From the Sponsor EXECUTIVE FORUM CYBER SECURITY

Dotting the "I"s and Crossing the "T"s

Cyber security is generally defined as protecting against the risks posed by the use of the Internet: the global interaction of computer networks and anonymous users, characterized by hackers, breaches and ransomware. However, the risks are often closer to home, as are the most effective protections: in the "IT" or information technology systems and controls used every day in every business. While it is crucial for every business to have an Incident Response Plan in place to guide its activities when a breach or hack inevitably happens, and to regularly assess IT risks in a formal Risk Assessment exercise so that security efforts will be directed where they do the most good, there are any number of smaller daily activities that can effectively reduce risks from technology use and protect valuable information. Taking the time to "dot the I's and cross the T's" of information technology is something every business can and should do immediately to improve its cyber security posture.

One of the obstacles to effective cyber security is that many users don't understand what it means, or think it doesn't apply to them. It's understood as a concern, just not for them. One way to make progress is to revisit many of the IT controls and safeguards that have been widely practiced for years, and are accepted by many as "best practices." This has three advantages. By digging in to an existing security practice, and asking "why?" and "what if?" that practice can be revised and improved in light of current business needs and threats. By formulating the risk discussion around a process that everyone already accepts, the risks and threats are better understood. Engaging users and decision makers in a discussion around an important practice can be a valuable learning experience in the meaning and relevance of cyber security.

William M. Prohn
Managing Director,
Dopkins Systems Consultants;
Director of Information Technology,
Dopkins & Company, LLP
Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

A good example is data backup. Most people agree that having a backup is a "best practice" and many have personal experience with its saving power. Engaging senior leadership (or board members) in a (relatively short) conversation around backup can be a valuable introduction to cyber risks and controls. What is the purpose of the backup: archival, error correction, disaster recovery? What data is getting backed up? How frequently? How long will it take to restore? Can we live with that? Where does the backup get stored: On-site/Off-site, On-line/Off-line, Cloud? What does the backup protect (i.e., it doesn't protect against a data breach)? Is the backup data itself vulnerable (concerns about third party access and theft of the disk or tape)? Should there be different backups for different types of data? A meaningful discussion of this type can take less than an hour, and initiate a badly needed dialog between IT and business leaders, where each re-discovers their dependence on the other and recognize that risks and controls are not so foreign after all.

Another example is passwords. Everyone "gets" the need for passwords, yet the need is often very poorly satisfied. A dialog with users on the need for passwords as critical for security, problems people have with creating, remembering or storing dozens of complex passwords, and ways to overcome these obstacles can be an important first step toward better cyber security. Everyone has an opinion on and experience with passwords. That common understanding can lead to buy-in and improvements in other areas of cyber security. Are application passwords as important as network passwords? What if the same strong password is used for everything? Maybe it's not a password problem at all. Maybe certain users shouldn't have access to certain data.

These efforts won't guarantee you won't get ransomware or suffer a data breach, but they can help overcome the two biggest obstacles to security: ignorance and apathy. If you're looking for a way to start, getting users engaged on a topic they understand can be a breakthrough.

An IT Audit is a good way to see if all those I's are dotted and the T's crossed. Are the little things that IT does actually getting done, and do they work? Are user accounts shut off when employees leave? Do the backups actually work? Are there exceptions to password requirements? Is anti-virus updated regularly?

Cyber security is more of a lifestyle change than a product that can be purchased. Lifestyle changes are about doing lots of little things consistently. It's about dotting the I's and crossing the T's.