Cyber℠

PREPARE | PREVENT | MITIGATE | RESTORE

TRAVELERS INSTITUTE® | TRAVELERS

LOS ANGELES, CALIFORNIA

L to R: Bill Detwiler, TechRepublic; Dianne Ewing, Hoffman Brown Company; Tim Francis, Travelers; Joan Woodward, Travelers Institute; Michael Echols, U.S. Department of Homeland Security; and Sian Schafle, Mullen Coughlin LLC

Travelers Institute launches cybersecurity education initiative for small and midsized organizations

Nearly 200 business owners gathered in Los Angeles on April 27, 2016, as the Travelers Institute launched its national cybersecurity symposium series *Cyber: Prepare, Prevent, Mitigate, Restore℠,* designed to teach organizations how to better protect their systems and sensitive data. The event, co-hosted by Hoffman Brown Company, the U.S. Small Business Administration Los Angeles District Office and CNET, kicked off a national education series convening industry leaders from the public and private sectors to discuss cyber risks and best practices for safeguarding computer systems and sensitive information.

Small and midsized businesses

"More than 60 percent of cyber attacks were against small and midsized businesses last year, while data breaches increased 23 percent in 2015," said **Joan Woodward**, President of the Travelers Institute and Executive Vice President of Public Policy at Travelers, citing Symantec statistics. "Experts agree that education is critical."

Keynote speaker, **Michael Echols**, Director, Joint Program Management Office, Office of Cybersecurity and Communications, U.S. Department of Homeland Security, said that smaller companies, which often serve as suppliers to critical infrastructures, are more vulnerable to hackers.

"They [small companies] are the easy way in. They do not use the best practices and they do not have the money or resources," said Echols, adding that many small business owners do not realize that a cyber breach can damage their reputation and cause them to lose their business.

Threat landscape

During a panel discussion, Echols joined other cyber professionals in describing some of the current threats within the cyber environment.

Employees

The participants stressed the need to educate and train employees on cyber-smart practices in the workplace. **Bill Detwiler**, Managing Editor, TechRepublic, cited examples, such as creating strong passwords and not plugging in USB devices or opening questionable emails and attachments.

"People have always been, and continue to be, the weak link" in many security breaches, said Detwiler. The use of encryption and other technology can help mitigate cyber risks, but "it only takes one or two people to create a hole that lets the attacker into the rest of the organization," he cautioned.

Vendors

"In other cyber events, vendors or business partners are the conduit to the breach," said **Tim Francis**, Enterprise Lead for Cyber Insurance, Travelers. In many of those incidents, the vendor or business partner is a small or midsized business, and the ramifications for that business can be significant.

"You are very quickly going to cease to be the client of that large business, regardless of what you do to fix it," warned Francis, who urged vendors to be mindful of their security policies, procedures and controls.

Steve Brown, Chief Executive Officer of Hoffman Brown Company (left), with Thomas McCormack, Regional President of Travelers

Michael Echols of the U.S. Department of Homeland Security gives the keynote address.

Ransomware

According to Symantec, ransomware attacks increased 113 percent last year. Echols explained that cyber criminals who use ransomware often target businesses and organizations that cannot function without their data, because these entities are more likely to pay the ransom. He cautioned that many systems have malware code running through them, even if the malware has never been activated.

Social engineering

Francis told the audience that he has seen a noticeable increase in social engineering fraud, in which people are manipulated into giving up confidential information or paying for a product or service that the company did not order.

"The bad guys are getting better at fooling companies into thinking that they represent either a senior official at the organization or a vendor," explained Francis. "What you do not realize is that the payment has just gone to an overseas bank, rather than to the customer you usually send that payment to."

Hacktivists

Hacktivists are those who use computers or computer networks to push a political agenda. **Sian Schafle**, Partner, Mullen Coughlin LLC, said hacktivists will threaten to hold a business ransom or threaten to penetrate the system if the company doesn't comply with their demands.

Denial of service

Malicious attacks that interrupt a company's website or computer network, preventing access, are known as denial of service. Similar to hacktivism, the culprits will maintain control of the system until the company pays a ransom, but the cost to recover is greater than just the ransom.

"The monetary cost is not just paying the ransom, it is also recovering your business's reputation," said Woodward.

Dianne Ewing, Vice President, Marketing and Business Development, Hoffman Brown Company, said insurance products are available to help companies recover from a cyber event, but many business owners are reluctant to buy insurance because they think they will not be victimized by cyber criminals.

Prepare, Prevent, Mitigate, Restore

During live audience polling, 53 percent of attendees said their company had a cyber response plan, while the remaining either did not have a plan or did not know. The panelists agreed that companies of all sizes should have a plan in place to prepare for and respond to a cyber incident.

Other recommendations included:

- Run through or test the company's cyber response plan.
- Adopt a cyber-safe culture, using an interactive process with employees that takes place throughout the year.
- Consider cyber insurance coverage to help the business recover from an incident.

Additionally, Schafle recommended that businesses hire breach coaches who understand cyber trends and laws, which differ from state to state. Breach coaches can identify cyber risks, develop a cyber response plan and help businesses that experience a cyber event.

Audience members were encouraged to visit the websites below for more information on cyber risks and tools for developing a cyber response plan:

- Travelers – travelers.com/cyber
- U.S. Department of Homeland Security – us-cert.gov
- NIST Cybersecurity Framework – nist.gov/cyberframework

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