COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 1. January 13, 2022 2022 Outlook: More Dangerous Ransomware Coupled With Inadequate Security Practices

By Jane Anderson

As the COVID-19 pandemic enters its third year, real "security fatigue" with pandemic-related issues will combine with cybercriminals' increasingly sophisticated capabilities to create an acceleration of ransomware and other security incidents, cybersecurity experts predict.

The threats of this year will look like those seen in 2021, with the caveat that they're likely to be worse, three experts told *RPP*. They warned covered entities (CEs) and business associates (BAs) to be wary of unsecured Internet of Things (IoT) devices, cobbled-together systems that allow staff to work on-site or at home, and lapses in performance of basic security strategies.

"Going into 2022, we will see more cyber threats directed against hospitals, especially ransomware attacks," said Chuck Everette, director of cybersecurity advocacy at cybersecurity company Deep Instinct. "In 2020 and 2021, ransomware criminal gangs have found that targeting and attacking hospitals, outpatient clinics and other health care facilities during the time of a global pandemic is lucrative."

In fact, HHS Secretary Xavier Becerra used his first-ever end-of-year message to warn of the "urgent need to remain vigilant against cybersecurity threats," and noted that cybersecurity experts have identified a vulnerability in Apache Log4j, a "ubiquitous piece of software that exists in thousands of applications—including control systems for medical devices and hardware—that, if exploited, could result in data exfiltration or ransomware and significantly disrupt your ability to deliver health care and pose a threat to national security."[1]

Becerra recommended that health care organizations:

- Implement the guidance issued by the Department of Homeland Security Cybersecurity & Infrastructure Security Agency (CISA) for the Apache Log4j information.[2]
- Review cybersecurity resources from HHS and CISA.
- Diligently monitor networks, raise cybersecurity awareness, and maintain readiness of emergency operations procedures and continuity plans.
- Promptly report any cybersecurity incidents to CISA or the FBI.

"As health care and public health leaders, we rely on your vigilance and partnership to protect our country from nefarious actors looking to disrupt or exploit our critical health infrastructure," Becerra wrote.

The COVID-19 pandemic has allowed cybercriminal gangs to expand and grow their own networks by leveraging many businesses' hybrid work-from-home model, plus migrations to the cloud, Everette said. "This has greatly expanded the health care industry footprint, in turn increasing the attack surface for these cybercriminals, creating a target-rich environment. Add in the sense of urgency to recover quickly from a cyberattack, and health care organizations typically will pay ransoms quickly in order to get back online and limit client impact. This also has resulted in cybercriminals increasingly attacking health care more [often], due to the rapid ransom payday."

Criminals Leveraging Pandemic

Cybercriminals already are using new, complicated code to impede analysis, and are spoofing modern anti-virus and security solutions, Everette said. "In 2022, we will see cybercriminals beginning to commercialize obfuscation techniques that employ polymorphic and metamorphic components to evade legacy security solutions as well as the newer advanced solutions utilizing machine learning," he said. "We will see a trend where common cybercriminals will have access to, and will be using, adversarial AI [artificial intelligence] techniques to bypass and confuse traditional security solutions."

These tools began with nation-state hackers, Everette said, but now are becoming readily available to common cybercriminal gangs. "As this new sophisticated technology gets in the hands of these cybercriminals, the list of victims will continue to grow at an exponential rate," he said. "It is a constant cat-and-mouse game that cybersecurity professionals cannot lose."

Rebecca Herold, president of SIMBUS360 and CEO of The Privacy Professor, agreed that ransomware techniques will become even more numerous and sophisticated. "What will be different are the increased ways in which the ransomware will be planted within the networks," she explained. "Besides using phishing messages and malicious sites, the ransomware crooks will utilize IoT devices, which are largely unsecured, as pathways into networks, where they will then plant the ransomware, subsequently launching ransomware some later date or after the occurrence of a specified trigger event."

