MEALEY'S®
Data Privacy Law Report

Protecting Company Assets With Cyber Liability Insurance

by
Eileen Garczynski
and
Syed Ahmad

Ames & Gough, Hunton & Williams LLP
Washington D.C.

A commentary article reprinted from the March 2017 issue of Mealey's Data Privacy Law Report

LexisNexis®

Commentary

Protecting Company Assets With Cyber Liability Insurance

By
Eileen Garczynski
Ames & Gough
and
Syed Ahmad
Hunton & Williams LLP

[Editor's Note: Eileen Garczynski is Senior Vice President and Equity Partner at Ames & Gough located in McLean, Virginia, and Syed Ahmad is a Partner with Hunton & Williams LLP, located in Washington, D.C. Any commentary or opinions do not reflect the opinions of Ames & Gough, Hunton & Williams LLP, or LexisNexis®, Mealey Publications™. Copyright © 2017 by Eileen Garczynski and Syed Ahmad. Responses are welcome.]

US retailers and other businesses face significant cybersecurity threats that jeopardize their infrastructure, their economic viability, and their reputations. While the means of cyber-attacks vary, the pattern of targets has been relatively consistent. Large databases, as well as point-of-sale systems, continue to be targeted for financial gain or for other motives. Hackers with possible ties to nation-states continue to target infrastructure as well as systems for political insight. The recent news of Russian agents allegedly being involved with the Yahoo breach is yet another example of the threats faced by companies.

The Heritage Foundation noted that in the last half of 2016 alone, there were several large scale attacks on several notable US businesses:

- Citibank had ninety percent of its North American networks taken offline after an employee in charge of the bank's IT systems, following a poor performance review, sent malicious code to 10 core Citibank Global Control Center routers. He has since been sentenced to 21 months in federal prison and fined $77,200.
- Banner Health had almost four million of its patients, physicians, and customer's information compromised. Yahoo reported in the fall of 2016, that more than 500 million of its users' names, e-mail addresses, birthdates, phone numbers, and passwords were compromised—possibly a state-sponsored breach.
- Yahoo began investigating the breach after 280 million users' information was being offered for sale on the dark web.
- CiCi's Pizza Restaurant Chain suffered a point-of-sale breach affecting customers' payment information that first broke on KrebsOnSecurity. CiCi's Pizza eventually acknowledged the breach and that the compromise to its systems began as early as the late Spring of last year.

This list of successful and notable cyber incidents barely scratches the surface of the number of smaller attacks or breaches that occur on a daily basis. A privacy or security incident can cause a company a great deal of unwanted press and involve substantial costs. If the company's systems go down for any amount of time, significant work time may be lost. Then there's also the cost of any forensic investigation, potential federal and state regulatory fines and notification costs; not to mention issues with third parties, a flurry of lawsuits, negative publicity, reputational damage, and disgruntled clients.

Managing Cyber-Risk

In the wake of so many cyber-breaches, cyber-liability insurance is a critical component of every company's

comprehensive breach response plan. Keep in mind, however, that all cyber-insurance policies are not identical, and unlike more traditional policies that have been around for decades, there is no "standard" cyber policy.

In choosing a cyber-liability insurance policy, employ experienced brokers and counsel to carefully outline the scope of coverage and exclusions under a data breach policy, including whether the policy covers costs related to lawsuits, regulatory investigations, internal investigations, and notifications to affected consumers, public relations management, and credit monitoring, and/or statutory penalties.

Standalone cyber-liability insurance policies, addressing both first- and third-party perils, offer a full range of coverage that is key to mitigating risk. The policies typically provide coverage through numerous insuring clauses that afford coverage for losses arising out of data or privacy breaches. These include expenses related to the management of an incident, such as forensic investigation, remediation, notification and credit checking. They also provide coverage for business interruption losses, extortion network damage, and regulatory investigation costs arising out of a cyber-event.

Understanding Potential Coverage Restrictions

Companies purchasing standalone cyber-liability insurance policies should thoroughly understand exactly what their insurance covers, the extent of coverage provided, as well as any coverage exclusions or restrictions. In comparing various cyber-liability policies offered by different insurance companies, be aware that many insurers will attempt to add exclusions. While it is not always possible to remove these exclusions, companies should understand their potential impact and attempt to have them modified or removed. There are more than a dozen specific types of coverage exclusions or restrictions that might appear in many cyber-liability insurance policies. Here are a few key examples:

