Opening Remarks
Chair Cathy McMorris Rodgers
Health Subcommittee Hearing: Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack
April 16, 2024

INTRO

Thank you to everyone for being here today as we discuss cybersecurity in health care and the recent Change Healthcare cyberattack.

While I am disappointed that UnitedHealth Group chose not to make anyone available to testify today, so the Committee and the American people could hear directly from them about how that specific cyberattack occurred...

...I will note UnitedHealth briefed E&C members recently on the matter and have committed to testifying at a future hearing.

Health care cybersecurity was already a concern before the Change attack, and I look forward to today's discussion about what the federal government, doctors, hospitals, and others have done right...

....and where there is opportunity to improve the resiliency of the health care sector.

CHANGE CYBERATTACK

The Change Healthcare cyberattack is just the most recent case of ransomware targeting our health care system...

...and, due to Change's integration with so many of the health care providers and payers, it is still impacting providers and health care organizations across the country.

I have heard concerns from providers, rural hospitals, and many others...

...all worried about what this cyberattack means for them.

And just this morning, the Change Health hackers were posting stolen data from the ransomware attack.

There are still many unanswered questions and lessons to be learned from this attack.

How did this attack gain entry to the Change system?

How can hospitals, doctors, and others best protect themselves?

What other third parties do our nation's health care providers rely upon that, if taken offline, could have a similarly negative impact on the U.S. health care system?

HEALTH SYSTEM CONTEXT FOR CHANGE

Health care infrastructure is crucial for patients receiving the care they need, and, sadly, this will likely not be the last breach or ransomware attack that will happen.

Patient data is valuable, and it is housed online.

That is why we must continue to examine health care cybersecurity and make sure that patient data remains protected.

HHS has overall responsibility for ensuring cybersecurity within health care across the U.S. federal government...
And the Administration for Strategic Preparedness and Response, or ASPR, has been designated as the “one-stop shop” responsible for leading and coordinating the cybersecurity efforts—both within HHS and with external partners.

However, there seems to be multiple offices and agencies that have some role in our cyber response.

The Office of Civil Rights, the HHS Chief Information Officer, the Office of the National Coordinator, and, in this most recent response, CMS, all played a role.

As our health care system becomes more consolidated, the impacts of cyberattacks—if successful—may be more widespread, pulling in even more agencies and offices within HHS.

E&C CYBER WORK

This Committee has led at examining cybersecurity across all sectors.

In 2019, Congress made explicit that part of the responsibilities of ASPR is preparedness and response to cyber threats.

In 2020, a bill led by Dr. Burgess, which passed through this Committee, encouraged health care organizations to adopt strong cybersecurity best-practices.

Last Congress, this committee worked to give FDA more authority over cyber security of medical devices.

And more recently, in the reauthorization of the Pandemic and All-Hazards Preparedness Act reported by this committee, we made it explicit that cybersecurity should be considered and prioritized as part of ASPR's National Health Security Strategy...

... and the Energy and Commerce Committee will continue leading the way in examining this issue.

CONCLUSION:

I hope we can use this hearing today to learn more about the Change Healthcare cyberattack and the response.

Is this a unique situation?

What do providers and patients need to know and look out for?

I don't want this committee to be back here in five or 10 years, after more patients' health care is disrupted by known criminal actors finding vulnerabilities in the cyber security of our health system.

To prevent that, I look forward to hearing from our witnesses about:

What can health care learn from other sectors?

Are there more federal authorities HHS needs?

What is the best balance to get better adoption of existing cybersecurity practices?

I look forward to the discussion today and yield back.