COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 5. May 09, 2024
UHG's Breach Response May Prove Enlightening for Others

By Theresa Defino

Organizations typically deal with ransomware attacks out of the public eye, but the massive scale of United Healthcare Group's (UHG) February breach made that an impossibility. UHG CEO Andrew Witty was recently on the hot seat before the Senate Finance Committee for two-and-a-half hours, explaining how the breach occurred. The hearing also featured pronouncements by committee chair Sen. Ron Wyden, D-Ore., and others about efforts needed in the wake of the nation's largest breach.[1]

Witty offered details about the steps UHG undertook in response to the breach. These may prove instructive to others in a similar situation.

"Our response to this attack has been grounded in three principles," Witty testified.[2] "To secure the systems, to ensure patient access to care and medication and to assist providers with their financial needs." He described UHG's response as "swift and forceful to contain the infection."

After locating the server that was breached, UHG "immediately severed connectivity and secured the perimeter of the attack [site] to prevent malware from spreading," a strategy Witty said was successful. "There is no evidence of spread beyond Change Healthcare" to other parts of UHG.

UHG alerted the FBI "within hours of the ransomware launch" and has kept the agency updated on its actions, Witty said. As has been publicly reported, UHG paid a $22 million ransom, a decision Witty said was his alone. "This was one of the hardest decisions I've ever had to make, and I wouldn't wish it on anyone," he told the committee. Witty said nothing else about this, and no committee member asked him about it.