Conquering Cyber-Readiness in Credit

When someone breaks into a house, the homeowner is likely to take preventative measures to improve security, whether it's installing heavy-duty locks, alarms or cameras. The same can be said for financial institutions (FIs) when cybercriminals breach a company's network and steal or leak confidential information. The latest and greatest cybersecurity programs aren't necessarily a company's most valuable asset, but rather, it's their knowledge and understanding that will better protect them in the long run.

Last year, data analytics company FICO Decisions collaborated with independent research company Ovum to survey security and IT employees across five industries in the U.S. and other countries, including financial services, health care, power and utilities, retail and eCommerce and telecommunications. A startling revelation came from the financial services, retail and eCommerce industries, where 80% of respondents in the U.S.—63% around the world—believe cyberthreats and data breaches will rise over the next year. Few U.S. respondents in financial services (20%) and retail and eCommerce (15%) said levels will stay the same, the remaining 5% of retail and eCommerce respondents anticipate a decline.

What surprised analysts was how the number of cyberattacks actually declined in the prior year in the U.S. In 2016, 61% of respondents said there was an increase in cyberattacks, yet only 33% said the same in 2017. However, this good news doesn't account for companies' current level of preparedness—only 31% of companies say they understand the risks at hand.

"While U.S. organizations are realistic about overall levels of risk and expect it to increase, they are not so realistic about their own cyber-readiness," the study states. "With attacks expected to increase in volume, breach risk is more important than ever before. Organizations must take the opportunity to objectively understand their likelihood of suffering a breach so they can take the necessary steps to transfer or mitigate risk."

Too few U.S. companies (28%) never update their risk assessment procedures, with 3% conducting no assessments whatsoever. The survey indicates that companies are "overly optimistic" regarding cyber-readiness.

In addition to employee training, some companies are engaging another preventative practice known as penetration testing, which involves third-party testers attempting to expose cyber vulnerabilities in companies through test hacks. During a 10-month period that ended in June, cybersecurity software firm Rapid7 conducted simulated cyberattacks on nearly 270 corporations for its *Under the Hoodie 2018* report. The tests concluded that the finance sector, for example, was more defensive against external threats, like websites and phishing, as opposed to internal threats, like connections and WiFi. About 61% of the tests resulted in no threat detection on behalf of the company.

"These results imply that if the penetration tester is not detected within a day, it's unlikely the malicious activity will be detected at all," Rapid7 analysts said in the report.

At Wagner Equipment Co. in Albuquerque, NM, Customer Account Representative Roberta Ortiz-Montoya said the company's IT department stays on top of any potential cyberthreats.

“We here in the credit department get emails from the IT department when there is a scam of some sort,” said Ortiz-Montoya, a member of the Albuquerque CFDD Chapter. “[We’re told] not to open any emails [when] we don’t know where they are coming from.”

CFDD Louisville Chapter Member and Western Regional Credit Manager Lynn Kendrick, CBA, of Whayne Supply & Walker Machinery, said not only do they refrain from opening sketchy emails, but they are also in the process of implementing a three-digit verification code on credit cards.

Managing employee credentials, such as implementing administrative credentials to complete specific actions, and encouraging a “see something, say something” policy can help mitigate cyberthreats, Rapid7 noted. Time-driven account locks and two-factor authentications aren’t as bulletproof on their own, but these strategies can be effective when utilized with other precautions.

—Andrew Michaels, editorial associate