Medical Devices Take Spotlight

David Harlow, chief compliance and privacy officer for medical device company Insulet Corporation, said it's a basic decision for cybercriminals to continue to target health care organizations: "Ransomware attacks are likely to continue simply because they continue to be successful," he said. "One growing trend is the threat to release versus destroy the ransomed data."

For Everette, the most important HIPAA security issue in 2022 is vulnerabilities in medical devices that lead to critical security risks. "As more and more medical devices are following the IoT movement, everything is being connected to networks and the internet," he explained. "In 2021 we [saw] several high-profile recalls and security alerts from the FDA [Food and Drug Administration] and other medical manufacturers related to vulnerabilities in these devices."

Soon, Everette said, cybercriminals will "start targeting these devices in earnest. Think of the ramifications of a criminal group gaining access to, say, pacemakers and the networks that they operate on, and able to reprogram or even disable devices unless a ransom is paid. This is a line they have already shown they are willing to cross. Manufacturers need to recognize the critical risks and be proactive and identify and patch before they make it into the wild. Additional funding for monitoring and safeguards is also critical."

Herold said she also sees IoT devices as a major threat. "Physicians, nurses, staff and other workers, and those within CE facilities, are bringing their personally owned IoT devices into the environment and using them for patient care," she said.

'Explosion' of Wired Devices

"For example, large numbers of doctors are already carrying their Amazon Echos with them from room to room while checking on patients and using these nifty IoT gadgets to ask questions about specific types of symptoms, to take notes and to record...patient injuries and other types of physical images. These types of devices typically lack sufficient security in general—the security capabilities that are available are almost never set as a default—so those using the IoT product often don't realize the security is not in effect. Practically none, or none, meet HIPAA security requirements. So, not only are CEs creating security risks to PHI [protected health information] by using IoT devices, they are also creating privacy risks to patients and co-workers, as well as creating HIPAA noncompliance situations. These IoT products are creating similar types of risks with the BAs' networks, which often connect to CE networks, as well," Herold said.

In addition to the IoT devices being incorporated within the networks, there's been "an explosion of medical devices" connected to CE networks, along with connections to Wi-Fi networks inside the CEs and to third parties, Herold said. "All these connections that can potentially access medical devices that patients are using to support treatments, and even their lives, give malicious code capabilities to literally kill people by shutting down devices, or changing the settings on the devices. This is the exploitation of killware. BAs also bring these threats to the CEs as well, through their even more unsecured and uncontrolled uses of IoT and the access that many BAs are given to medical devices," she said.

"Add on to this that many-to-most of these devices and systems use devices with software and firmware that have significant vulnerabilities, such as those within Log4j," Herold said. "Most CEs, and virtually all except for the largest BAs, will likely not apply the patches to protect against Log4j exploits. So, there will be a significant increase in 2022 from these types of security incidents, on top of all the other types of increasing security problems and incidents."

Still, Harlow said it may be unlikely for ransomware gangs to "deliberately start killing people by exploiting flaws in systems and device security, since that would inevitably increase law enforcement efforts to find and punish them. Right now they are enjoying a lower level of attention from law enforcement."

Risk Assessments Lacking

Most CEs and BAs continue to fail in performing risk assessments regularly enough, Herold said. In addition, they fail in performing risk assessments following major systems changes, organizational changes, when incorporating new technologies within their digital business ecosystems, and following security incidents and privacy breaches, she said.

Also, most CEs and BAs need to update their security and privacy policies, with the associated procedures, she said, adding, "these very important documents, which all staff should know about and reference regularly during the course of performing their job responsibilities that involve PHI, are rarely read and rarely updated. That leads to what is often the reason for out-of-date policies and procedures, and not performing adequate risk assessments: the lack of sufficient training, and not being provided with ongoing awareness communications and supporting activities. Lack of adequate and frequent training, and little-to-no awareness communications, have been problems within CEs and BAs since HIPAA was enacted. Training and awareness practices need to be improved significantly."

