Chairman Peters Opening Statement As Prepared for Delivery
Full Committee Hearing: In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector
March 16, 2023

Today's hearing will examine cybersecurity threats facing the healthcare sector, how both the federal government and health care providers are working to combat these threats, and what actions Congress should take to bolster our cybersecurity defenses against these attacks.

Health care is a rapidly growing sector of our economy that employs more than 18 million workers, and is made up of both public and private sector organizations related to patient services, medical devices and manufacturers, and electronic health and medical records, that store considerable amounts of personal information, making them frequent targets of attacks.

In recent years, increasingly sophisticated cyber-attacks in the healthcare and public health sectors have posed alarming threats to people in Michigan and across the country.

Cyber-attacks on hospitals, and other health care providers, can cause serious disruptions to their operations, and prevent them from effectively providing critical, lifesaving care to their patients. Breaches can also lead to the exposure of sensitive personal and medical information of patients and health care personnel.

Most recently, the DC Health Link, a health insurance marketplace for residents and lawmakers in the nation's Capital, experienced a cyber-attack that exposed the personal data and information of tens of thousands of people, putting victims at risk of identity theft, scams, and additional cyber-attacks.

Earlier this year, in my home state, the University of Michigan Health System experienced a cyber-attack that temporarily limited access to their public websites. Thankfully in that attack, no patient information was compromised and the issue was quickly resolved.

These relentless cyber-attacks show that foreign adversaries and cybercriminals will stop at nothing to exploit cybersecurity vulnerabilities our critical infrastructure and most essential systems.

What is most concerning about these attacks is that they don't just compromise personal information, they can actually affect patient health and safety.

Last month, a ransomware attack on Tallahassee Memorial HealthCare in Florida took the hospital's IT systems offline for more than a week, and required them to divert patients to other facilities and cancel procedures until they could restore their networks.

A 2019 catastrophic ransomware attack on the Spring Hill Medical Center in Mobile, Alabama may have even led to a patient's death. The attack prevented health care providers from using equipment to monitor a baby's condition during delivery. As a result, the infant tragically passed away because of delayed medical care.

This shocking example shows just how grave the consequences of cyber-attacks in the healthcare sector can be. Given the threats facing this sector, and the potential life or death consequences, there is no question that investments in healthcare cybersecurity are also investments in patient care.

This Committee has already taken important steps to strengthen cybersecurity for our critical infrastructure sectors, including the healthcare sector. Last Congress, the Committee advanced a bipartisan bill I introduced along with Senator Portman to require these organizations to report cyber-attacks and ransomware payments to the Cybersecurity and Infrastructure Security Agency.

This law will help ensure that government is able to better track cybersecurity threats to our critical infrastructure, provide more transparency and situational awareness for our cybersecurity defenses, and enable CISA to warn potential victims of ongoing attacks, so they know if they could be a target next.

This is an important first step, but there is much more Congress can do to ensure that critical networks in our healthcare and public health sector remain resilient against cyber-attacks.

I'm grateful our colleague, Senator Rosen, is leading efforts to that would improve the way CISA and the Department of Health and Human Services share information about cybersecurity threats with the healthcare sector, as well as provide cybersecurity training to medical professionals. I look forward to working together to build on these efforts.

Today, I am pleased to have an expert panel of healthcare cybersecurity professionals who can speak more about the challenges we face and discuss potential solutions.