Change Healthcare cyberattack was due to a lack of multifactor authentication, UnitedHealth CEO says

May 1 2024, by Tom Murphy

Andrew Witty, Chief Executive Officer of UnitedHealth Group, testifies at a Senate Finance Committee hearing examining cyber attacks on health care, and the Change Healthcare cyber attack, Wednesday, May 1, 2024, on Capitol Hill in Washington. Credit: AP Photo/Jacquelyn Martin

The Change Healthcare cyberattack that disrupted health care systems nationwide earlier this year started when hackers entered a server that lacked a basic form of security: multifactor authentication.

UnitedHealth CEO Andrew Witty said Wednesday in a U.S. Senate hearing that his company, which owns Change Healthcare, is still trying to understand why the server did not have the additional protection.

His admission did not sit well with Senate Finance Committee members who spent more than two hours questioning the CEO about the attack and broader health care issues.

"This hack could have been stopped with cybersecurity 101," Oregon Democratic Sen. Ron Wyden told Witty.

Multifactor authentication adds a second layer of security to password-protected accounts by having users enter an auto-generated code. It's common on apps protecting sensitive data like bank accounts and meant to guard against hackers guessing passwords.

Hackers gained access to Change Healthcare in February and unleashed a ransomware attack that encrypted and froze large parts of the company's system, Witty said. The attack disrupted payment and claims processing around the country, stressing doctor's offices and health care systems by interfering with their ability to file claims and get paid.

Andrew Witty, Chief Executive Officer of UnitedHealth Group, testifies at a Senate Finance Committee hearing examining cyber attacks on health care, and the Change Healthcare cyber attack, Wednesday, May 1, 2024, on Capitol Hill in Washington. Credit: AP Photo/Jacquelyn Martin

While UnitedHealth quickly disconnected the affected systems to limit damage and paid a $22 million ransom, Witty said. The company is still recovering.

"We've literally built this platform back from scratch so that we can reassure people that there are not elements of the old attacked environment within the new technology," Witty said.

Witty told senators that the company was in the process of upgrading

Change's technology, and he was "incredibly frustrated" to learn about the lack of multifactor authentication, which is a standard across UnitedHealth.

In March, the Office for Civil Rights said it would investigate whether protected health information was exposed and whether Change Healthcare followed laws protecting patient privacy. The company said earlier this month that personal information that could cover a "substantial portion of people in America" may have been taken in the attack. But company officials have said they see no signs that doctor charts or full medical histories were released after the attack.

Protesters hold up signs saying "Stop Denying Us Care" as Andrew Witty, Chief Executive Officer of UnitedHealth Group, front, gathers his papers after testifying at a Senate Finance Committee hearing examining cyber attacks on

health care, and the Change Healthcare cyber attack, Wednesday, May 1, 2024, on Capitol Hill in Washington. The people were protesting claim denials and prior authorization requests that they say delays care. Credit: AP Photo/Jacquelyn Martin

Protesters hold up signs saying "Stop Denying Us Care" as Andrew Witty, Chief Executive Officer of UnitedHealth Group, front, gathers his papers after testifying at a Senate Finance Committee hearing examining cyber attacks on health care, and the Change Healthcare cyber attack, Wednesday, May 1, 2024, on Capitol Hill in Washington. The people were protesting claim denials and prior authorization requests that they say delays care. Credit: AP Photo/Jacquelyn Martin

Andrew Witty, Chief Executive Officer of UnitedHealth Group, testifies at a Senate Finance Committee hearing examining cyber attacks on health care, and the Change Healthcare cyber attack, Wednesday, May 1, 2024, on Capitol Hill in Washington. Credit: AP Photo/Jacquelyn Martin

Witty also told senators he was "deeply, deeply sorry," and the company would not rest until the problem had been fixed.

Change Healthcare provides technology used to submit and process insurance claims—about 14 billion transactions a year. UnitedHealth bought Change Healthcare in a roughly $8 billion deal that closed in 2022.