Commissioner's Column
Managing Cybersecurity Risks
March 2015

Cyberattacks, or crimes that try to damage, tamper or take data from a computer, system or network without approval, are a hazard of today's electronic information world. Attacks may come by way of internet sites and email and when a data breach occurs, reputational, legal, financial, and at times, regulatory risks are top concerns.

The recent cyberattack on Anthem, Inc. was the latest wake-up call to the corporate and regulatory world. Over the last 12 months, we have witnessed security data breaches of major U.S. corporations including Sony Pictures, Home Depot, Target and J.P. Morgan. But it is not only large corporations that are at risk. According to the U.S. Small Business Administration, nearly 20 percent of small businesses become victims of cybercrime and many of those businesses never fully recover from the attack.

Often small businesses don't realize their exposure to such risks. Not only is the business being attacked vulnerable to great harm, so are the businesses and individuals with which that company interacts. Small businesses are targeted by scammers not solely to steal the business' electronic data, but also to access larger sets of data held by those with whom the company conducts business. This snowball effect has the potential of causing even more widespread damage.

Protecting Your Business from Attack

When addressing cybersecurity concerns, experts recommend two primary strategies. The first focuses on prevention. Common practices include frequent back-ups of your important data as well as having antivirus protection. Small businesses may also incorporate layers of protection which can be recommended for their particular business needs by security experts.

Secondly, since cyber risk is not 100 percent eliminated through preventative security measures an important method of managing cyber risk is the purchase of a cyber liability insurance policy. Such a policy is in addition to a commercial general liability policy. A cyber liability policy protects both the business and its consumers when a data breach occurs.

Cyber liability insurance is not broadly purchased in the small business sector. It has been difficult to sell since small business owners are often not fully aware of the potential for loss in revenue, reputation and customer base they can face with just one cybersecurity failure. Insurance agents are critical in this discussion since they can change the level of preparedness for small businesses in their local areas.

The goal of the agent is two-fold. First they can educate small business owners on cybersecurity and make them aware of their options when it comes to cybersecurity insurance. Secondly, they are responsible to protect their own place of business and business data. Agents face

significant risks and liabilities since they handle a large amount of personal data. Protecting such data is just as urgent and important for insurance agents as it is for the small businesses with which they work.

Getting Out the Message

At the state level, agents may gain a strong knowledge base on cybersecurity when attending continuing education classes required for their license renewal. Such sessions are conducted as part of our annual Filing and Compliance Seminar and may also be found through other CE opportunities.

I am, along with the National Association of Insurance Commissioners (NAIC), committed to addressing cybersecurity in the insurance sector. The NAIC website is a robust source of information on cybersecurity and serves as a great resource. It includes a new section for small businesses called *Insure U for Small Businesses* which contains useful information for agents and consumers alike.

The NAIC is closely monitoring the Anthem cybersecurity breach. Indiana Commissioner Stephen Robertson is meeting with Anthem executives regularly and has ensured that the best possible identity protection services have been provided to those impacted by the security breach. The Louisiana Department of Insurance has joined all insurance commissioners, directors and superintendents in a weekly NAIC conference call for updates on Anthem progress in mitigating damage. Regulators are also conducting a multi-state financial and market conduct examination. The NAIC Cybersecurity (EX) Task Force will monitor these efforts, update best practices and determine whether regulatory action is warranted.

In addition, in mid-March the NAIC released two draft documents on cybersecurity for comment. The first, *Principles for Effective Cybersecurity Insurance Regulatory Guidance,* outlines the process for regulators to identify cyber risks and will help state insurance departments identify uniform standards. The second draft document, *Annual Statement Supplement for Cybersecurity policies*, is a form for companies providing cybersecurity coverage to provide comments about their exposures.

The National Conference of Insurance Legislators (NCOIL) has also indicated a high level of concern on cybersecurity measures needed in the business sector, particularly the insurance sector. Over at their 2015 Spring Meeting, NCOIL and regulators expressed their concern over how the insurance market as a whole can be impacted by a significant cyberattack. A panel of insurance regulators suggested that new tools are necessary to prepare for such an attack, giving regulators monitoring capabilities over insurers' current level of preparedness.

Additional Measures to Protect Yourself Against Fraud

Other practical measures one may take to protect against fraud include regular reviews of your credit reports as well as bank and credit card account statements for signs of suspicious or

fraudulent activity. If an incident of identity theft is suspected, report it to your bank or credit card company immediately. Also report it to your local law enforcement, the Federal Trade Commission (FTC) or your state attorney general.

Federal and state governments, along with the private sector, are taking seriously the urgency to prioritize cybersecurity and follow best practices to prevent possible breaches in their data systems. I encourage you to join in the efforts by protecting yourself and educating your clients about the risks and solutions regarding this matter.