Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Oversight and Investigations Ranking Member Kathy Castor

Hearing on "Examining the Change Healthcare Cyberattack"

May 1, 2024

Cyberattacks have become an unfortunate part of our daily lives. We are so interconnected online now — communications, energy grids, online platforms, and health claims clearinghouses like Change Healthcare — they are all targets. Ransomware groups and other threat actors are constantly probing corporate and government systems for vulnerabilities. And there are reports of major data breaches almost every week - sometimes due to malfeasance, sometimes sophisticated cyber hackers. Despite regular cautionary warnings, the largest health insurance company in the country was caught totally unprepared.

Change Healthcare, which is part of the mega-health conglomerate United Healthcare, did not have basic cybersecurity protections in place. Because of that, it suffered a ransomware attack and was unable to recover its systems in a reasonable period of time, leading to serious harm to doctors, providers, pharmacies, and patients across America.

Even with the limited information that has been made public, it is clear that there were multiple system failures.

First, UnitedHealth was not using multi-factor authentication on a remote desktop access application, Citrix. Multi-factor authentication is a very basic yet effective security measure that everyday Americans have implemented on their mobile devices, bank accounts, and email logins. In fact, the Department of Health and Human Services has recommended the practice since 2022 through its publication "Cybersecurity Practices for Medium and Large Healthcare Organizations" and specifically called out the importance of multi-factor authentication in a June 2023 newsletter. In that advisory, HHS noted that multi-factor authentication or other authentication processes stronger than a single password were necessary when an entity provided remote access. UnitedHealth ignored that advice.

Second, it appears that hackers freely roamed through Change Healthcare's systems for a week without being detected. There are essential network cybersecurity monitoring features that might have picked up and flagged unusual user activity, but that apparently did not happen here.

Third, whatever user credentials the hackers had access to appear to have allowed them to roam across the entire Change Healthcare system unimpeded.

Fourth, the hackers were able to deploy a ransomware attack within the Change Healthcare network, suggesting a lack of adequate controls or user permissions that could have prevented malicious software from holding their system and valuable health data ransom.

And fifth, there appears to have been a lack of any continuity or contingency plan to address such a crisis. As your testimony states, Mr. Witty, lots of time and resources were spent completely rebuilding your network. Yet it is unclear why there was not a reliable backup or continuity plan in place that would have both prevented the need for complete network reconstruction and dramatically reduced the amount of time for transactions to begin moving again.

At each of these key points, UnitedHealth Group failed. Whether it was a failure to properly invest in cybersecurity or a lack of adequate oversight and accountability within the company is an open question, but the bottom line is that there were multiple opportunities to prevent, detect, and mitigate this attack, and UnitedHealth Group failed at every single one.

In case any other companies, particularly health companies, are asleep at the wheel when it comes to cybersecurity, this is yet another wake-up call. Cyber threats are pervasive and worsening. Ransomware attacks can hold hostage the most sensitive of personal data and profits from paid ransoms only strengthen and encourage ransomware groups to grow and carry out more attacks. These are no longer exceptional events—they are a constant and must be properly prepared for.

While there are lessons to be learned, I want to make clear that this crisis is not yet over by any means. There are pharmacies and providers that have not yet been able to reconnect to Change Healthcare's systems. There is a massive amount of personal health information out there that needs to be accounted for. And in addition to the questions you will receive today, there are numerous questions outstanding from this Committee in a bipartisan letter that we sent you on April 15, and we look forward to your written answers promptly.

I thank the Chairman for putting on this important hearing, and I yield back.