Report on Patient Privacy Volume 24, Number 1. January 11, 2024 2024 Outlook: AI-Fueled Cyberattacks May Proliferate But It Could Aid Recovery: It's Not All Bad News

By Jane Anderson

Bad actors will continue to exploit known and unknown vulnerabilities, launch phishing attacks and deploy ransomware in 2024, experts say. However, there's a new, worrisome twist as privacy and security professionals ponder the year ahead: artificial intelligence (AI) has the potential to make all the threats much, much worse.

AI tools such as ChaosGPT—a malevolent version of the popular tool ChatGPT—can help hackers craft more effective cyberattacks. These tools also will help new generations of bad actors try their hands at the craft, experts say.

"Essentially, I expect more of the same [threats in 2024 as in 2023], but many of them will be supercharged by generative AI and other tools that are readily accessible to all," said David Harlow, vice president, chief compliance and privacy officer of Insulet Corporation. (Harlow noted that the views he expressed were his own.)

"There are already threat actors buying cheap, easy-to-implement 'ransomware as a service' packages, and the ease with which these can be deployed—with reasonably well-written phishing emails drafted by ChatGPT, among other vectors—means that the volume of attacks will only continue to increase," Harlow added.

Michael Hamilton, founder and chief information security officer of Critical Insight, predicted the rise of AI-generated adaptive malware such as ChaosGPT. Still, it's not all bad news, Hamilton said. "Detection and analytics using AI will begin to work, so we will be able to start fighting back here," Hamilton said during a webinar. "I don't have any examples of that now, but I believe that'll come to pass in the upcoming year."[1]

RPP asked privacy and security experts about the top threats to protected health information (PHI) in 2024 and steps organizations should take to prepare. AI was top of mind.