Navigating the Cyberblitz: Risk Management with Cyber Liability Insurance

By Michelle C. Harrell

Everywhere we turn today, we are blitzed with the word “cyber” as a prefix to describe a multitude of hazardous computer or internet issues, such as cybercrime, cyberattack, cyberhacking, and cyberliability. The cyberlist goes on and on and continues to evolve. As business connectivity and globalization increases, business risk due to internet security issues also increases. There is a new “old” saying that “there are only two kinds of companies: those that have been data breached and those that just don’t know that they have been data breached.” As revealed in the *2014 Cost of Data Breach Study: Global Analysis*, the average cost to a company for a data breach was $3.5 million, up 15% from 2013. The costs increase exponentially if statutory notice requirements are triggered due to a breach involving private personally-identifiable information (PII) that are subject to heightened protection and reporting requirements. For many companies, the level of cost due to a cyberbreach may force the company into bankruptcy or, at least, dire financial straits.

How can a business manage the risks to its own data, PII and other sensitive information that it receives from others and stores? There are several components to a proper and sufficient business cybersecurity plan. One of the most important components of a proper cybersecurity plan is the procurement of cyber liability insurance coverage for your company. The components of a strategic, complete cybersecurity plan are developing in many sectors. On February 12, 2013, President Barack Obama issued Executive Order 13636 that mandated the improvement of critical infrastructure cybersecurity due to repeated cyber intrusions into critical infrastructure to promote national security. As required by such Executive Order, the National Institute of Standards and Technology issued its *Framework for Improving Critical Infrastructure Cybersecurity* on February 12, 2014. Although the *Framework* is directed to infrastructure companies, many consultants believe that it will evolve into broader regulatory requirements and will be used to determine various government incentives. The *Framework* includes a “Framework Core” which is a set of cybersecurity activities, desired outcomes,

and applicable references that are common across various business sectors, and identifies five concurrent and continuous functions: Identify, Protect, Detect, Respond, Recover. Cyberliability insurance enables a company to quickly respond to, and recover from, a cyberbreach event, and could be key to getting back to business post-breach.

A company has several options when considering cyberliability insurance, which is a term used to generally describe a broad range of information security types of coverage. Some of the specific types of cyberliability coverage to consider are:

1. Data Loss and System Damage: While your property damage coverage may cover damage to the physical computer itself, it likely will not cover the intangible data stored in the computer.
2. Business Interruption: This coverage addresses the loss of revenue after a cyberattack from downtime, denial of service, presence of a virus that causes a long-term or temporary shutdown.
3. Notification and Credit Monitoring Expense: Almost every state has notification requirements that are triggered after a breach has occurred. These notification requirements arise when a breach involves certain types of access, disclosure or acquisition of private information. In addition to notification, ongoing credit monitoring may also be required. For example, Michigan's Identity Theft Protection Act, MCL 445.61, *et seq.*, states that a company that maintains a database that includes information that the company does not own or license must provide notice of a security breach to the owner or licensor of the information without unreasonable delay. MCL 445.72.
4. Public Relations and Crisis Management: Most companies who were surveyed for the *2014 Cost of Data Breach Study* indicated that the most significant damage that was immediately suffered was extensive damage to the companies' reputations. Repair to customer confidence and public image can be very expensive.
5. Content Liability: This coverage addresses the content of your company's website or other internet presence such as a blog, including any claims for copyright infringement, defamation claims, or similar exposures.
6. Regulatory Coverage: In this era of government investigations, it is possible that your company may be subjected to a compliance audit. Many policies exclude coverage for the expenses relating to such audits. However, depending upon your company's regulatory environment, you may want to check with your insurance agent about this coverage.

Determining the nature of coverage needed can be a tricky endeavor and a company should enlist the expertise of its insurance agent when assessing the types of coverage that the company should obtain. Cyberliability insurance is an important part of any cyberliability program.