Cyber Risk: Danger from Inside & Out

Overview

Fifteen years ago, few people used email, websites were a novelty and banking on-line was a pipe dream. Today, WiFi is an expected service at hotels, Intranet “team rooms” are as common as copy machines, and you can use a cell phone to check your bank balance.

This dramatic change in the use of technology has a major impact on the risks businesses face, particularly those firms that process, retain, or manage personal information or protected health information. Today, virtually every organization faces “cyber risks”, a host of new perils that can strangle an organization if the proper precautions are not taken.

Cyber Risk: What is it?

Cyber risk comes in three key forms:

1) actual or threatened damage to physical property such as servers, networks and media storage devices;

2) loss of income due to downed systems (yours or your suppliers); and

3) liability for damages caused to others by your Internet-based operations.

While the damage to physical property is finite, the potential damage caused by one’s liability for failing to protect sensitive data of others is less tangible.

Limited insurance coverage for certain types of “cyber risks” may be found in traditional property and liability insurance policies, although most exposures fall outside the scope of coverage or are excluded outright. For instance, a traditional general liability policy would not cover the cost of notifying third-parties of a data breach or the cost of credit monitoring.
Why has “cyber risk” become such an issue for insurors? Simple: damages due to cyber related activity is inevitable for many organizations, but it has not been properly factored into the pricing structure of traditional property and liability policies.

Cyber Risk & Organized Crime

Organized criminal networks are a major source of cyber damage and have developed sophisticated means of targeting on-line retailers, banks, data processing companies and the medical industry. Once the criminals are in possession of confidential data, they typically do one of two things: sell the information to scam artists throughout the world or blackmail the breached company with the threat to publish the data in a public forum. With the economic downturn, criminal activity is expected to rise, placing organizations at heightened risk for data breach incidents.

Several years ago a well known national retailer’s network was breached by an Eastern European criminal ring and thousands of customer records were stolen. When the retailer refused to pay the “ransom”, the cyber criminals published the data on public websites. The retailer experienced a public relations nightmare. In addition to the loss of customer confidence and goodwill, the retailer incurred significant expense notifying customers of the breach. Class action lawsuits followed, along with heavy fines and penalties from state and federal agencies for failing to properly protect the customers’ confidential information.

While the ultimate cost of this breach was extraordinary, this scenario has the potential for repeating itself.

Another cyber risk is an online attack against an organization’s IT network for extortion purposes. Rather than stealing data, criminals extort businesses by shutting down, or simply threatening to shut down, their networks and websites. By launching huge spam and denial-of-service attacks from “zombie” computers throughout the world, cyber criminals can cripple an organization’s ability to conduct Internet-based operations.

Conclusion

The growing demand for insurance products to protect businesses against “cyber risks” has spawned a range of new and complex products, leaving buyers with the daunting task of finding the appropriate policy. Premium costs vary widely by insurance company as well as the scope of coverage. Determining your exposures and objectives is a critical first step in matching your organization’s risks with the appropriate coverage form. Fortunately, with insurers competing for market share in this relatively new world of “cyber insurance,” first time buyers are attracting strong competition on price and policy terms.

This notice is provided as information only and should not be considered a legal opinion. If you have questions about this Client Advisory, please contact Seacrest Partners at 912-544-1900.