COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 1. January 07, 2021 Security Threats Soar From Nation-State Bad Actors as the New Year Gets Underway

By Jane Anderson

Security threats to health care entities will continue to escalate in 2021, as bad actors with significant capabilities target pandemic-weary organizations still struggling with a stay-at-home workforce, cybersecurity experts report.

This year's threats will look familiar: phishing, ransomware and information technology (IT) changes will all play a role, experts told *RPP*. However, those threats are evolving to become more sophisticated, making defense against them more difficult even as new tools arrive.

"As artificial intelligence is being rolled out on the defensive side, bad actors have similar tools that allow for a once-complicated task or hack to be as simple as the push of a button," reported Roger Shindell, founder and CEO of Carosh Compliance Solutions.

In addition, the pandemic has caused massive uncertainty, said John Ford, a strategist at IronNet Cybersecurity. "Attackers excel when change and uncertainty consume our efforts," he said. "They have the benefit of watching and anticipating both old and new vulnerabilities while the rest of us are trying to do our jobs, whether that is directly tied to care delivery or the monumental support system that our health care system requires."

There's little good news, said Michelle O'Neill, director of corporate compliance at Summit Health Management in New Jersey. Last year "included a variety of new security threats and attacks directed at hospitals and health care organizations," O'Neill told *RPP*. "The thought is that in 2021, hospitals and health care organizations will continue to be a target, but that the cybercriminals will improve their abilities and become more successful."

To ease the way through the pandemic, OCR provided some leeway to health care organizations during 2020, specifically providers and business associates (BAs) that provide telehealth services, O'Neill pointed out. "This was very helpful in providing patients the care they need and quickly, without fear of penalty. But this also added new security threats to patients, physicians, organizations and business associates that provided these telehealth platforms," she added.

The pandemic has heightened both the urgency and impact of attacks, Ford said. "If you roll back time to before the pandemic, ransomware and data theft was still an issue, but the covered entities were operating in an expected state and had better availability of resources to address the attacks. Fast forward to today, and we have an extremely stressed workforce, an IT and security environment that has been significantly modified, and the volume and scale of the attacks has been amplified."

Rebecca Herold, president of SIMBUS360 and CEO of The Privacy Professor, noted that through much of 2020, there has been less scrutiny and oversight of BAs by covered entities (CEs) and no perceptible oversight of subcontractors by BAs. "This is concerning given that now a large portion of CE, BA and subcontractor employees are working remotely, typically from home offices. Keep in mind that these home offices are usually also the work areas for the others in the home, and also the new school rooms for the students, from pre-K through college, who also inhabit the homes."

When multiple people from multiple organizations or schools livestream in close proximity and on the same network, the risks are significant, Herold said. "Rarely are the online meeting tools and internet connections secured appropriately, leaving them open to attackers that have access to the wireless network, and also those connecting to each of the computing devices attached not only to the wireless network but also to the various organizations' and schools' networks."

Threats Include Impersonation, BYODs

In addition to the well-known security threats of 2020, new threats likely will emerge this year. For example, Shindell said he expects bad actors to begin impersonating employees or business partners. Anything is possible with today's technology, he said. "It's just human nature to trust people visiting your organization, and even more so if they mention names or things particular to it."

The way to prevent this problem is having strong policies and training, Shindell said. "Have a chain of approval methods, standard questioning of each person, and a list of approved/vetted vendors," he said. "Also, you should have an organization perform a physical penetration test to ensure the plans are utilized."

Herold said she anticipates new telehealth attacks, along with attacks through employee-owned devices and patient-owned devices that are connected to health care networks and systems.

This year, Herold said, expect more ransomware attacks against BAs and their subcontractors. "Ransomware makes cybercrooks very rich, and those cybercrooks are realizing that each covered entity is using dozens, hundreds or even thousands of business associates to perform mission-critical services or to provide products for them. They are realizing that the CEs depend upon their BAs, and that the BAs are potential goldmines." She said that, in her experience, BAs "do not comply with all HIPAA requirements" and are often "generally very lax and deficient in their security practices for the protected health information [PHI] that their clients have entrusted to them."

Phishing attacks for other types of security and privacy exploits beyond ransomware—for example, to get access to PHI "treasure troves"—also will start targeting BAs and subcontractors, Herold said. In addition, the Internet of Things (IoT) will proliferate "at unprecedented rates," she said, noting that "each of those devices creates an entry point into the networks to which they attach, and each may be attaching to many different networks. Attacks will increase through these new IoT pathways."

Ford said ransomware will take center stage this year, ramping up even further from the high 2020 levels. "We've seen a substantial rise in ransomware since the onset of COVID, and as advancements in vaccine creation and distribution continue, so will the prevalence of these attacks," he said. "We anticipate an increase in the sophistication of these attacks, with criminal groups leveraging tools that rival nation-state actors. As the operating environments for most organizations have changed due to COVID, we also anticipate a greater number of these attacks focused on cloud-based environments."

Organizations likely will see more instances where these threat actors apply additional pressure for ransom by putting exfiltrated data on data leak sites, where additional bad actors can buy and access PHI, leading to additional privacy concerns, Ford said.

"What I see being different for 2021 is the boldness and reach of the attacks," Ford said, adding that the recent hacks of federal agencies and the cyberdefense firm FireEye serve as notice of escalation. "While these events are not exclusive to health care, it is reasonable to anticipate brazen efforts on a larger scale directed at health care entities and their supply chain," Ford said.

"How these events translate to HIPAA compliance will remain to be seen, but I can only hope that our regulatory community takes into consideration the fact that health care entities are not fighting a fair fight when it comes to nation-state-level attacks," he said. "These events are simply beyond the capabilities and budgets of all but a few health care entities in our nation. Certainly negligence can and should remain an enforceable component of HIPAA violations, but this sector would better be served by having both HHS and health care entities join hands and battle these threat actors as one team in place of doing so in isolation. I suspect they will. Until then, stay tuned as this further develops in 2021."

Old Devices Pose Problems

Still, small threats can cause big problems for health care. "There are so many specific issues that pose an unusual/unique threat to the security of PHI," O'Neill said. "Believe it or not, old devices, like fax machines, USBs that security is unaware of, and PCs that are out there and not approved by security are definitely areas that keep privacy and security professionals up at night. These will continue to be a threat into 2021."

Health care entities often deal with these issues reactively, but proactive measures can help catch these devices before they become a problem, she said. Education can help encourage team members to tell security personnel about these devices so that security can intervene and protect the data stored on the devices, she added.

Contact 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.