Back to Basics: How Employee Training Can Be the Most Cost-Effective Way to Eliminate Security Threats

BY ELAINA M. MARAGAKIS, RAY QUINNEY NEBEKER

CYBERSECURITY CAN BE A substantial investment, but one of the most effective means of preventing a data breach can also be the most cost-effective: employee security awareness training. According to the Verizon 2018 Data Breach Investigation Report, "[h]ealthcare is the only industry where the threat from inside is greater than that from the outside," and human

Employee training should be manageable and ongoing. Employee training should be regularly conducted and mandatory for all persons who use the company's computer systems. Scams are becoming more sophisticated, so training must be nimble to adjust for new trends in threats. Providing short training sessions more frequently helps keep security issues at the forefront of employees' consciousness.

error is the major contributor to those threats.[1] With these risks in mind, one of the most overlooked—but critically important—first steps to lessening security risks is simply to train employees.

Set an expectation of privacy. Security awareness should be a core value of the organization, and that means leading by example. The top levels of management must reinforce the importance of data security, and then incorporate best practices into their own routines. Communicating the importance of data security across the organization helps create a culture of privacy.

Employee training should cover all employees, and everyone who utilizes a company's system. Security awareness must be an enterprise-wide endeavor to be effective, so it is important that everyone receive consistent training and understand their respective obligations. Everyone who uses a company's computer system is susceptible to clicking on bad links or opening malware attachments, so it is critical that all employees be uniformly trained on how to spot suspicious emails. And don't forget internal threats—employees should only be able to access materials that are related to the performance of their job functions. If an employee is accessing information out of "curiosity," that is a major security risk to the organization.

Employee training should be manageable and ongoing. Employee training should be regularly conducted and mandatory for all persons who use the company's computer systems. Scams are becoming more sophisticated, so training must be nimble to adjust for new trends in threats. Providing short training sessions more frequently helps keep security issues at the forefront of employees' consciousness. And don't forget new employees—create a way to introduce security awareness training when you are onboarding a new employee to shore up their security awareness until the next regularly scheduled training. Training should be conducted by someone with experience in data security, but should not be too technical. Much of data security training centers on using common sense and training employees to slow down and think before taking action.

Concentrate on phishing training. One of the most vulnerable points of entry in an organization is simply clicking on a link in a phishing email. With phishing attempts on the rise, a primer on how to look for emails that might be malicious will go a long way in protecting a company's system. A healthy level of skepticism should become part of every employee's makeup.

Make training comprehensive. Remember that security awareness extends beyond cybersecurity. Hard copy documents contain sensitive information and must be protected with the same rigor as electronic documents. Additionally, be sure to canvass physical security within the organization. For example, who has physical access to areas where sensitive information is stored? Are visitors to the organization required to sign in and be escorted while in the building? Are security barriers like access cards kept up to date?

Run internal tests. Consider running phishing tests internally to help identify problem areas and potential vulnerabilities, and use the results as a training tool. And, if employees are aware of the possibility that an email may be part of a test, their motivation to scrutinize potential emails scams will be heightened. It is also important to make sure

BACK TO BASICS | *continued on page 20*

BACK TO BASICS | *continued from page 19*

that good security behavior, such as locking computer terminals when they are unattended, is rewarded.

Listen. Listening to the concerns of employees can help improve internal systems and open a window into security weaknesses. Often, employees are aware of security problems that management has not observed.

Taking the first step of implementing a security awareness training program can be one of the most inexpensive ways to ensure that your systems are protected from human error. ■

Elaina Maragakis is a shareholder and director at Ray Quinney & Nebeker and practices in the Firm's Litigation Section. Her practice focuses on complex commercial litigation. She has tried a significant number of cases and has experience managing complex disputes through trial. Ms. Maragakis has represented numerous companies in connection with contract and business disputes, including class actions. Ms. Maragakis has also represented a number of health care entities, including nursing homes and hospitals, in HIPAA analysis litigation and medical staffing issues. Ms. Maragakis is the Chair of the Firm's Cybersecurity and Privacy practice group. She has obtained her designation as a Certified Information Privacy Professional/US (CIPP/US), a certification from the International Association of Privacy Professionals. She assists clients in all aspects of legal compliance with data security laws, including helping companies minimize their risks by preparing Information Security Policies, including Data Breach Response Plans and Employee Data Security Policies. In the event of a breach, she assists with managing a company's compliance with breach notification laws. She has given presentations to various groups on the issue of data security across the state of Utah, and has written extensively on the subject.

[1]Available at https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf