Protecting Businesses from Cyberattacks

Last week, the U.S. Chamber hosted the latest installment of its Cyber Series—which included conversations to help businesses secure remote workspaces, deploy new telework infrastructure, and manage cyber risk in the current environment and beyond.

Why it matters. "Law enforcement officials have seen $26 billion in losses due to cyber fraud in the last three years. In addition, ransomware trends are exploding, along with payment card fraud, network intrusion, the use of virtual currency, and COVID-19 related fraud, according to him," said Mike D'Ambrosio, assistant director for investigations at the Secret Service.

"We have a vulnerable public looking for assistance. The adversaries know this and are looking to take advantage of the public in a time of crisis. We focus our efforts on complex, cyber-enabled fraud," he added.

What Members of Congress think. We need a National Cyber Director "who has a global perspective on not only the U.S. government, but also what is happening in the private sector space so that he or she can help to be traffic cop and coordinate things similar to what the Director of National Intelligence has done for the Intelligence Community," said Rep. Raja Krishnamoorthi (D-IL).

"The NIST Cybersecurity Framework is a great tool to build a plan to reduce and better manage cybersecurity risk. It is valuable to take a higher-level view of cybersecurity and will play a central role in our economy, our national security, and many other aspects of our society," said Rep. Mike Quigley (D-IL).

What businesses can do to protect themselves. After hearing from cybersecurity experts Doug Clare (Vice President, FICO). Ed Cabrera (Chief Cybersecurity Officer, Trend Micro), and Charles Carmakal (Senior Vice President and Strategic Services CTO, Mandiant), Chamber Senior Vice President Christopher Roberti closed the event with a call to action:

1. **Think like your adversaries, but don't act like them.**

2. **Follow the "good neighbor" rule.** In other words, try to make yourself a hard-enough target that the bad actors skip over you and knock on your good neighbor's door.

3. **Get to know your local law enforcement.** Get to know local law enforcement and officials from the FBI, Secret Service, and DHS's Cybersecurity and Infrastructure Security Agency (CISA), before a cyber incident; not during one. The Chamber can help get you in contact with these people if you need help.

4. **Backup, backup, backup!** Securely store data backups for your crown jewels either in the cloud or in secure offsite systems and test the recovery of these backups to ensure the minimal amount of business interruption in the event of a cyber incident.

ICYMI. Earlier this week, the Chamber published an update to its Assessment for Business Cyber Risk with a special focus on the role of cyber liability insurance.