From the Sponsor EXECUTIVE FORUM CYBER SECURITY

What you don't know CAN hurt you

A recent (March 2017) report from the Pew Research Center reflects alarming statistics for businesses with respect to employee awareness of cybersecurity issues. The survey consisted of 13 questions designed to test Americans' knowledge of a number of cybersecurity issues and terms, and found that a substantial majority of adults surveyed were only able to correctly answer two of the questions. While a 15% correct response rate may not bode well for individual internet usage for personal activities, it poses an even bigger threat to businesses when these same people bring their habits and lack of understanding into the workplace.

Many businesses have unique or complex transaction systems or are subject to specific requirements or legislation that far exceeds the typical technology risks which an individual might encounter in their personal life, with the potential for a single lapse to cause much greater problems. For a business to have any hope of an effective cybersecurity policy, it must take steps to ensure that its employees, volunteers and vendors understand the cyber threats the business faces and the various controls it has in place to protect against them. They must also understand the greater business risks that their actions (or inactions) might cause. It is not enough to assume that employees and others understand the risks and act accordingly. Here are five things every business must do to help turn its employees, volunteers and vendors from "weak links" into "cyber defenders."

William M. Prohn
Managing Director,
Dopkins Systems Consultants;
Director of Information Technology,
Dopkins & Company, LLP

Have clear, written policies which layout and explain what employees must do and cannot do in order to keep the business, its information and that of its customers and employees safe. These policies may vary widely between businesses based on their markets, procedures and information gathering needs. It is not reasonable to expect employees to know this without being told.

Take the time to "classify" information used by the business. It's not all the same. For example, customer account numbers and patient records should not be treated as loosely as the lunch menu. Information should be grouped into "public", "internal use only", "confidential", etc. with examples to help employees understand the differences and the behaviors and controls that each one requires. Employees are better equipped to understand the need for controls when the information (and the threat) is specific. "Never share social security numbers" is a much clearer directive than "beware of suspicious emails."

Have an education and awareness program to regularly reinforce the need for cybersecurity and to introduce new threats and behaviors as they become necessary. Posters, email reminders and short videos sent regularly can all help drive the message home. Prepared programs are available from vendors like SANS and KnowBe4. Cybersecurity can be complex and addressing the issues from multiple perspectives and in various ways can help employees internalize the importance of their actions.

Test your users. Like anything new that has to be learned, cybersecurity behaviors need to be reinforced through testing and feedback. A report from 2016 stated that more than 90% of cyberattacks and resulting data breaches start with a spear phishing campaign. Emails with attachments or web links that appear to be something they're not can be hard to detect. By sending phishing email tests, employees get practice and feedback to help identify the phishing threat, and businesses get valuable intelligence on how their employees are behaving and whether their message is getting through.

Use technology to block activities that don't have a valid business purpose. Utilization of the company's technology is a privilege, not a right. Today's firewall technology offers multiple levels of sophisticated protections and monitoring of information coming into and going out of an organization. Best practices include blocking access to personal email accounts from office computers as well as blocking incoming traffic from countries where your organization does not have any customers or suppliers. Don't allow use of personal devices such as phones, tablets or laptops for business activities. Prevent employees from using "cloud" services (such as DropBox or Amazon Web Services) that are not authorized. These are activities which an individual may use in their personal life, and see no threat, but which pose unnecessary risk to a business and certainly increase the cost of monitoring and controlling cyber threats.

October is National Cybersecurity Awareness Month, and there is simply no better time to initiate a new program to boost employee awareness, and ultimately protect your organization.