Cyber Security Awareness Training is A Must in 2020

The events of 2020 are bringing former concerns to light as businesses shift the way they conduct operations. The 2020 Travelers Risk Index revealed broad economic uncertainty as the top concern among businesses this year, despite a No. 6 ranking in 2019, which many have attributed to the COVID-19 pandemic that hit the U.S. eight months ago. Nearly 50% of respondents noted the business environment is becoming riskier, specifically citing concerns of cyber risks, which ranked No. 2.

Cyber Training Components

Cyber risks come in many forms, but the Travelers Risk Index deemed security breaches, hackers accessing financial systems and employees putting information at risk as the latest business woes. Working remotely has fueled these concerns as businesses with at least 40% of remote employees has more than doubled. However, where there are problems, there are also solutions, beginning with businesses conducting in-house cyber security awareness training.

Companies can break training down into several components, Travelers reports, most notably, document management and notification procedures, passwords and email use.

“Employees should be educated on your data incident reporting procedure in the event an employee's computer becomes infected by a virus or is operating outside its norm (e.g., unexplained errors, running slowly, changes in desktop configurations, etc.),” Travelers states. “They should be trained to recognize a legitimate warning message or alert. In such cases, employees should immediately report the incident so your IT team can be engaged to mitigate and investigate the threat.”

Strong passwords are a great protector from cyber threats, yet what were once thought to be secure passwords are no longer suitable. According to Norton Security, personal information, such as a name, address, phone number or birthday, is often public knowledge and, therefore, easy for hackers to access. So, rather than use this information and/or real words, Norton emphasizes using special characters—asterisks, exclamation points, dollar signs, ampersands, etc.—in addition to creating passwords with a minimum of 10 characters.

Password creators must also avoid writing them down and, instead, create a passphrase to remember them. Norton’s example involved taking a lyric from a song and substituting some of the letters with numbers that look similar. For example, using the lyric, “Don’t stop believin’” by Journey, a usable passphrase could be “D0n*T st0P BeliEvIN*.”

“Change passwords on a regular basis. Passwords for your online financial accounts should be changed every month or two,” Norton states. “Computer login passwords should be changed at least once a quarter. Using the same password for longer periods could put your information at risk if a data breach occurs.”

Emails are another hotspot for attracting cybercriminals, Travelers added, therefore, businesses must educate employees on when to accept an email. Did the email come from someone they know? Have they received an email from this individual before? Were they expecting the email? If the answer to these questions is, “Yes,” then the email is likely safe.

October’s OFAC Advisory

For the credit professional, cyber-related issues that are of utmost concern are those that will impact businesses' payment systems. This recently garnered the attention of the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) when they issued an advisory in October regarding the facilitation of ransomware payments. OFAC notified businesses of perpetrators threatening to release victims' confidential information if their demand for payment is not met.

"OFAC has imposed, and will continue to impose, sanctions on these actors and others who materially assist, sponsor, or provide financial, material, or technological support for these activities," the report states, and will continue to abide by regulations currently in place to prohibit ransomware payment facilitation. This includes the International Emergency Economic Powers Act (IEEPA) and the Trading with the Enemy Act (TWEA), and enforcement under its Economic Sanctions Enforcement Guidelines that state U.S. persons cannot engage "in transactions, directly or indirectly, with individuals or entities (persons) on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons…"

"With more employees relying on their ability to connect with company systems from remote locations, and many consumers preferring online transactions in an age of social distancing, it's more important than ever for companies to do all they can to mitigate exposure to cyber threats," Tim Francis, Enterprise Cyber Lead at Travelers, said in a press release. "Taking appropriate precautions and having a plan in place should something go wrong will put an organization in position to seamlessly get back up and running. This is critical in ensuring that employees will be able to continue to access systems and maintain productivity, while also delivering a high level of service to customers."

—Andrew Michaels, editorial associate