TOLMAN & WIKER INSURANCE SERVICES, LLC
INNOVATIVE RISK ADVICE SINCE 1923™
VENTURA | LOS ANGELES | SALINAS | SANTA MARIA | BAKERSFIELD

A Peek Under the Cyber Covers

March, 2014

The Rough Notes Company, Inc.

The insurance industry has put a tremendous amount of focus on the topic of cyber liability over the past 12 to 18 months. Virtually every insurance-related conference presents at least one cyber-related session, and many insurance trade publications include at least one article addressing the subject in each issue.

But what exactly does “cyber” refer to? These days, when the topic is raised, one might naturally think of computer- and/or Internet-related exposures—issues such as cyber attacks, computer hackers, computer viruses, cyber extortion, cloud computing, and the like.

While those are definitely exposures that many cyber liability insurance policies available in the marketplace aim to address, focusing solely on the computer and technological risks is insufficient. Upon closer examination, one may discover that cyber insurance covers more than what’s generally considered “cyber.”

The primary exposure is data breach—defned for the purposes of this article as the unauthorized access to an individual’s personally identifiable information (PII) or protected health information (PHI). PII includes such information as name, address, birth date, Social Security number, driver’s license number, credit card information or, as one state specifies, postal ZIP code. PHI includes an individual’s health care policy number, biometric information, medical condition, and so on.

Many of today’s cyber liability insurance policies cover the data breach exposure regardless of the medium in which the information is stored.

Data breach exposure is real, and businesses of all sizes ought to be concerned. Each firm possessing such information must be a vigilant guardian and trusted steward of that data as long as it’s in the company’s possession. It doesn’t matter whether the information is maintained in electronic format (stored on a server, computer hard drive, hand-held device or tablet, or “in the cloud”) or in a non-electronic format (such as paper files kept in a desk drawer or at an off-site storage facility).

Many data-rich firms and organizations with access to their customers’ PII and/or PHI traditionally relied on paper-centric record keeping, and many still do. Educational institutions, churches, doctors, accountants, lawyers, and even insurance agents, just to name a few, are typical examples. The information maintained is not limited to customer information. It includes PII and PHI for any current, former, or potential employees as well.

Keep in mind that some instances of wrongful access might not be considered at first to be a data breach.

For instance, there have been documented cases across the country over the past several years of thousands upon thousands of patient x-rays having been stolen from hospitals, medical imaging facilities, and off-site warehouse storage facilities. The x-ray files—purportedly stolen to be sold for the value of the silver they contain—included information such as patient name, birth date, and patient number. Even though the x-rays were not in electronic format, the loss of the files containing the confidential information could technically be considered a data breach.

Another good example of a potential non hacker- related data breach can result from leased photocopiers being returned to office equipment vendors without first having their internal hard drives erased. The same might also occur with the all-in-one print/copy/scan/FAX machines that small businesses purchase from electronics or office supply stores that may get recycled when no longer in use. Depending on the type of information previously copied or scanned on the equipment—for example, health records, financial records, employment records, driver’s licenses, or passports—an unintended data breach might result if that data is accessed.

One final common example is the improper disposal of paper files. Businesses must properly shred or destroy files containing PII or PHI— and not just send them to a recycling center or dispose of them with regular trash, where almost anyone can gain access to them.

Coverage and services

Robust cyber liability insurance policies, such as those available with the ISO E-Commerce program, make available first- and third-party insurance coverages designed to help protect commercial insureds from data breach exposures. Such policies generally include coverage for:

• security breach expenses

• public relations expenses

• business income and extra expenses

• extortion threats

• replacement or restoration of electronic data

• Web site publishing liability

• security breach liability

• programming errors and omissions liability

For smaller commercial risks eligible for business owners policies, many carriers make available optional endorsements that generally address the first-party coverages only.

Beyond the insurance coverage perspective, your clients might also need to consider the services of a firm that provides pre-breach assessment and/or post-breach remediation and crisis management services. Many carriers offer such services to their insureds as part of their overall insurance program offering.

Currently, 46 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted legislation generally requiring businesses that suffer a data breach to notify all affected and potentially affected parties. In addition, various federal laws—such as HIPAA and its 2009 HITECH modification—also hold companies in the financial services and health care industries liable for the disclosure of confidential customer information.

Here are some topics to discuss with your clients as you educate them and help them evaluate their need for, and the benefits of, a cyber liability insurance policy:

• What confidential information do your clients collect and maintain in electronic and non-electronic formats? What security measures do they have in place to protect that information from inappropriate disclosure?

• Do your clients have a document retention policy, and do they follow it? What procedures do your clients have in place to discard properly and destroy files containing PII or PHI that they no longer need to maintain?

• Do your clients utilize the services of a third-party firm to convert paper documentation into electronic format or to store those paper files off-site? Do your clients receive the original paper files back or ensure their destruction? How secure are those off-site files?

• Will your clients be able to comply with state data breach notification requirements if they experience a data breach? Do they have a data breach response plan in place, and do their employees know what to do if a potential data breach is discovered?

Help your clients take a peek under the “cyber” covers and understand the non-computer-related aspects of PII and PHI protection. Doing so may help them avoid the monster that might indeed be lurking beneath the bed.

www.roughnotes.com

Forward this article to a colleague


Address To
Recipient Name
Subject
Message
Send
Reset