COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 1. January 11, 2023 Outlook 2023: Ransomware Threats Multiply as Rogue Nation-States Sponsor More Attacks

By Jane Anderson

Ransomware—including increased attacks from criminal groups affiliated with rogue nation-states such as Russia and North Korea—will continue to dominate the health care security landscape as 2023 gets underway and the COVID-19 pandemic begins to fade into the rearview mirror, cybersecurity experts said.

In addition, the proliferation of Internet of Things (IoT) devices across health care likely will lead to new breaches, and privacy and security issues surrounding web trackers such as Meta Pixel will draw scrutiny to code on organizations' web pages and apps, the experts said.

The anticipated threats for 2023 evolved from those prevalent over the past several years, said Michael Hamilton, co-founder and chief information security officer of security firm Critical Insight. "Threats will continue from mainly criminal groups known for intentionally targeting the health sector," Hamilton told *RPP*. "However, there are now three nation-states engaged in theft and extortion using cyber methods and changing tactics by state-sponsored actors may create new urgency."

For example, Hamilton said, "China has been found to have engaged in COVID relief fraud, the FBI is warning that the Sandworm group—also state-directed by Russia—will be using ransomware, and North Koreans are responsible for billions in direct losses. Disruption in the health sector also serves the strategic goals of these countries. I think nation-state actors will be moving up as a threat priority to the sector."

Business email compromise will be the most important HIPAA security issue in 2023, Hamilton said, adding, "[it's] not because of regulatory penalties, but because hospitals are struggling financially, and any direct monetary loss could be existential to small organizations. There is also more money lost to [such incidents] than ransomware, and tactically it is simpler to execute."

Threat Readiness: Poor

Ransomware trends in 2022 saw a drop-off in the third quarter, according to a report released in December by cybersecurity firm Guidepoint Security.[1] The health care industry remained in the top three targeted industries and most frequently was attacked using Lockbit ransomware, the report said.[2]

However, Rebecca Herold, president of SIMBUS360.com and CEO of The Privacy Professor, told *RPP* that most covered entities (CEs) and nearly all business associates (BAs) still are failing to guard against ransomware.

"Instead of building and using more secure code for applications and systems, to strongly encrypt all data in storage and transit, establishing more effective backup and recovery procedures and practices, and providing employees with more frequent and effective education about how to spot ransomware attempts and how to react to them when they slip through, most organizations decided instead to either just take the chance that they would not be 'targeted' and did nothing, or they purchased cyber liability insurance and assumed—usually incorrectly—that the insurance would cover all the costs of a ransomware attack," Herold said. "Wake up! Every organization is a target."

Ransomware will continue to expand until business leaders recognize the need to invest in strong and effective security practices, Herold said. These include improving their secure systems engineering and coding practices, encrypting all data everywhere in storage and transit, strengthening backup and recovery practices and tools, and providing education to workers to help them stop ransomware attacks from succeeding in the first place, she said.

David Harlow, chief compliance and privacy officer at Insulet Corporation, said ransomware's popularity among criminals stems from the fact that it's reasonably simple to use and effective. "I don't see ransomware attacks declining any time soon, especially given the ease with which they may be mounted at scale—there are even ransomware-as-a-service packages available and the barriers to entry are low to nonexistent," Harlow said. "That just emphasizes the need to have appropriate countermeasures in place."

Pixels, IoTs Pose Challenges

CEs and BAs also are failing to guard against threats inherent in the use of IoTs, Herold said, adding that IoT products have increased the attack surfaces and threat vectors in most organizations.

"The number of IoT products increased from 11.28 billion in 2021 to 13.1 billion in 2022," she said. "That is a couple of billion more devices, mostly unsecure, that can be used to create more pathways into and out of organizations' networks, systems, applications and databases. They can also be compromised and used as bots to launch DDoS [distributed denial of service] attacks, to spread other types of malware and to use in many ways to surveil those within the digital ecosystems. And most of the associated organizations are completely unaware of the activities that IoT products are supporting and performing within their digital ecosystems."

IoT products have become ubiquitous within most organizations, Herold said, and the associated business leaders do not realize all the IoT devices that are attached to their networks.

Harlow agreed that IoT devices would represent an increasing threat in 2023. "As the Internet of Things grows, and as more and more people resume pre-pandemic travel and other activity levels, I think breaches of connected devices—not just smartphones, not just laptops as part of the email threat vector—could be a big growth area," Harlow said.

Still, Harlow said he views "widespread misunderstanding of web tracker configuration" as the most important HIPAA security issue in 2023. Several CEs have reported large breaches stemming from misconfigured web trackers, such as Meta Pixel, and OCR in December issued guidance on web trackers.[3]

Health care organizations need to determine what web trackers, if any, are active on their systems, Harlow said. "A self-audit is required, with external help, if necessary," to mitigate that risk, he explained.