In fact, Herold said she believes the most important HIPAA security issue for CEs and BAs in 2022 is updating their risk assessment and HIPAA compliance audit processes. She added that some may be surprised at her choice for the number one issue, but noted that "I've seen significant degradation of risk assessment policies in the past several years, and a large portion of CEs, and most BAs, are back to doing a checklist-type of activity instead of doing a true, thoughtful and comprehensive risk assessment. This is resulting in really bad decisions made by CEs and BAs, such as sending unencrypted PHI in emails and text message, posting PHI on social media sites, and not responding to the requests and questions from insureds and patients for which HIPAA gives them the legal rights to obtain accurate and timely answers."

Herold pointed out that HIPAA requires CEs and BAs to perform risk assessments, “and from penalties and resolution agreements, it is clear that the expectation from HIPAA is for CEs and BAs to perform them at least annually.” A properly performed risk assessment can reveal major and minor security vulnerabilities and threats, she said, and this then allows CEs and BAs to mitigate the risks before hackers exploit them.

Complexity Drives Problems

Harlow said that “the complexity of the technology stack” is the biggest security risk for health care in 2022. “We often say that humans are the weakest link, and that’s not really fair to all the very dedicated people involved in the delivery of health care services and in the privacy and security efforts we undertake to protect health care data,” he said. “When a vulnerability in an open source logging tool used in myriad software packages effectively exposed much of the world’s critical digital infrastructure to hackers—the recently reported Log4j vulnerability—it is clear that we can’t blame social engineering or human error of end users for all security ills.”

The combination of “ubiquitous connectivity and antiquated connected devices used in health care” represents “one of the great subterranean security threats to PHI,” Harlow noted. “Unless old connected infusion pumps used in hospitals, for example, are updated (if possible), replaced (if affordable) or put on their own network (though a proliferation of networks creates its own problems), they can be used as vectors for attacks to the broader institutional infrastructure.”

And, as the COVID-19 pandemic enters its third year, Harlow said, it’s clear that people are worn down: “Security fatigue is a real issue. People are tired of masks, tired of COVID tests, and tired of extra hurdles erected by IT security teams related to the evolving threat environment and continued remote work by many knowledge workers.”

In addition, Everette said, “health care today still fails to identify cybersecurity as a critical or as an investment priority. IT budgets over the past two years have been used to expand cloud infrastructure and help provide access to staff working from home. At the same time, security infrastructure should have been at the core of the execution and design, but we are seeing more and more that some organizations are just now going back and trying to bolt it on after the fact, for it was skipped or not thought of. Hopefully, it is not too late.”

Basics Remain Unaddressed

A ransomware attack on a health care organization, Everette said, “is 100% preventable. There are security solutions today that are able to predict and prevent even the newest ransomware attacks. The issue is over the past five to seven years, it has been drilled into C-level executives that you can’t prevent an attack, the best you can do is monitor, detect and respond—EDR [endpoint detection and response] systems. This is not a valid solution for ransomware today. These EDR systems play into the cyber-gangs’ hands by granting them additional time on health care networks. The attacks need to be prevented before they are launched, shutting down the attack itself and the lateral movement.”

Herold said that no health care organization can be “100% secure” unless it completely unplugs and uses trusted workers to do work involving PHI manually—something that’s impossible. “However, security will be dramatically improved, and lead to far fewer or even no significant hacking incidents, when CEs and BAs implement security basics. With comprehensive and thoughtful security management programs, not only will a significant number of attempted hacks be blocked, but those that get through will be identified much more quickly, thus mitigating the harms that would have otherwise occurred with a hit-or-miss type of security program in place.”

Contact Everette via Katie Brookes at brookes@merritgrp.com, Herold at rebeccaherold@rebeccaherold.com and Harlow at dharlow@insulet.com.

[1] Xavier Becerra, Letter to health care and public health leaders, December 30, 2021, https://bit.ly/32UedbV.
[2] "Apache Log4j Vulnerability Guidance," Cybersecurity & Infrastructure Security Agency, December 2021, https://bit.ly/3mOwsH3.