New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
Litigation
An ALM Publication
WWW.NYLJ.COM
MONDAY, DECEMBER 15, 2014

Finding the Right Level Of **Cyber Insurance Protection**

BY ALAN R. LYONS

We have all seen the headlines. Every week it seems that cyber-criminals attack yet another major corporation. In September, Home Depot confirmed that hackers stole debit and credit card data for more than 40 million of its customers. With that attack, Home Depot joined a growing list of high-profile companies, including Michaels, P.F. Chang's, Wyndham Hotels, and Neiman Marcus, all of which have had sensitive customer data stolen or compromised via cyber attacks. Over the last year, these attacks have grown in their boldness, frequency and scope, and the collateral damage to corporations and consumers alike has been widespread.

Although data breaches affecting large, well-established companies have grabbed the headlines, a cyber attack can happen to any business, large or small. All businesses that conduct business online or store sensitive data on a network are susceptible, and the range of customer and employee data that could be exposed by a breach makes the potential fallout significant.

Like it or not, companies must be prepared for cyber attacks. That starts with having an up-to-date network security system to protect corporate data. But no security system, however state-of-the-art, is completely fail-safe. That's because hackers by nature are forward-thinking. They continually adjust their strategies and relentlessly look for even the slightest weakness to leverage to their advantage.

Beyond in-house data security systems, all businesses at risk of a cyber breach should consider purchasing cyber insurance. This insurance can play a key part of a company's overall protection against the significant financial and reputational consequences of a cyber attack, and help safeguard against losses stemming from data breaches, compu`ter hacking, computer viruses, theft of information and employee sabotage.

A wide variety of cyber policies and levels of protection are available. In short, no two policies are identical. Since the policy terminology can be confusing, it is recommended that a company obtain the advice of a qualified insurance broker and experienced legal counsel prior to the purchase of cyber insurance. This can help a company ensure that the scope of cyber coverage is tailored to meet its specific needs, including its size, sector, number of customers and type of data, and to avoid common insurance purchasing pitfalls.

The first step is for a company to determine if, and to what extent, it already has coverage

ALAN R. LYONS, *counsel with Herrick, Feinstein, represents both insureds and insurers in a wide variety of complex insurance coverage issues.*

for cyber risks under its existing "traditional" insurance policies, such as commercial general liability (CGL) and commercial property policies. In most cases, such an analysis will reveal insufficient, if any, coverage for cyber risks.

Since December 2001, standard-form CGL policies issued by Insurance Services Office (ISO) expressly state that physical damage and/or loss of use of electronic data are not covered as "property damage." In addition, standard CGL policies issued by ISO since December 2004 contain an Electronic Data exclusion for property damage "arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."

CGL policies also contain "personal and advertising injury" liability coverage, which includes injury arising out of "[o]ral or written publication, in any manner, of material that violates a person's right of privacy." Earlier this year in a landmark ruling, the N.Y. Supreme Court ruled that this language did not require Sony's CGL insurers to defend it in connection with numerous underlying lawsuits alleging violation of privacy arising from a 2011 cyber attack on Sony's PlayStation Network (*Zurich American Insurance v. Sony*, Index No. 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014)).

In that matter, the hackers stole personal and financial information from millions of PlayStation Network users. Judge Jeffrey K. Oing ruled that, although the large-scale data breach constituted a "publication" of private information, the data breach was not covered because the policy only covered publications made by Sony itself as the insured, not by third-party hackers. The court rejected Sony's argument that the phrase "in any manner," which qualified the word "publication," was sufficiently broad to encompass the actions of third-party hackers. Sony has appealed, and the decision of the Appellate Division First Department could have a significant impact upon coverage for cyber attacks under CGL policies.

Another pending lawsuit that could potentially limit the scope of coverage for cyber attacks under CGL policies was filed in October by Travelers against its insured, P.F. Chang's, in Connecticut federal court. In that case, Travelers seeks a declaratory judgment that it has no duty to defend or indemnify P.F. Chang's in connection with three underlying class actions arising from the restaurant's recent data breach. Travelers argues that the claims are not covered because the breach does not constitute "bodily injury," "property damage," "personal injury" or "advertising injury." Interestingly, Travelers' complaint alleges that P.F. Chang's is currently being defended in the underlying lawsuit pursuant to a separate cyber liability policy issued by a different insurer.

