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."