Cyber℠

PREPARE | PREVENT | MITIGATE | RESTORE

TRAVELERS INSTITUTE® | TRAVELERS

HOUSTON, TEXAS

L to R: Joan Woodward, Travelers Institute; Edward Schreiber, BancorpSouth/GEM Insurance Services, Inc.; and Chris Hauser, Travelers

Federal Reserve Bank of Dallas Houston Branch leader headlines cybersecurity symposium examining secure payment technologies

The Travelers Institute convened cybersecurity professionals in Houston, Texas, for its *Cyber: Prepare, Prevent, Mitigate, Restore*℠ symposium series, which is held around the country to educate businesses and organizations on how to help keep their systems and data secure. More than 150 owners of small and midsized businesses attended the May 11, 2016, symposium, the second event since the series was launched in April of 2016.

"Cybersecurity is the fastest-growing concern among business owners," said **Joan Woodward**, President of the Travelers Institute and Executive Vice President of Public Policy at Travelers.

The cyber threat landscape

Social engineering

During his keynote address, **Jason Ritchie**, Assistant Vice President, Bank Administration, Federal Reserve Bank of Dallas Houston Branch, talked about the various cyber scams targeting businesses. Business email compromise (BEC) is a new method for committing wire transfer fraud.

"Someone – a hacker, a criminal – is posing as a very important person in the organization and has somehow either hacked that person's email or is spoofing that email and sending urgent emails to someone who might be able to send wire transfers," explained Ritchie, who added that there was $750 million in fraudulent BEC-related transfers during the last couple of years.

Edward Schreiber, Houston Region President, BancorpSouth/ GEM Insurance Services, Inc., said companies can lose money and sensitive data in spoofing scams. He stressed the need to take precautions.

"If you do nothing else, make sure that anyone in your organization who is in charge of sending money electronically does a verbal confirmation of any email" that gives different bank or address routing details, "because once the money is gone, it is gone," said Schreiber.

Credit card fraud

Ritchie said the biggest scam, credit card fraud, hits the U.S. more than other regions of the world and cost the nation $8 billion in 2015.

He said many people are victimized when they make a purchase using a card reader because criminals put skimmers on the machines, providing access to credit card numbers. Ritchie said the Europay, MasterCard and Visa (EMV) chip cards will help reduce credit card fraud, but the U.S. is lagging behind other countries in the use of EMV technology.

Ritchie said mobile wallets are a good option for making credit card purchases, because people can buy items right from their smartphones or an EMV terminal without presenting their credit card to a merchant.

Dot-bank domain

Ritchie also talked about the dot-bank (.bank) domain, toward which many banks are transitioning. He said the dot-bank domain has stricter technology requirements and is more secure than the dot-com domain.

"Anyone in the world can create a dot-com," said Ritchie. "Dot-bank requires banks to have a charter, so not just anyone can get a dot-bank domain."

He said dot-bank domains will help prevent scam artists from setting up fraudulent banks online.

David Lavergne, Regional President of Travelers

Jason Ritchie, Federal Reserve Bank of Dallas Houston Branch

Employees

During a panel discussion, the cyber professionals talked about additional risks for businesses and organizations, including employees.

"Employees are our greatest asset, but the untrained employee is really the biggest liability in any organization," cautioned **Peter Thomas**, Chief Technology Officer, Blue Lance.

Ransomware

Cyber criminals are using advanced cryptography to carry out ransomware attacks, in which computer systems are hacked and held for ransom.

"The reality is that it is a vastly evolving threat that has many faces," described **Chris Hauser**, 2nd Vice President, Risk Control, Cyber Program, Travelers. He urged business owners to have adequate backups to recover stolen data.

Hacktivists

Hacktivists are cyber criminals who push their agendas by threatening to expose a company's sensitive data unless the company changes a certain business practice.

"It puts a sense of urgency on these businesses to make a tough decision with their data exposed. It can be a very alarming matter for many organizations," said Hauser.

Denial of service

Denial of service is a scam in which a hacker takes control of a company's web server or other externally facing service and prevents access until a ransom is paid.

Prepare and prevent

Nearly 40 percent of attendees indicated that their company did not have a plan in place to respond to a cyber incident. Hauser advised businesses that store sensitive data to develop such a plan to help protect against theft.

"In cyber, it is all about the data. Organizations need to be concerned about the customer information that they collect," said Hauser. "Many organizations could not function in today's modern business environment without their email systems, without the ways that they communicate among each other."

Panelists shared guidance for creating a cybersecurity plan:

- Ensure that management is involved in developing the plan.
- Appoint a dedicated cybersecurity professional to establish controls and monitor the system for breaches.
- Vet vendors to determine whether they have sound cyber controls and practices in place.
- Talk to your insurance agent about cybersecurity insurance options.
- Develop strategic relationships with law enforcement, such as the FBI, to share information about current cyber threats and to report a cyber incident.
- Train employees on safe use of computers.

Mitigate and restore

"One of the most common ways a business finds out they have been breached is someone tells you," said Hauser. A bank, a merchant processor or law enforcement may contact the business saying they observed suspicious activity, and this should begin to enact a business response plan. The panelists advised business owners to immediately investigate to determine what occurred and whether their cyber response plan needs to be enacted. A business should report the incident to law enforcement and contact their insurance agent if they have cyber insurance.

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