Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Oversight and Investigations Chair Diana DeGette

Hearing on "Stopping Digital Thieves: The Growing Threat of Ransomware"

July 20, 2021

Good morning. It is good to see many of you in person, after being remote for so long.

Today's oversight hearing tackles a growing threat to our national security, economic security, and public safety, which is ransomware.

In short, a ransomware attack occurs when criminals break into a network, lock it down, steal data, and then extort everyday Americans into often massive ransom payments.

These digital thieves are infiltrating our schools, hospitals, food suppliers, and critical infrastructure companies.

The seriousness of the issue is hard to overstate. All you need to do is look at the front page of the newspaper to see that the problem is getting worse.

Earlier this year, the country watched as a single attack on Colonial Pipeline's information technology system shut down the gas and fuel supply to nearly the entire eastern seaboard.

This attack alone caused massive gas lines, hoarding, and many stations ran out of fuel.

Last year, more than 560 healthcare organizations—many of which were already reeling from the COVID-19 pandemic—found themselves victims of ransomware.

Hospital systems had to cancel appointments and surgeries, reroute ambulances, and delay critical treatment for cancer patients.

Our food supply was recently in the crosshairs, too. Just a few weeks ago, cyber criminals attacked the company JBS, the largest meat producer in the world, threatening a vital link in the nation's food supply.

And these are just the attacks we know about.

Companies and organizations wanting to save face and maintain the confidence of the public often meet the ransom demands in secret, almost always paying in hard-to-trace cryptocurrency.

Like many of the issues we have examined in the last year and a half—such as vaccine confidence and the state of our public health infrastructure—the ransomware challenge is not new, but it has been exacerbated by the COVID-19 crisis.

Cybercriminals thrive on exploiting vulnerabilities in our networks. The explosion of remote work and remote school during the COVID-19 pandemic greatly expanded those vulnerabilities.

For example, experts are projecting our K-12 schools will face a nearly 90 percent increase in the number of ransomware attacks just this year.

And it is not just the breadth of targets that is growing. The average size of ransom payments has also increased, reaching an estimated $312,000 per organization in 2020.

Simply put, the time to address this issue is now.

To win this fight, we need not just a whole-of-government approach, but a whole-of-society approach. Both the public and private sectors have important roles to play.

First, the public sector must continue to develop and lead a well-coordinated response.

This includes coordination across US government agencies and private industry and working closely with our international partners.

With President Biden's recent actions, we are seeing the outlines of such a response take shape, and the Administration is rightfully treating the issue as a national security threat.

For example, our nation's first National Cyber Director was sworn in just last week. And our federal agencies are conducting a series of collaborations with the private sector to address ransomware and other critical cyber issues.

I applaud the efforts that the Cybersecurity and Infrastructure Security Agency (CISA) announced last week. CISA is working to ensure that small-to-medium sized businesses across our country that are victimized by ransomware attacks have the resources needed to minimize harm and restart operations.

Internationally, it is imperative that countries no longer provide safe haven for these criminal organizations, and President Biden has vowed that America will take any necessary action to defend its people and its critical infrastructure.

In fact, we have already seen the President address the international part of this issue head-on, both at the G7 summit and in multiple one-on-one discussions with Russian President Vladimir Putin. And, just yesterday, the United States, along with our European Union and NATO allies, condemned China for its state-sponsored cyber activities, including ransomware attacks.

While the Administration's actions are promising, the public sector cannot defeat ransomware on its own.

For example, following a ransomware attack, we too often hear of lax cybersecurity requirements or known vulnerabilities that were ignored.

It is critical that private companies of all sizes address chronic underinvestment in cyber defenses. Better cyber hygiene, more cyber expertise, and meaningful information sharing will be necessary to address this threat.

And Congress has an important role to play in this. In fact, just last week, key government cyber experts indicated that additional executive authorities may be needed to ensure the private sector gets to where it needs to be.

As a Committee, we must ensure the executive branch has the tools and authorities it needs to mandate effective cybersecurity requirements for our vulnerable industries, modernize our defenses, and ensure we are postured to compete with these threats.

There is no shortage of policy proposals being discussed. These include mandatory reporting of ransomware attacks, prohibitions on ransom payments, and increased regulation of critical industries and cryptocurrencies.

This morning we have a terrific panel of experts who have spent decades addressing ransomware and other cybercrimes, and I look forward to hearing from our witnesses on these and other ideas.

One thing is certain: this problem is not going away.

The ransomware threat has grown exponentially over the last decade, and our response must grow in-kind. We must do everything we can as a nation to fix our vulnerabilities and protect our critical industries.

Thank you.