Peter Schablik is a partner at WeiserMazars LLP.

Scott M. Higgins is a director at WeiserMazars LLP.

CYBERSECURITY

Empower Your People to Protect the Bank

Cyberattacks aren't just getting more frequent, they are also becoming significantly more vicious and sophisticated. The majority of today's data breaches result from human error, making cybersecurity a "people problem" as well as a technology issue. The solution to this people problem can't be solved by purchasing new hardware or software or implementing sophisticated network testing. It involves cultivating an entirely new employee mindset around cybersecurity that is based on continually raising awareness and putting secure actions and decisions at the forefront of the company culture.

Cyberbreaches can result in dramatic and immediate financial repercussions. Some of the costs are direct and are incurred when banks remediate the damage done. Beyond those direct expenses, however, lies more serious damage. The indirect costs of a data breach are far-reaching and can continue long after the immediate damage is repaired. Once customers, vendors and partners learn of a data breach, the institution's reputation is tarnished. The company name and brand become associated with risk to sensitive information, to finances and to security.

IBM's 2015 Cyber Security Intelligence Index revealed that 95 percent of cyber breaches occur as a result of human error. According to the research, the average number of security events detected dropped to 81 million in 2014 from nearly 92 million in 2013, but the number of incidents remained constant. (A security event is a change in the everyday operations of a network or information technology service, indicating that a security policy may have been violated or a security safeguard may have failed. A security incident is a warning that there may be a threat to information or computer security.) While the attempts were lower by 12 percent, the number of successful breaches remained the same. Even though IT detection efforts are improving, so are the criminals. This makes the human element in cybersecurity even more critical, and adds urgency to finding more effective methods to address it.

The average employee typically doesn't recognize the role they have in cybersecurity defenses or the consequences of their actions. Fortunately, the significant risks that clicking, tapping and browsing employees represent can be effectively mitigated with a carefully delivered cybersecurity campaign that includes three key elements.

Make People Care

Any effective cybersecurity program must start with this human element—get employees invested in the subject and help them become more receptive to the learning or awareness activities that follow.

Build Awareness and Knowledge

Once people care, a successful awareness campaign can be built that alerts employees to key risks and enables them to make the right decisions when going online, using devices or handling company information. Companies must continually create awareness among employees at all levels.

Employees must be equipped with strategies, rules and basic knowledge about cyberrisks and how to mitigate them. Training and awareness are not the same (although the two can work hand in hand), and each creates a different level of protection. An awareness program should integrate a deep, instinctive layer of knowledge into the automatic actions employees take.

Creating and deploying a best practice cybersecurity program is just the first step. Programs need to be carefully reviewed and measured systematically over time—to identify, implement and test possible improvements that might make the program even more effective.

Assessing a Company's Approach

To assess the effectiveness of a company's approach, it's important to measure employee awareness, attitudes, knowledge and motivation regarding the cybersecurity materials, policies, and training they have provided.

Carefully crafted survey questions can assist in establishing current employee knowledge and awareness levels in relation to company-provided cybersecurity information and policies.

Used effectively, the three key elements can cultivate a culture of cyber awareness where employees recognize and avoid risky situations and take instinctive action.

When employees are properly prepared, they will not view cyberattacks as technology-based threats. Instead, they will be motivated to safeguard company systems and information, recognizing that they play an important role in keeping data and systems safe and secure.

WeiserMazars

ACCOUNTING | TAX | ADVISORY

As seen in the 4th Quarter 2016 issue of *Bank Director*