In Cyberspace ...

COVID-19 has accelerated years of technological advancements into a few short months, and we know that digitalization will play a big role in our global economy moving forward. To support that growth, we must protect our critical systems, automate our processes, and upgrade our legacy networks to better prepare for the future.

U.S. Chamber Cyber Series

Last month, we held our third virtual Cyber Series event of the summer. These events promote cyber education and build relationships between the private sector and government cybersecurity and law enforcement agencies.

The event: During the event, I had the opportunity to have a discussion with Bill Evanina, director of the National Counterintelligence and Security Center. For several years, Director Evanina has worked closely with the Chamber on engaging the private sector in our nation's cybersecurity efforts.

The dialogue: We discussed everything from critical infrastructure to trade, public-private collaboration, threats from state actors, election security, and COVID-19. Watch the conversation and full event here.

- **The threat:** "The economic threat that we face from international actors and nation-state threats has grown to a level that's really unconscionable. We're looking at just over $500 billion a year in economic theft just from the country of China and just from the theft of intellectual property and trade secrets."—Director Evanina.

- **The good news:** "What we need is resiliency and redundancy. Whether you're a small company, a large company, or a town or local chamber," everyone plays a role, according to Director Evanina. He added that it doesn't cost much—no more than a pot of coffee—to have a better cross-organizational understanding of cyber risk.

Director of the National Counterintelligence and Security Center Bill Evanina provides a cybersecurity update at the Chamber's Cyber Series event.

Food for thought: Director Evanina posed the following questions and identified issues for business leaders to consider:

- What is the consequence of data loss? Does the board lose confidence in you? What about your shareholders? Your customers?

- What are the top three things your company does to manage that consequence? Are you having regular meetings with your CISO, general counsel, head of procurement, and human resources? Do you have a policy on how to protect things and are you exercising it?

- Who are the malicious actors that want your crown jewels?

- If you are a small company and don't have a lot of money, can you build partnerships with others to share CISO or CIO resources to advise on vulnerabilities and risk management?

- You need a whole-of-company approach to protect what you do, understand the risks, and have relationships with your employees, your customers, your competitors, your community, and the government.

Learn more:

Senior Vice President for Cyber Intelligence and Supply Chain Security Policy Christopher Roberti—CRoberti@USChamber.com or 202-463-5449