still be waiting a year from now.”

Roger Shindell, founder and CEO of Carosh Compliance Solutions, said he expects training and general security awareness to be the most important HIPAA security issues this year. In response, health care entities should conduct online and in-person training on the latest threats and how to respond to them appropriately, he said. “Entities should also focus on defining HIPAA to employees and building that directly into their day-to-day culture.” Shindell lists three top priorities for health care entities to address:

1. **Employee training.** This should include planned in-depth training that keeps employees engaged, Shindell said. It also can be enhanced by creating monthly meetings or committees to help advise leadership.

2. **Incident response plans**. Organizations already should have an incident response plan, but the plan should be tested quarterly with either a tabletop review or a planned “incident,” Shindell said.

3. **Updating policies and procedures**. These should be reviewed regularly, he said. “With COVID changing how some organizations function on a day-to-day basis, they need to be updated. This is important to hold all employees accountable to the standards of business” and HIPAA compliance.

John Ford, strategist at IronNet Cybersecurity, said that health care entities need to realize they cannot defend their organization by themselves. “They simply can’t spend their way to an environment where they alone can withstand attacks from nation-states and criminal groups with nation-state capabilities,” he said. That said, health care entities should take several steps to defend themselves:

- They should look for capabilities that allow them to have visibility and situational awareness in real time across health care and other sectors, Ford said.

- They should invest in multilayered backup solutions that are operationally tested and proven effective in restoring files in order to recover rapidly from a ransomware event, he said. “This capability should come with the knowledge that threat actors tend to go after the backup solution first, so having penetration testing and red team engagements performed externally” to identify gaps should be integral to this overall solution.

- Health care entities should make it a priority to perform a very comprehensive tabletop exercise that involves people from all aspects of their organization, Ford said. “In general, these exercises involve several scenarios, and the goal is to understand what everyone’s responsibility is during an event and to address gaps that are identified during the exercise. This is an invaluable exercise to invest in and could potentially reduce severe impacts to patient outcomes,” he explained.

The massive attack stemming from the SolarWinds system spotlighted the level of risk facing health care entities, Ford said. “This platform is used by thousands of organizations, health care included, to manage IT devices in various environments,” he said.

“This is happening on a scale we have not seen before,” Ford said. “Instead of this being a direct attack on a health care entity, this attack focused on the product that supports thousands of these entities. This is a huge threat, as the attack came from an update to a trusted software application and therefore bypassed traditional security controls.”

To help defend themselves against these types of attacks, organizations need to closely monitor alerts coming from the Cybersecurity and Infrastructure Security Agency and implement recommendations from Microsoft, Ford said. In addition, they need to invest in solutions to provide advanced detection of unknown threats, he said.

Rebecca Herold, president of SIMBUS360 and CEO of The Privacy Professor, warns all organizations, including covered entities, business associates and subcontractors, to be more diligent in confirming the security of the actual security tools they are using. “In 2021, we know that U.S. entities are being targeted—and successfully infiltrated—by nation-state hackers,” she said. “And we know that these hackers are coming through the tools that have been compromised...Organizations cannot assume that simply because they are using a security tool that the tool has not itself been compromised by hackers.”

More broadly, Herold noted that many of the current remote working and telehealth practices were put into place quickly and without sufficient security and privacy planning. “Every covered entity needs to review their remote working and telehealth practices to identify security risks, and then take appropriate actions to mitigate them, and they need to ensure they incorporate security requirements for the Internet-of-Things devices that could be incorporated by workers into those environments.” Specifically, Herold recommended that organizations:

- Start with performing a risk assessment, focusing on work-from-home environments that may include family members in their own coworking or remote school situations, and connections to business associates and other third parties.

- Update the security and privacy policies and procedures, and then provide training to employees and send frequent awareness reminders for these policies and procedures.

- Pay more attention to the security and privacy oversight of business associates and business associate subcontractors.

Michelle O’Neill, director of corporate compliance at Summit Health Management, strongly recommended staying on top of federal alerts and keeping organization boards and leaders informed.

Education is key, and monthly newsletters with quick videos and quizzes—with prizes—have been an effective way to provide tips and training, O’Neill said. “Phishing campaigns also go out monthly, and we monitor the results of those campaigns so that we can continue to remind workforce members how easy it can be to fall victim to an attack” and gauge where we need to focus our training efforts, she said.

Contact Harlow at dharlow@insulet.com, Shindell at rshindel@carosh.com, Ford via Cara Masessa at masessa@merrittgrp.com, O'Neill via Joy Lee-Calio at jleecalio@shm.net and Herold at rebeccaherold@rebeccaherold.com.