Companies are unlikely to find much coverage for cyber risks under their commercial property policies. Standard ISO policies exclude "electronic data" from the definition of "Covered Property," and instead provide coverage for "the cost to replace or restore electronic data which has been destroyed or corrupted by a Covered Cause of Loss" under an "Additional Coverage" subject to a sublimit of only $2,500. Although insurers may be willing to slightly increase this sublimit by endorsement, the increased sublimit will pale in comparison to the costs of responding to a data breach.

That said, some coverage for cyber-related risks may be available under a company's commercial crime policy. For example, in *Retail Ventures v. National Union Fire Ins. of Pittsburgh, Pa.*, 691 F.3d 821 (6th Cir. 2012), Designer Shoe Warehouse (DSW) was covered for cyber attack expenses incurred for customer communications, public relations, lawsuits, regulatory defense costs and fines imposed by Visa and MasterCard under the computer fraud coverage of its crime policy. This stemmed from a 2005 cyber attack in which hackers accessed DSW's computer system and stole credit card and checking account information from 1.4 million customers.

Although coverage for cyber risks may exist under some traditional insurance policies, they likely do not fully address cyber exposures in scope or amount. In addition, now that cyber-specific policies are available, some insurers are taking steps to expressly exclude cyber attack claims and losses from their traditional policies. For example, effective May 2014, ISO introduced new data breach exclusions available as endorsements for its CGL policies that exclude "personal and advertising injury" arising out of "any access to or disclosure of any person's or organization's confidential or personal information . . .."

Therefore companies should identify gaps in their existing coverage and consider filling them with cyber policies specifically tailored for their particular business, the data they manage and the risks that they face.

These cyber policies can provide both first-party and third-party coverage. First-party losses are those sustained directly by the insured company. Third-party losses are those sustained by others who assert claims against the insured company to recover those losses, and typically cover the insured against privacy liability and/or network security liability.

Privacy liability insurance covers the insured's liability to third parties arising out of its failure to protect personally identifiable or confidential corporate information in its care, custody or control. It can also provide coverage for regulatory proceedings and investigations brought by a government agency alleging the violation of privacy laws.

Network security liability insurance covers the insured's liability to third parties arising out of (1) the failure of its network security to prevent computer attacks, including unauthorized access or use of corporate systems, which results in deletion, corruption or theft of data; (2) a "denial of service" attack, i.e., an attack that makes a network unavailable to its intended users; and (3) the failure to prevent the transmission of malicious code.

Privacy and network security liability policies can cover the cost of defending claims, lawsuits, and/or regulatory proceedings and investigations resulting from a covered cyber event, and pay for covered judgments and settlements. Some policies also cover regulatory fines and penalties assessed against the insured.

First-party cyber coverage can cover certain types of expenses incurred by a company resulting from a data breach, including expenses to (1) retain a computer forensics firm to determine the cause and scope of a breach; (2) comply with privacy regulations; (3) notify and provide credit monitoring services to affected individuals whose personally identifiable information was compromised, including setting up call-centers to field enquiries from concerned customers; (4) retain legal counsel to respond to regulators; and (5) retain public relations and/or crisis management services to restore the company's reputation.

First-party policies can also include "Information Assets Coverage," which covers the cost to recreate, restore or replace the company's lost, corrupted or damaged software or data, and the cost to replace its damaged computer hardware. The policy may also cover business income loss sustained when business operations are interrupted or suspended as a result of a security breach. "Extortion" coverage is also available that covers payments made in response to a ransom or extortion demand to prevent a threatened cyber attack.

There are many questions and issues to consider when purchasing cyber insurance, the most important of which are discussed below. The advice of an experienced attorney and insurance broker can be invaluable in helping a company navigate this process.

What Type of Data Is Covered?

