COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 4. April 09, 2020 COVID-19 Creates Crisis in Security; Experts Warn of Thin Resources, Unprepared Teams

By Jane Anderson

The COVID-19 crisis poses massive security risks for HIPAA covered entities, with some employees sent home to work with little notice and frontline clinical staff members pressed to their limits, security experts say.

To ensure protected health information (PHI) is guarded, covered entities and business associates need to step up security, particularly in the work-at-home environment and in bring-your-own-device situations. They also should quickly roll out network safeguards to reduce risk.

"Unfortunately, bad actors excel at taking advantage of any opportunity that creates concern in health care," says Cathie Brown, vice president of professional services at Clearwater Compliance LLC. "COVID-19 has created a perfect storm for HIPAA-covered entities. We no longer have a 'normal,' and things are changing by the minute."

As an industry, health care does not have a mature security posture, Brown warns. "I'm concerned the bad actors are using COVID-19 as an opportunity to infiltrate our networks and systems undetected," she tells *RPP*. "Once we are over this hurdle, we will see exploits increase."

Ransomware and data breaches remain the top threats, "simply because they work," Brown says, but she adds, "Unfortunately, I think we will see new types of exploits result from this time of crisis as well."

Art Ehuan, vice president for cyber risk and resilience management at The Crypsis Group in McLean, Virginia, told a March 30 webinar audience that his company is seeing a spike in attacks.[1]

"Companies are being targeted since this event started escalating in the United States," Ehuan said, adding that he's spoken with antivirus companies and other security companies, and they're seeing a spike in attacks and risks. "One of the messages I keep carrying is, we weren't prepared for this pushing out of the remote workforce, and we are definitely afraid that we have created vulnerabilities inside of our companies by pushing out so quickly."

Working from home poses the biggest risk to security. Organizations have been required to act quickly to send workers home and may be relaxing security controls as well as their existing policies and procedures, Brown says. "We already know how sophisticated bad actors are in crafting email campaigns to lure users into phishing attacks. We are already seeing emails that may play into our emotions promising the 'latest news' or 'a potential vaccine.' Links contained in these emails can open the door for malicious code such as ransomware to enter the systems," Brown warns.

The fast switch to remote work has been overwhelming to many security and IT staffs, said Cynthia Larose, chair of the privacy and cybersecurity practice at law firm Mintz, Levin, Cohn, Ferris, Glovsky and Popeo PC. "This is something that usually takes months to accomplish within an organization, but this has been done in days." There are gaps in security, Larose told webinar attendees, and security personnel need to be aware of those gaps in order to start fixing them.