COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 5. May 09, 2024 'I Will Not Rest'; 'I Am All In': Remarkable Breach Hearing Sees Pledges by UHG CEO, Sen. Wyden

By Theresa Defino

United Healthcare Group (UHG) CEO Andrew Witty was in a board meeting on Feb. 21 when officials interrupted with the news that Change Healthcare—a clearinghouse UHG subsidiary Optum had purchased for $1.3 billion in October 2022—was in the throes of a ransomware attack.

Hackers had actually entered the system nine days earlier via a single, external "portal" that—contrary to UHG policy—was not protected with multi-factor authentication.

"The minute we knew about this, in fact, even before I'd been briefed, our team had followed the right steps and disconnected Change from all other connections because it was critical to prevent the infection [from] affecting any other provider or network in the country," Witty recently testified before the Senate Finance Committee.[1] "That worked. We know that did not happen. So, we contained the blast radius to just Change."

But however "contained" Witty believed the blast to be, months later, the ripples continue as UHG itself now works to identify—and notify—affected patients, who likely number in the millions. Witty described other steps UHG took after the biggest health care data breach in history, including building a new system "from scratch," details that may prove instructive to other covered entities (CEs) and business associates (BAs). For example, Witty said he alone decided to pay a ransom to get data back but did not mention the amount, reported to be $22 million.[2]

UHG—along with providers and other customers—is still struggling to return to what Witty termed "pre-incident" operations. For their part, members of Congress and the HHS Office for Civil Rights (OCR) are eager to learn why the server was left vulnerable, if UHG will face sanctions once OCR completes the investigation it announced in March and what new laws or regulations might be needed.

At the hearing, Sen. Ron Wyden, D-Ore., Finance chair, floated the idea of creating mandatory minimum cybersecurity standards for CEs and BAs and perhaps others, a concept Witty embraced (from the witness table, at least).

Wyden also argued that because of its size—UHG is the nation's largest insurer in terms of revenue—it is among those with "an obligation to protect their customers and to lead on this issue" and that the firm had "let the country down" by not preventing the attack and by employing inadequate recovery efforts.

Ensuring the security of health care data "is one of the most important issues I've taken on," Wyden said. "The intersection of health policy, economics, and national security is now front and center. And I am all in on this."

UHG Repels Attacks 'Every 70 Seconds'

Witty repeatedly apologized and expressed regret about the breach, including UHG's initial handling of it. And while he took responsibility, Witty said health care as a whole needs help "to reduce the attack velocity." According to his written testimony, given to the committee in advance and posted online, UHG "alone repels an

attempted intrusion every 70 seconds—thwarting more than 450,000 intrusions per year."[3]

Following the breach, firm officials "deployed the full resources" of UHG," Witty testified. "I want to assure the American public we will not rest—I will not rest--until we fix this," he said, adding that "cyber experts continue to investigate the incident."

The May 1 hearing was remarkable for a variety of reasons, including that details about how firms handle ransomware attacks aren't often discussed in public. Senators were rarely argumentative with Witty, and the hearing contained less grandstanding than usual for Capitol Hill. Senators seemed genuinely interested in what Witty had to say and shared with him details of providers in their states that are still reeling and need UHG's help. Witty promised to provide assistance.