- *Definition of covered information.* Some policies define covered information as only Personal Identifiable Information (or PII, such as date of birth, Social Security number, driver's license ID, etc.). However, cyber insurance policies providing broader coverage define protected information as many other kinds of confidential information.
- *Encryption exclusions for mobile devices.* Some policies exclude coverage if the company's mobile devices are not encrypted. Encrypting these devices is sound risk management and should be standard practice. Ideally, however, coverage is not contingent on this being done.
- *Retroactive date.* Some policies exclude coverage for claims that could have been reasonably foreseen. For this reason, companies should try to limit their knowledge of claims to key individuals at the company such as the head of IT or the company's CIO. Furthermore, coverage under a good cyber insurance policy is triggered by the "discovery of the network security event" and not the occurrence of the incident. This negates the need for full prior acts or a retroactive date prior to the inception of the policy. However, if you do not have date of discovery language, you will need a full prior acts policy or one with a retroactive date prior to the inception of the policy.
- *Definition of damages/loss.* Certain risks covered by cyber-policies may have unique remedies and involve related costs. For example, privacy violations can result in a duty to notify affected individuals and to provide credit monitoring for defined periods of time following the violation. Companies should be sure the "loss" as defined and covered by the policy addresses the types of relief they may be required to provide.
- *Data outside an insured's network or premises.* This wording affects cloud providers or other outsourced vendors and should be reviewed carefully. Most cyber-insurance policies define a "computer system" to include third-party networks with which you have contracted to support your business. Thus, in the event of a breach, the policy will respond regardless of where data was stored when the breach occurred. In other words, the coverage should follow the data, no matter where the data is stored.
- *Voluntary notification.* During the past several years, most states and various countries have enacted breach notification laws. Generally, they require businesses to provide written notification to all individuals potentially affected by a breach of personal data. Even without a legal obligation to do so, voluntary notification is becoming increasingly common to protect the

company's brand and reputation. Not all cyber-policies cover costs of providing a breach notice, so be sure to check whether and how your policy will respond to these circumstances.

- *Limitations on the cost to investigate, defend, and settle issues surrounding civil penalties and fines.* While most cyber-liability policies cover civil fines or penalties imposed by a governmental agency, as well as the costs incurred in connection with a governmental investigation, some permit coverage only to the extent they are insurable by law in that jurisdiction. This coverage limitation raises questions of law not directly specified in policy terms. Policyholders should consult knowledgeable personnel in their corporate risk and legal departments, along with their other professional and legal advisors.

- *Breaches caused by rogue employees.* All policies have a specific "conduct exclusion" barring coverage for loss arising out of some improper conduct; however, these kinds of exclusion should be limited to dishonest, fraudulent, or criminal acts committed by the company or its senior management. While most data and security breaches result from negligent acts, such as failure to properly configure software or firewalls, many breaches are caused by malicious acts, perpetrated or assisted by insiders. Thus, companies should seek an exception to the conduct exclusion for "rogue" or disgruntled employees to guarantee coverage for malicious conduct by an insider. Moreover, the conduct exclusion for fraudulent or criminal acts of senior management should be worded to apply *only after final adjudication*, or determination, that the excluded conduct did, in fact, occur.

In addition, there are likely to be restrictions for restoration of intellectual property or proprietary business information. And when related coverage is provided, it typically is limited to the amortized value.

Another area to check involves the policy's requirements regarding use of vendors to address data breaches and related issues. Many insurers require policyholders to use the insurance company's preferred vendors and additional premium may be required to have this language changed to allow the purchaser of a cyber policy to choose its own vendors.

Determining How Much Coverage You Need

While there's no simple formula for determining how much cyber-liability insurance any company should purchase, there are three key considerations when choosing insurance policy limits and deductibles:

1. *What is the most likely total dollar amount of any particular risk?* Companies maintaining a significant amount of personal identifiable information, intellectual property, or highly confidential information either for clients or staff, may need higher limits. When evaluating appropriate limits, typically first-party costs incurred when a cyber-breach occurs include lost billing time, forensic investigation, legal fees to determine regulatory or notification obligations, notification, communication, public relations costs, credit monitoring, and regulatory fines and penalties.

   Third-party costs may include settlement or judgments for claims by third parties, legal fees to respond to a third-party loss, damages to network security of a trading partner or vendor, intellectual property infringement, and regulatory proceedings.

2. *How much of these costs can your company afford to retain, either by not purchasing insurance or through a deductible or retention?* Even if your company has multiple safeguards to prevent a cyber-attack, the risk exists and recovery cost can be substantial. In determining insurance needs, many companies consider the worst-case scenario.

3. *What are your business's contractual obligations?* Companies serving institutional clients may be contractually required to purchase certain minimum limits of cyber-liability insurance. Increasing numbers of clients, particularly financial institutions and health groups, for example, are requiring their counsel to carry this insurance.

As Internet and cyber-related risks become increasingly widespread and complex, managing these exposures requires a comprehensive approach that includes sound risk management practices and a careful evaluation of available insurance. Companies need to evaluate their coverage options carefully, identify potential coverage restrictions, and work with insurance companies to ensure that the coverage being sought is actually the coverage that is provided. ■

MEALEY'S DATA PRIVACY LAW REPORT
edited by Mark C. Rogers
The Report is produced monthly by

LexisNexis®

1600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA
Telephone: (215)564-1788 1-800-MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com
Web site: http://www.lexisnexis.com/mealeys
ISSN 2378-6892