Managing Cyber Risks

By Eric Nordman, CPCU, CIE, Director, Regulatory Services Division and the CIPR

◆ Introduction

As I write this article, I long for the days when life was simpler … when the post office brought my mail instead of a desktop computer … when I gave my handwritten notes or dictation to the typing pool and eventually a letter came back for my review … when people did not stand in line overnight to get the latest, greatest Apple iPhone. OK, so now you know that a curmudgeon is writing this article on cyber risk management. It is still worth reading, as my background tends to push me into evaluating everything from a risk-management perspective.

All of this new technology comes with risk. Once these risks are identified, understood and quantified, they can be avoided, controlled, combined, retained or transferred using insurance or other risk-management techniques. So now you get the picture. This article will discuss cyber risks and have some suggestions about what to do with them. Some creative insurers have already done much thinking about cyber risks and are offering innovative insurance products to meet businesses' risk management needs.

◆ Cyber Risk Management

If you own a computer, you are at risk. If you have the computer connected to the Internet, you are at greater risk. If you use the computer to send and receive email, you are at risk. If you store anything on the computer, you are at risk. If you let employees place sensitive information on a laptop, your risk increases. If you allow employees to use memory sticks or thumb drives, you are at risk. Nearly anything you do with a computer creates risk for you.

The cyber risks for a business are almost endless. As data breaches occur more frequently, there are additional pressures for business to step up efforts to protect the personal information in their possession. In fact, there is legislation requiring the protection of personal financial information and personal health information. Some of the key risks associated with owning a computer are:

- Identity theft as a result of security breaches where sensitive information is stolen by a hacker or inadvertently disclosed, including such data elements as Social Security numbers, credit card numbers, employee identification numbers, drivers' license numbers, birth dates and PIN numbers.
- Business interruption from a hacker shutting down a network.
- Damage to the firm's reputation.
- Costs associated with damage to data records caused by a hacker.
- Theft of valuable digital assets, including customer lists, business trade secrets and other similar electronic business assets.
- Introduction of malware, worms and other malicious computer code.
- Human error leading to inadvertent disclosure of sensitive information, such as an email from an employee to unintended recipients containing sensitive business information or personal identifying information.
- The cost of credit monitoring services for people impacted by a security breach.
- Lawsuits alleging trademark or copyright infringement.

Applying avoidance by selling all of your computers is probably tempting on some days, but is not generally the risk-management technique of choice. That leaves various forms of mitigation and risk transfer on the table for consideration. Because managing computer networks is outside my scope of knowledge, the remainder of this article will focus on managing cyber risks through insurance.

◆ Cyber Liability Policies

Most businesses are familiar with their commercial insurance policies providing general liability coverage to protect the business from injury or property damage. However, most standard commercial lines policies do not cover many of the cyber risks mentioned earlier. To cover these unique cyber risks through insurance requires the purchase of a special cyber liability policy. The markets for these policies are relatively new, with a growing number of insurers offering coverage. Like all new markets, coverage contained in the policy forms is evolving as risks evolve and competitive forces come into play. As a result, if you have seen one cyber liability policy you will have seen one cyber liability policy. It will be different than the cyber liability policy from the next insurer.

There are some risks that are commonly covered by cyber liability policies. Generally, cyber liability policies cover a business' obligation to protect the personal data of its customers. The data might include personal identifying information, financial or health information, or other critical data that, if compromised, could create a liability exposure

(Continued on page 29)

for the business. The policy will cover liability for unauthorized access, theft or use of the data or software contained in a business' network or systems. Many policies also cover unintentional acts, errors, omission or mistakes by employees, unintentional spreading of a virus or malware, computer thefts or extortion attempts by hackers.

Cyber liability policies tend to be customized to meet the risk-management needs of the policyholder. Because businesses are unique in many ways, this customization feature allows the insurer to tailor a policy to meet the unique nature of each business. Thus, the type of business operation will dictate the type and cost of cyber liability coverage. The size and scope of the business will play a role in coverage needs and pricing, as will the number of customers, the presence on the Web, the type of data collected and stored, and other factors.

Cyber liability policies might include one or more of the following types of coverage:

- Liability for security or privacy breaches. This would include loss of confidential information by allowing, or failing to prevent, unauthorized access to computer systems.
- The costs associated with a privacy breach, such as consumer notification, customer support and costs of providing credit monitoring services to affected consumers.
- The costs associated with restoring, updating or replacing business assets stored electronically.
- Business interruption and extra expense related to a security or privacy breach.
- Liability associated with libel, slander, copyright infringement, product disparagement or reputational damage to others when the allegations involve a business website, social media or print media.
- Expenses related to cyber extortion or cyber terrorism.
- Coverage for expenses related to regulatory compliance for billing errors, physician self-referral proceedings and Emergency Medical Treatment and Active Labor Act proceedings.

Securing a cyber-liability policy will not be a simple task. Insurers writing this coverage will be interested in the risk-management techniques applied by the business to protect its network and its assets. The insurer will probably want to see the business' disaster response plan and evaluate it with respect to the business' risk management of its networks, its website, its physical assets and its intellectual property. The insurer will be keenly interested in how employees and others are able to access data systems. At a minimum, the insurer will want to know about antivirus and anti-malware software, the frequency of updates and the performance of firewalls.

◆ CONCLUSION

The market for cyber liability insurance policies is relatively new. Like many new markets, it is off to a good start, but expected to grow dramatically over time. New competitors are closely following what early entrants have done. Businesses are gradually becoming more aware that current business policies do not adequately cover cyber risks. With each announcement of a system failure leading to a significant business loss, the awareness grows. Soon, business leaders will recognize what their information technology staff has been telling them. Running a computer operation with exposure to the Internet is risky, but necessary, for a business to succeed in the modern world. Thankfully, there are ways to protect the business from financial ruin through this rapidly growing niche insurance market.

National Association of Insurance Commissioners
& The Center for Insurance Policy and Research

NAIC Central Office
Center for Insurance Policy and Research
1100 Walnut Street, Suite 1500
Kansas City, MO 64106-2197
Phone: 816-842-3600
Fax: 816-783-8175

http://www.naic.org http://cipr.naic.org

The National Association of Insurance Commissioners (NAIC) is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and five U.S. territories. Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their regulatory oversight. NAIC staff supports these efforts and represents the collective views of state regulators domestically and internationally. NAIC members, together with the central resources of the NAIC, form the national system of state-based insurance regulation in the U.S. For more information, visit www.naic.org.