The Strong Case for Program Administrator/MGA Cyber Protection

By Kevin Ribble - E.V.P.
Edgewater Holdings

If you have not given this issue a great deal of thought, here are a few compelling reasons to employ cyber risk management and risk transfer to protect your business.

The broker and MGA business segment has been quick to capitalize on the new technologies of the 21st century, providing a variety of innovative tools reducing operating costs and expanding productivity from CSRs to customers. E-mail, online quotes, social media, mass marketing and webinars are just a few examples. New tools are now being utilized by small businesses including cloud computing and mobile applications. It is now easier for small businesses to store and access individual customer's and businesses' private information from anywhere in the world. Unknown to many small businesses, however, is the fact that certain legal responsibilities apply to the storage and management of data.

Would your agency be ready to respond to a data breach? In a recent case, a small insurance broker's employees showed up on a Monday morning and found they were unable to log into their computers. When the supervisors investigated they found their data had been stolen and their servers frozen. They discovered what may be a small business's worst nightmare - they were shut down and unable to conduct business. Loss of revenue was just the start of the problem. This event triggered a breach and customer notification requirement (required in several states). An average small employer breach response costs in excess of $100,000.

This type of event is on the rise as reported by William Weber, General Counsel, Cbeyond, Inc. to the Congressional Subcommittee on Health and Technology Protecting Small Businesses Against Emerging and Complex Cyber-Attacks, March 21, 2013.

"The recent string of cyber-attacks on high-profile companies is a stark reminder of the current threat. Although small businesses don't make the headlines, a recent report shows nearly 20 percent of cyber-attacks are on small firms with less than 250 employees. Small businesses

generally have fewer resources available to monitor and combat cyber threats, making them easy targets for expert criminals. In addition, many of these firms have a false sense of security and believe they are immune from a possible cyber-attack. The same report shows 77 percent of small firms believe their company is safe from a cyber-attack—even though 87 percent of those firms do not have a written security policy in place. There is clearly a gap in education and resources. Moreover, the sophistication and scope of these attacks continue to grow at a rapid pace."

Risk management and risk transfer

The subcommittee heard testimony from a number of professionals from the tech industry on how and why cyber risk is just as much, or even more, of a danger for small companies as it is for larger ones. The overarching theme of the discussion was that the cyber liability landscape is menacing and constantly changing. Cyber policies frequently do not keep up with the expanding methods of hacking attacks, leaving policy holders poorly protected. There are great variations between cyber forms, and some do not adequately address the potential liabilities for an insurance agency. Policies should at a minimum contain provisions for breach response, cost of informing customers, post-attack credit-monitoring, internet slander, credit card vendor fines and loss of business from denial-of-service attacks.

The following is a summary of security tips offered as part of the testimony before Congress.

1. Create a written security policy for employees.

When it comes to cyber security, one of the biggest problems is the lack of education among small-business owners and their employees.

In your security policy, determine whether employees should be allowed to have personal data on business devices, he said. Conversely, figure out whether business data should be permitted on their personal devices and what to do in case a device is lost or stolen.

2. Use stronger passwords.

This might seem like a no-brainer to some, but business owners have been "dumb" about creating smart passwords. If your password is a common word, or something that can be guessed based on public information, consider changing it to something more difficult to crack.

3. Encrypt your data.

You can't always keep hackers out of your computer systems, so take steps to protect the data contained within those systems. That's where encryption comes in. Disk encryption tools come standard on most operating systems, including BitLocker for Windows PCs and FileVault for Macs. These programs essentially convert the data on your systems into unreadable code that isn't easily deciphered by hackers.

4. Implement Bluetooth controls, pairing only known, trusted devices.

5. Protect against Trojan emails with blacklisting and whitelisting applications.

6. Have policy controls over web browser use and website access.

7. Install a firewall for mobile devices to restrict inbound connections and prevent use of mobile device as a bridge.

Small businesses are soft targets for hacker criminals, and the cost to deal with repercussions of a cyber attack could be disastrous for your agency. Purchasing cyber insurance should be a strong consideration. Purchasing coverage from someone who has the required expertise to ensure your particular business is fully protected is critical. ■

Footnote:

Statement for the Record
William Weber, General Counsel, Cbeyond, Inc.
Before the
United States House of Representatives
Committee on Small Business
Subcommittee on Healthcare and Technology
Hearing on
Protecting Small Businesses Against Emerging and Complex Cyber-Attacks
March 21, 2013