The Metropolitan
Corporate Counsel®
National Edition
www.metrocorpcounsel.com
Volume 22, No. 7

July/August 2014

Cyber Insurance: The Basics Of The Coverage

Annmarie Giblin *is an Attorney with Leader & Berkon LLP and is resident in the firm's New York office. She has over seven years of litigation experience and focuses her practice in commercial, toxic tort and product liability litigation. Interviewee* ***Matthew Magner, Esq.,*** *is a Senior Underwriting Officer with the Chubb Professional ("ChubbPro") business unit of Chubb Specialty Insurance (CSI). He specializes in writing the professional and management liability lines for law firms. Matt frequently speaks and writes about information privacy exposures and has worked in the insurance industry for more than 15 years with experience in insurance defense litigation, claims and underwriting.*

Annmarie Giblin

Matthew Magner

In the time it took to research and draft this article, approximately two months, three major cyber attacks were reported in the news. The most recent was the Heartbleed bug, which was dubbed the biggest security threat the world had ever seen. These attacks do more than threaten both business and private security. They open up whole sectors of business to a new class of liability unlike any contemplated before. And while the litigation floodgates are just starting to open, what has become clear is that many business entities are ill-prepared for the potentially catastrophic fallout from an information security or cyber breach.

In response, cyber insurance is becoming a necessary protection. However, cyber insurance policies are not all the same. In fact, insurance clauses, exclusions and terms can vary significantly from one policy to the next.

Considering the ramifications of choosing the wrong policy, deciding which policy to select can be a daunting task for many companies. That is why I asked Matt Magner, Esq., who has expertise in cyber liability and is a senior underwriter with The Chubb Group of Insurance Companies, to share some best practices to help mitigate the risk of a data breach. Matt specializes in providing professional and management liability insurance for businesses and for law firms, and he frequently speaks and writes about information privacy exposures. He has worked in the insurance industry for over 15 years with experience in insurance defense litigation, claims and underwriting.

Giblin: Who needs cyber insurance?

Magner: All businesses that deal with electronic information need this type of coverage, from a small independent store owner to a large corporation. For example, a small corner store owner may be more worried about liability insurance for injuries on his property, but if the business has a website or accepts credit cards as a form of payment, cyber insurance may be just as important to protect a business as a general liability policy. The potential damage, in the form of liability and out-of-pocket losses, could be greater with a cyber incident than if someone was injured in his store. The cyber dangers seem more obvious to most large and professional corporations and businesses, especially those that deal with sensitive information, but many smaller businesses do not fully understand the risks.

Giblin: Is there anything that businesses should do before buying a cyber insurance policy?

Magner: The first step a business should take is to have penetration testing performed on its system. This will help to determine if there are any security weaknesses in the company's computer system that would allow a hacker to gain access to confidential information.

Second, companies should have an up-to-date, written security policy — this acts as a business plan to help prevent a data breach. The security policy should address the types of information with which the business deals and ways to protect it. It should include rules for employees on how

Please email the interviewer at agiblin@leaderberkon.com or the interviewee at mmagner@chubb.com with questions about this interview.

they are expected to store and disseminate information, including medical records. In addition, employees should be educated about the rules and trained on how to follow them.

Third, businesses should develop an incident response plan (IRP). An IRP lays out the business's response to a breach. The IRP designates a "Tiger Team," consisting of both internal and external personnel who will be called upon in the event of a breach. A Tiger Team will differ for each business but should include, ideally at pre-negotiated rates:

- a public relations professional, who will help break the news of the breach to the public and clients/customers;
- a forensics analyst, who will help to identify what was taken and how the breach happened; and
- a legal professional, to help navigate the state and federal response obligations and manage any potential liabilities/litigation that may arise from the breach.

Designated internal personnel will be responsible for reporting the incident internally, and if necessary, externally — and overseeing the coordination of the response.

Fourth, mobile devices used by employees on a daily basis, including laptops, smart phones and portable hard drives, should be encrypted. Encryption utilizes software that renders data unreadable and should also include the ability to wipe data and destroy information if the device is lost or stolen. Certain state laws will respond more favorably when devices are encrypted, which could help businesses avoid heavy fines in the event of a breach.

The final step involves hiring a third-party vendor or consultant to come in and help the business enact these protocols and assess how strong they are. Some insurance companies help their customers with these tasks. For instance, Chubb provides its cyber insurance customers with access to eRisk Hub, an online site that provides a template to help develop an incident response plan, access to a data breach attorney, and recent articles, white papers and other risk management tools.

All businesses that deal with electronic information need this type of coverage, from a small independent store owner to a large corporation . . . a small corner store owner may be more worried about liability insurance for injuries on his property, but if the business has a website or accepts credit cards as a form of payment, cyber insurance may be just as important to protect a business as a general liability policy.

Giblin: How does a professional liability policy interact with a cyber policy?

Magner: Both the professional liability policy and the liability portion of the cyber policy may be triggered in the event of a data breach. Assume, for example, an attorney loses her laptop, resulting in a data breach. A lawsuit may arise, with defense expenses and an award or settlement. The liability portion of the cyber policy will be designated as either primary or excess with respect to the professional liability policy. However, even when the cyber policy is designated as excess, it may remain primary with respect to any out-of-pocket first-party expenses, such as notification costs or crisis management expenses incurred by the insured.

Giblin: What are the essential elements for a cyber insurance policy?

Magner: The needs of each business/company will vary, and most companies can customize a cyber policy based on those needs.

Essential insurance coverages available include:

- liability insurance for data breaches to cover defense expenses, awards and settlements in connection with a lawsuit;
- notification/crisis management expenses, which can include costs for legal counsel, public relations, forensics, drafting and dissemination of notices and credit monitoring;
- business interruption and extra expense coverage, which will provide lost income and cover expenses to facilitate the insured's return to operation;
- electronic vandalism, which provides coverage to pay for blank media and transcription for electronic data corrupted in the event of cyber incident;
- extortion coverage to cover ransoms for hackers who hold a network or data hostage; and
- defense of regulatory proceedings and coverage for fines and penalties.

It is important for the company to discuss its business with an experienced broker to ensure that the appropriate coverage is in place.

Giblin: In what ways do you see cyber insurance policies changing over the next few years?

Magner: Cyber liability insurance is currently in a state of flux. When the policies were first written over a decade ago the exact exposures were not fully understood, and even today, the risks and liabilities are still being defined. With each new claim and incident that occurs, the industry's understanding of what protections are needed is constantly being updated. This will only be compounded as time goes on and technology becomes more sophisticated. Cyber insurance policies will continue to evolve as our understanding of the risks evolves.