THE STANDARD
NEW ENGLAND'S INSURANCE NEWSMAGAZINE
Published Since 1865 Boston, Mass. September 22, 2017 Vol. 281 No. 6

Data Security: A Homegrown Approach for Small Business

By: Michael Stango

Navigating the ever-changing landscape of data security has a tendency to tire even the most seasoned security experts, with good cause. Every day, countless cyber threats surface and wreak havoc on businesses without discrimination, whether they top the Fortune 500 charts or operate a small insurance agency from a home network.

Many small-business owners hear buzz words like ransomware, spear-phishing and denial of service and wonder how they can possibly defend their businesses from an endless barrage of cyber crime. The answer is not quite as overwhelming as one would think, and with some dedication, any business can come up with a plan to mitigate the risk of a data security breach.

A good way for small-business owners to begin addressing data security is to determine what exposure they have as a business and to translate that exposure into a data security policy. Most states have laws pertaining to the protection of the personal information of its residents and protecting that information should be the primary goal when developing a data security policy.

It's important to understand how the business handles personal information and what processes might be vulnerable to either accidental loss or a data breach. This might include such processes as emailing documents containing Social Security numbers or saving copies of checks on a computer.

Once vulnerable processes and procedures have been identified, it's crucial to develop a way to manage the security of these processes. Maintaining and updating hardware, such as firewalls, web filters and company computers, should be included in every data security policy, but shouldn't stop there. Also include upkeep for software, such as antivirus and email encryption.

Another way to manage security is to develop a retention schedule, which determines how long the business holds onto sensitive documents and information. If it's not there, it can't be breached.

Maintaining hardware and software and expunging unnecessary data are passive approaches as far as employees are concerned. It's also important to involve staff members in the process of developing a data security policy as they have first-hand experience with the processes that need to be safeguarded. Each team needs the opportunity to provide feedback and input or vulnerabilities may be overlooked.

Now that the data security exposure has been identified and safeguards have been developed, a plan can be created to keep the business' data safe.

Small-business insureds should review their policy on a regular basis, especially as procedures change and processes are added or eliminated. They should share the finished policy with employees as they are often the first line of defense against a data breach.

Unfortunately, data security plans have a tendency to be overlooked by employees. Therefore, it can be beneficial for small-business owners to take security a step further with cyber awareness training. They should consider providing employees information via email that covers a wide array of topics from identifying phishing emails to describing different types of cyber crimes.

We do this annually at A.I.M. Mutual and have found the training to be incredibly effective. There has been a significant increase in emails from employees asking questions like "Is this safe to click on?" or "Should I be seeing this pop-up on my computer?" It's a good

S·P 1865 Standard Publishing Corporation
www.spcpub.com

sign to be asked these types of questions because it means the employees are paying attention to the training.

To take the training a step further, some businesses may want to consider using a third-party vendor to send phishing emails to employees as a test. These emails entice employees to click embedded links for anything from breaking news to free hamburgers or gift certificates. Once clicked, the link can direct the employee to a page that explains the dangers of opening unidentified emails and clicking on malicious links. Here at A.I.M. Mutual, these phishing expeditions aren't winning us any popularity contests, but they have resulted in a 60% reduction in links clicked after just three campaigns.

A less invasive approach with employees is to send out periodic emails detailing current events in the world of cyber security. For example, business owners could periodically notify employees about major events in the cyber security world. If the event is a data security breach, remind employees about the dangers of phishing emails and clicking on malicious links online.

The recent Equifax breach of over 140 million records will directly affect many small-business employees, so business owners should take the opportunity to provide tips on what to do and what not to do after a breach.

Approaching data security is not a simple or straightforward task, but it is certainly possible for businesses both large and small to undertake. The key is to commit time to developing a data security policy, implement cyber awareness training and continually remind employees that the threat of a data security breach is real and that its impact could be devastating for the business. ■

Michael Stango is the information technology supervisor for A.I.M. Mutual Insurance Companies, a regional workers compensation insurance carrier. He has a background in data security, information systems analysis and project management, and leads A.I.M. Mutual's cyber awareness training program. Stango is the current chair of the company's Data Security Committee.