ISO Products Perspective

Shawn E. Dougherty

CYBER PREPAREDNESS

Addressing a data breach takes more than insurance

It took a while, but you persisted. After you spent quite a bit of time working with your clients, helping them analyze the exposures and weigh the various pros and cons, they finally decided to bite the bullet and purchased cyber insurance coverage. Now you can sleep better at night, and so can your clients.

But wait—one day, several months later, you receive a call from one of your clients with news that they suspect they've suffered a data breach. They ask you what they're supposed to do. Now what?

Procuring cyber insurance coverage was an excellent move, but it doesn't stop there. As your clients decide how they want to manage their risks, they need to be prepared for a data breach incident, which can come in many forms.

Data breach incidents

Many people mistakenly believe that data breaches occur only when unscrupulous hackers make their way into a company computer system and siphon away customer information. That customer information is commonly referred to as personally identifiable information (PII) and protected health information (PHI). PII includes, for example: names; addresses; birthdates; and Social Security, credit card, or bank account numbers. PHI refers to such data as health care policy information, medical records, and health conditions. During the past year, there have been many reports of data breaches among popular retailers such as Target, Michaels and P.F. Chang's as well as many health care facilities, educational institutions, and government offices.

While hacking tends to be a popular way to conduct a data breach, it's not the only way.

• Physical theft: In today's connected world, many companies conduct business with mobile devices, such as smartphones and tablets. When those devices are lost or stolen, it can have a profound effect on a business's operations. In fact, lost or stolen devices were the most frequent cause of cyber insurance loss, according to a survey by NetDiligence® last year.

• Improper disposal: Paper files containing Pll or PHI are another consideration. Misplacing or forgetting to shred documents with confidential information can result in a data breach as can the theft of paper files.

• Cyber extortion: Using ransomware, cyber extortionists can hijack a company's computer system, deny access to employees, and threaten to erase files unless they're paid a ransom. Those businesses then are often left with the difficult question of whether to pay such ransom or risk losing valuable information.

Cyber Preparedness

Cyber preparedness should begin well before a data breach incident ever happens. The first step is to develop a comprehensive cyber emergency response plan for all employees before an incident occurs. A well-thought-out plan should include best practices to help minimize the potential for a data breach as well as outline steps to follow if an incident takes place. For example, an effective plan will typically identify managers to contact in the event of a breach and also will outline when to make such contact.

Developing and distributing a cyber emergency response plan, though, is often simply not enough. A company also should identify ways to make the response plan normative throughout its workforce—that is, make it almost second nature as opposed to an afterthought. One generally effective method to educate staff is periodic tabletop drills. Walk all staff members through hypothetical cyber scenario exercises outlining the steps they should follow throughout the response process. During the exercise, it’s critical for everyone—including company management and key decision makers— to be on board and know who will handle what. This includes identifying a key spokesperson to serve as the voice of the company should a breach occur.

More than just insurance

Many of the tasks necessary to prepare for a potential breach, and then those tasks that may be necessary after a breach occurs, sound daunting. For example, a company that has suffered a data breach may need to provide notification to its customers. Currently, 47 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have enacted laws that require companies to notify potentially affected individuals of a data breach. (Visit the National Conference of State Legislatures website, www.ncsl.org, for details.) Additionally, that company may also need to determine whether a data breach has actually occurred. That may require a forensic analysis, which would also help determine what, if any, PII or PHI was accessed and how the system was attacked.

Companies need not fret, however. They don’t have to go through this process alone. Many insurers offering cyber insurance have partnered with cyber-related service firms that provide pre-security-breach services, designed to prepare for and reduce the likelihood of a breach, and aftersecurity- breach services, designed to respond to and reduce the impact of an incident. Firms such as Identity Theft 911, ID Experts, Kroll, and NetDiligence are just a few of the companies that provide various tools and services to help educate, assess, and prepare companies prior to experiencing a cyber-related incident and offer remediation services after a data breach incident. Companies that experience a data breach incident may find that leveraging the services of a skilled service provider—seasoned professionals who are experts in the field and who know how to navigate the potential land mines of a data breach—may make dealing with such an incident a less stressful process.

At the end of the day, a company’s cyber preparedness goes well beyond just having insurance coverage in place. Companies need to do all they can to prepare for and survive a cyberrelated incident.

The Author

Shawn Dougherty is assistant vice president of Specialty Commercial Lines at ISO, a member of the Verisk Insurance Solutions group at Verisk Analytics (Nasdaq:VRSK).