Data generally falls into three main categories: (1) personally identifiable information (PII)—a customer's/employee's name, date of birth, email address, Social Security number and ZIP code are likely the most valuable; (2) protected health information (PHI)—healthcare-based treatment information such as medical history, including many elements of PII in medical records; and (3) payment cardholder information (PCI), such as credit card data, including account numbers, expiration dates and security codes. Protected data can also include financial information such as bank, brokerage and insurance account information. It may also be important for a company to ensure its confidential corporate information is covered. Many companies possess valuable customer lists, marketing lists and other corporate information that could be beneficial to competitors and that may result in liability if compromised. If a company's data is not stored on its own system but on the system of a third-party vendor, it is vital to ensure that coverage is not limited to data stored on the insured's own system.

What Constitutes a Covered Data Breach?

For example, the policy should cover: (1) unauthorized disclosure of data, whether accidental or intentional; (2) unauthorized acquisition of data when the company's data ends up in the possession of an unauthorized third party; and (3) the compromising of data when data is corrupted, erased, altered or held for ransom.

What Are the Applicable Policy Limits?

An important consideration is obviously the overall policy limit. For third-party policies, defense costs may be included within, and therefore erode, the policy limit. In that event, the amount of anticipated defense costs must be factored in when selecting an appropriate policy limit. In addition to the overall policy limit, companies should also pay particular attention to whether the policy provides sufficient sublimits for legal, computer forensics, public relations and/or crisis management expenses. Many cyber policies include those coverages, but only at low sublimits. Those expenses can often be substantial, particularly the computer forensic expenses, and can exhaust the sublimits very quickly. Another consideration is whether the policy provides coverage for regulatory fines or penalties, and if so whether such coverage is subject to a sublimit.

Cyber policies may contain a separate deductible for each type of coverage. A single cyber attack may implicate several types of coverages, thereby triggering multiple deductibles. Some insurers may offer a coverage enhancement stating that one retention applies to the entire policy, instead of having to exhaust multiple deductibles.

Companies should consider the applicable "trigger of coverage" under the policy. Third-party liability policies can be triggered on a "claims-made" basis, which means that coverage applies to a claim first made against the insured during the policy period, or on a "claims-made-and-reported" basis, which means that the claim must also be reported to the insurer during the policy period. Alternatively, they may be written on an "occurrence" basis, which means that the breach must occur during the policy period regardless of when a claim is made against the insured. Another possibility is for coverage to be written on a "discovery" basis, which means that the policy covers a breach if it was first discovered by the insured during the policy period.

Does the Policy Include 'Prior Acts' Coverage?

Hackers often "footprint" a company for a significant period of time before they attempt to infiltrate its network (so-called Advanced Persistent Threats). This occurred in the Neiman Marcus data breach, which involved a hacker having access to its network for a long period of time. Without "prior acts" coverage, a company might be left with no coverage for this type of breach, as the insurer may determine that the cyber attack first occurred prior to the policy period. "Prior acts" coverage can be invaluable to cover a situation in which hackers gain access to the company's network prior to the policy period without the company's knowledge.

If the policy includes business income coverage, it is important to analyze whether coverage is triggered only by a complete "suspension" of business operations, or whether a mere "interruption" in business operations is sufficient.

Another important consideration with third-party policies is whether the insured or the insurer retains the right to select defense counsel to represent the insured in defending lawsuits. Many insurers insert a provision in the policy giving them that right. However, many insureds have long-standing relationships with law firms who are familiar with their business, and it is therefore important to check whether the policy allows the insured to select defense counsel.

What Are the Policy Exclusions?

The exclusions in the policy must be read very carefully. For example, companies should be wary of exclusions for attacks through unencrypted laptops or mobile devices. In today's modern business world, corporate employees routinely store data and sensitive information on laptops, tablets, cell phones and USB drives. Therefore, it is important that a cyber attack that uses mobile devices as the entry point is covered in the same way as a breach of a company's network system.

In addition, some policies may contain a "wild virus" exclusion, which means that coverage would only apply to a cyber attack targeted at the insured entity itself. However, many viruses circulating over the Internet are "wild" in nature and not directed at any particular entity.

The policy will likely contain an exclusion for criminal and/or dishonest acts by the insured. It is important for a company to ensure that this exclusion is limited to the acts of senior officers/directors so that criminal/dishonest acts by a rogue employee are covered.

To conclude, companies should invest the time and resources to make sure that they are buying the right type of cyber policy for their business, and to analyze the scope of coverage and policy language upfront. After hackers strike, it will be too late.