At the same time, he reminded organizations not to neglect the basics. "Sometimes, the things that are not on anybody's radar are the things that should be on everybody's radar, and therefore we don't put them on lists," Harlow said. "One recent example is patch management to protect against zero-day exploits. That should be really basic, but we know that it is regularly handled poorly by organizations that should know better."

Christopher Strand, chief risk and compliance officer at Cybersixgill—which offers automated, real-time dark web threat intelligence—said he expects cybercriminals to continue to use a variety of social engineering attacks, such as phishing, as 2023 gets underway. These are used "with the primary goal of commandeering critical systems via third-party systems or data request spoofs that can give them access to health care systems," Strand told RPP.

"The goal of either method will be to either successfully gain access and implement ransomware or exfiltrate the

data after the illicit data request is successful," Strand said. "With the multitude of proposed changes to the [HIPAA] health care rules around the 'right to access' and ownership of private health care data, we may see an increase or change in 2023 where criminals build or evolve the many data request spoofing techniques or exploitation vehicles like pretexting to gain access and exploit sensitive health care data."

Although the price of Bitcoin plunged in mid-2022, leading to a reduction in traditional ransomware,[4] Strand noted that cybercriminals are simply changing their objectives, "often turning to crypto swap markets and sometimes targeting systems that have access to real dollars like payroll where they can conduct low and slow attacks, profiting over time." He added, "Although it may be a reduction, ransomware is still prevalent and still a frequent choice when targeting health care systems."

Cloud Migration Poses Threat

Jon-Michael Smith, health IT futurist and head of healthcare & life science analytics – data integration at Qlik, said he believes the most critical data security issue health care organizations will face in 2023 "and beyond" will likely be connected to—and stem from—organizations' large-scale migration of data and protected health information to cloud-based applications.

"While cloud-based applications provide the scalability, flexibility, and real-time decision-making health care organizations need for both operational/business decisions and to support better patient care, it is more critical than ever to work with vendor partners that support strong data governance and meet or exceed HIPAA compliance to protect their users," Smith told *RPP*.

"One of the most important things health care organizations can do to maintain data security is to strategically control data accessibility—and these two things can be done simultaneously," Smith added. "Data security does not have to come at the expense of data accessibility—doing both at the same time is possible and critical."

Meanwhile, use of aging or unsupported IT systems within health care remains prevalent, Strand pointed out. "Due to cost factor in procuring many types of health care systems across the industry, as well as the need for them to operate with little downtime, there has consistently been an over-reliance on stretching systems as far as possible—which can include employing systems in production that are no longer supported or no longer have security patches available," he said.

"This situation invites the possibility of a multitude of vulnerabilities that cyber-criminals can act upon, as often the exploits are re-used to deliver the payload that will execute and exploit, such as a ransomware attack," Strand said. "The most important security issue then will be the need for health care enterprises to become more proactive in prioritizing their system gaps and remaining vigilant to possible and predictable targeting that may occur due to the nature and state of their systems."

Strand added: "There is a huge need for security personnel to move to a continuous risk-based approach when monitoring systems for potential problems."

Phishing, Ransomware Emails Remain Constant

Harlow said he views security for health care organizations similarly to protective actions taken in the COVID-19 pandemic: A robust security system should include "a steady diet of security certifications for staff and systems; penetration testing; and layered administrative, technical and physical protections, like the Swiss cheese model of COVID protection: vaccines, masks, isolation, handwashing, etc. No one element of the system of protection is adequate. But if we layer them all on top of each other, we have a better chance of preventing a compromise," he said.

"There are always changing conditions. And there will always be new threats—old wine in new bottles," Harlow said. "The subject lines of the phishing and ransomware emails may change, and there are always some new sorts of attacks, which are effective and dangerous because they are novel and unpredictable, but the broad range of social engineering exploits linked with simple 'click me!' campaigns for the most part change only on the surface."

Contact Hamilton and Strand via Danielle Ostrovsky at ostrovsky@hi-touchpr.com, Harlow at dharlow@insulet.com, Herold at rebeccaherold@rebeccaherold.com, and Smith via Michelle Schaefer at schafer@merrittgrp.com.

1 Guidepost Security, "GRIT Ransomware Report – Q3," July-December 2022, https://bit.ly/3CiVUvZ.
2 Jane Anderson, "HC3 Warns of LockBit Ransomware Threat as Affiliates Ramp Up Attacks," *Report on Patient Privacy* 21, no. 12 (December 2021), https://bit.ly/3vAH1RZ.
3 Jane Anderson, "OCR Issues Guidance, Checklist on Web-Tracking Technologies," *Report on Patient Privacy* 22, no. 1 (January 2023).
4 U.S. Department of Health & Human Services, "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates," December 1, 2022, https://bit.ly/3XS8GL1.