Cyber℠

PREPARE | PREVENT | MITIGATE | RESTORE

TRAVELERS INSTITUTE® | TRAVELERS

CAPITOL HILL
WASHINGTON, D.C.

L to R: Tim Francis, Travelers; Siobhan Gorman, Brunswick Group; Brett Leatherman, Federal Bureau of Investigation; Joan Woodward, Travelers Institute; Ben Edson, VariQ; and John Mullen, Mullen Coughlin LLC

Federal Bureau of Investigation headlines *Travelers Institute*® cybersecurity symposium on Capitol Hill

The Travelers Institute brought its national cybersecurity symposium series to the nation's capital on June 17, 2016, to teach business owners and organizational leaders about evolving cyber threats and strategies for protecting systems and sensitive data.

More than 200 people attended the *Cyber: Prepare, Prevent, Mitigate, Restore*℠ symposium, which was held in collaboration with the Small Business & Entrepreneurship Council, Women Impacting Public Policy, the National Association of Women Business Owners' Greater DC Chapter, and the Small and Emerging Contractors Advisory Forum.

Cyber threats

Keynote speaker **Brett Leatherman**, Assistant Section Chief, Cyber Division, Federal Bureau of Investigation, described various cyber threats and the intent behind each scam. He explained that there are "hactivists" who target organizations for political or social causes to address an injustice, adding that these criminals typically are less harmful than other cyber scam artists. In contrast, Leatherman said, cyber "actors" who want to "monetize data" target organizations to exploit information for money. In yet another scam, a ransomware attack, a cyber criminal accesses a company's system and holds data for ransom.

Threat detection

Organizations spend millions of dollars on preventive technology. While Leatherman acknowledged the importance of being prepared, he also stressed that prevention alone is not sufficient, especially for small to medium-sized businesses. "You can never 100 percent protect your environment from being compromised by a sophisticated adversary."

He advised organizations to focus additional attention on detection capabilities. He said businesses need to be aware of what is happening within their environments, and they should look for adversaries with the mindset that their systems are already compromised. The ability to detect adversaries before they move laterally can be tremendously valuable, explained Leatherman.

"As an organization, you are responsible for preparing your environment," Leatherman said. "If you are not prepared when your data gets encrypted by a threat actor, you are not going to recover that data."

The symposium also featured a panel discussion moderated by **Joan Woodward**, President of the Travelers Institute and Executive Vice President of Public Policy at Travelers, focusing on how organizations can address cyber risk.

L to R (back row): Leatherman; Mullen; Thomas Gresham, Regional Vice President, Bond & Specialty Insurance, Travelers; Sarah Novascone, Government Relations, Travelers; Gorman; (front row): Karen Kerrigan, President and CEO, Small Business & Entrepreneurship Council; Woodward; Francis; Edson

Leatherman gives the keynote address.

Employees

"Employees have a critical role to play when it comes to cybersecurity," said **Siobhan Gorman**, Director, Brunswick Group. Cybersecurity is a "human problem," in that hackers are human and they are using other humans in organizations they are trying to infiltrate, she said. Gorman explained that phishing attacks use emails that are laced with malware to access an organization's system. She advises employees to think carefully about emails that seem "a little off," and to have someone in the IT department take a look at an email if they are unsure about it. Educational programs are critical in helping employees understand the role they play in cybersecurity, Gorman said.

The panel agreed that companies should stress the importance of good cyber hygiene on the part of every user, from the top down. They should focus on educating everyone, including executives and board members, as well as on adopting technologies to minimize the threat.

Vendors

Ben Edson, Founder and CEO, VariQ, defined vendors as the "partners that we deal with to get things done." He stressed the need to secure the supply chain to help ensure that not only your company's vendors, but also your vendors' suppliers have sound cyber practices within their organizations.

Prepare, Prevent, Mitigate, Restore

During audience polling, 65 percent of attendees said their company has a plan in place to respond to a cybersecurity incident, but only 15 percent said their company has exercised or tested it. Additionally, 57 percent of attendees said they did not know what actions to take in the event of a data breach. The panelists advised business owners to develop and test a cybersecurity plan to help prevent and respond to cyber incidents.

When a cyber crime occurs, **Tim Francis**, Vice President and Enterprise Cyber Lead, Travelers, told business owners and organizational leaders to consult with law enforcement and legal counsel.

"Every [hacking] situation is unique, which is why you need access to this counsel to make the right decision for your situation," he said.

The panel provided other recommendations as well:

- Develop a cyber communications plan to help everyone understand what role they will play if an incident occurred.
- Identify vendors who have access to your business's network and devices.
- Prepare in advance for media exposure relating to your company's handling of a cyber crisis, and decide how information will be disseminated to customers and key stakeholders.
- Work with your insurance agent or broker to help prevent and respond to a cyber incident.

Learn more: travelersinstitute.org/cyber
Contact: institute@travelers.com

TRAVELERS INSTITUTE® | TRAVELERS

travelersinstitute.org

The Travelers Institute, 700 13th Street NW, Suite 1180, Washington, DC 20005