What Government and Business Can Do to Protect Against Ransomware and Cyberattacks

With ransomware attacks crippling businesses and critical infrastructure, cybersecurity is more important than ever.

Last Friday, the Chamber called on the U.S. government to act decisively against cyber threats to deter further attacks.

Our take: "Cybercriminals must be put on notice that attacks on our country and economy will not be tolerated," said Christopher Roberti, Chamber Senior Vice President for Cyber, Intelligence, and Supply Chain Security Policy. "The U.S. and allied governments must work together with the private sector to confront these challenges head on. It is time for our government to utilize its full range of capabilities – including criminal and cyber – to take the fight to these cyber gangs."

Why it matters: "Today thousands of businesses will be successfully attacked by criminal gangs using ransomware. The average downtime due to an attack is 21 days and on average it takes a business 287 days to fully recover," Roberti explained. "Enough is enough. Businesses are outnumbered and law enforcement doesn't have the resources to keep up."

Today, the Chamber in partnership with the South Carolina Chamber of Commerce and CyberSC, hosted the NOW + NEXT: Cyber Conference, where policymakers and experts examined the current landscape of cyber threats and provided advice for business owners.

Key takeaways:

- Cyber threats have increased tremendously with ransomware-as-a-service. “You don’t need technical skills. It’s really enabled scale,” Raj Samani, Chief Scientist for McAfee, said.

- “We’re seeing [ransomware] targets being more broad in scope,” said Nitin Natarajan, Deputy Director for the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA). “We’re seeing an impact in nontraditional targets: hospitals; schools; local governments.”

How to protect your business: During the pandemic small businesses have become bigger targets for cybercriminals. Kiersten Todt, Managing Director of the Cyber Readiness Institute, offered these tips at the event:

1. Make sure your systems have strong authentication like multifactor authentication.

2. “Have a patching program in your small business to ensure they’re installed when they’re available,” Todt advised.

3. Have a workable backup that can be accessed easily.

Dig deeper:

- Global Cyber Alliance Cybersecurity Toolkit for Small Business
- CISA’s Ransomware Guide
- U.S. Secret Service’s guide to Preparing for a Cyber Incident