COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 6. June 09, 2022 Cybersecurity Experts Urge Senate to Act, Say Health Care Threats Have Never Been Greater

By Jane Anderson

Federal lawmakers, fresh on the heels of approving bills mandating swift reporting of breaches and ransomware payments to the Department of Homeland Security, are ramping up their focus on cybersecurity in hospitals and health systems, citing threats to patient care and sensitive information from cyberattacks.

At a Health, Education, Labor and Pensions Committee hearing,[1] experts painted ransomware and phishing attacks as the greatest cybersecurity threats to the health care sector, and urged Congress to help by facilitating safe information sharing, incentivizing cybersecurity best practices, and requiring security measures that currently are voluntary.

"Ten years ago, 'cyber' and 'health care' were not even placed in the same sentence," said Denise Anderson, president and CEO of the Health Information Sharing and Analysis Center (ISAC) in Oakton, Virginia. "Today, because of the rise in digital health care, the proliferation of advances in technology, and the efficiencies of connecting devices and data, the cyber threat surface in health care has ballooned and the threat actors have followed."

Cybersecurity Experts Urge Senate to Act

Joshua Corman, who founded the volunteer cyber-safety initiative I am The Cavalry and served on the federal Health Care Industry Cybersecurity Task Force, concurred that the threat level has never been higher.

"I'd like to bring you good news," Corman told the committee. "However, the more consequential the subject matter, the more important it is to be forthright and avoid exaggeration in either direction. The candid truth is, I am more concerned about the cybersecurity of U.S. health care than I ever have been. Attacks have gotten stronger, but defenders have not—and many got weaker. The number of health care attacks has grown. The costs of the ransomware payments [have] grown. The impacts of attacks are no longer merely measured by record count, fines, ransom payments or recovery costs, double-digit millions of lost revenue and worse—they include degraded patient care and human life."

'Death Danger Zones' Magnified

Corman said that "ransoms can strain hospitals to levels associated with excess deaths." He cited a study of a state hit hard by ransomware for a statistically significant observation period, and said that in the same state, with the same population, during the same pandemic, controlling for hospital type and size, "locations hit by ransom both achieved these excess death danger zones sooner and stayed there longer than their peers."

He added, "delayed and degraded care affects outcomes for time-sensitive conditions. [Intensive care unit] strain significantly added delays. Cyberattacks made them worse. While this excess death math is a feature of the pandemic strains, the systems analysis revealed the elevated risk of loss of life when, for example, ambulance diversions are too far away for the time-sensitive conditions. Also, with the financial strains from COVID and the substantive losses of skill workers in health care, we will not return to safer capacity levels for some time."

Corman said he was pleased to see that Congress enacted legislation in March that mandates swift reporting of breaches and ransomware payments to the Cybersecurity & Infrastructure Security Agency.[2] However, he noted that he was "disappointed to see a multiyear rulemaking process. With so many attacks and such poor reporting, we need to move as quickly as possible. We cannot shift to studying and preventing attacks without adequate and timely visibility into them."

He also said that Congress may want to consider mandating certain security measures, citing specifically the National Institute of Standards and Technology (NIST) Cybersecurity Framework. "Industry prefers voluntary, and yet, we're now seeing more and more devastating attacks to health care. FDA [Food and Drug Administration] has done a great job raising the bar for the cybersecurity of new devices and [has] even issued safety communications and affected recalls, yet hospitals continue to use these recalled devices and unsupported devices—as the norm," he said. "Surveys show legacy and unsupported software remains unaddressed."

Corman concluded: "Seatbelts weren't voluntary. I don't believe fire escapes were voluntary—nor kitchen sanitation codes for commercial restaurants. Public safety isn't free. The lack of sufficient public safety and public good is also dis-economic. Further crisis of confidence in the public in modern health care will drive devastating harms to the public safety, economic and national security. The cybersecurity of health care is not trending in the right direction. We can do something about that. We must."