Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Cyberinsurance: Does Your Policy Have You Covered?


Bob Steinberg
Latham & Watkins LLP


Peter Rosen
Latham & Watkins LLP


Margrethe Kearney
Latham & Watkins LLP


Neil Rubin
Latham & Watkins LLP


Martha O'Connor
Latham & Watkins LLP

Law360, New York (May 07, 2014, 12:09 PM ET) -- As recent news reports confirm, cyberattacks present a growing risk to businesses and individuals that is not likely to go away soon. Although security technologies continue to improve and play an important part in defending against these attacks, the very nature of computer and network technology means that security technologies cannot detect or block every threat.

Even where technology is effective, it can often be undermined by trusted individuals who fail to follow proper procedures, are tricked into doing dangerous things or themselves have malicious intent. Because there are no silver bullets to solve this problem, organizations that face cyber-risks must approach them with serious, well thought-out strategies, combining effective technology, careful security practices and qualified and diligent people. They must also carefully plan for how to respond when the inevitable attacks do occur.

Insurance is an important tool for businesses in managing risks. Traditional business insurance products are unlikely to cover losses from cyberattacks; instead, businesses must turn to specialized cyberinsurance products to protect themselves. Companies at risk of financial loss from cyberattack should take a careful look at the available cyberinsurance products and consider whether these products can play a role in their plans for managing cyber-risks.

Every company has a unique cyber-risk profile and coverage should be tailored to address that profile most effectively. Cyberinsurance policies typically cover both first-party and third-party losses suffered as a result of a cybersecurity breach. However, the scope of coverage is increasingly refined and can be tailored to a variety of

risk scenarios. There are some unique features of cyberinsurance policies companies may not be familiar with and there are some important issues to consider when purchasing policies so as to minimize coverage disputes down the line.

First-Party Losses

Cyberinsurance policies typically include a variety of first-party coverage options. Two of these options that require careful consideration, and may be somewhat unique to these types of policies, are coverage for event management and business loss coverage.

Breach Remediation Coverage/Event Management

One of the unique aspects of cyberinsurance coverage is event management, or breach remediation coverage. This covers the direct expense of responding to a cybersecurity breach. Covered expenses typically include:

- Hiring an independent information security forensics firm
- Public relations
- Notification of affected parties (i.e., business customers and/or individuals whose data was accessed or acquired in the data breach)
- Credit monitoring for individuals
- Identity theft resolution services
- Call centers
- Costs to resecure, recreate and/or restore data or systems
- Legal services/advice
- Crisis management services
- E-extortion costs (i.e., company is forced to pay hacker in order to get data/access back)

The scope of event management coverage can vary among carriers. Policyholders should carefully assess those differences to insure adequate coverage and to minimize the potential for a coverage dispute. Form policies typically offer a menu of options, not all of which may be beneficial to the policyholder. For example, some policies require use of approved vendors to handle all breach response activities. Others require insurer agreement for any outside firm hired to advise the policyholder on breach response, especially with respect to attorney, investigator and public relations costs.

Sometimes losses are time-limited, typically about one year. Also, call centers are not always included in coverage and there is not developed case law that can guide policyholders as to whether call center costs might be covered under more general provisions. For example, it has yet to be determined whether call center costs could be considered “reasonable and necessary” costs of notifying persons who are affected by the breach.

Call centers can be a significant portion of the policyholder’s total response costs. For example, in response to the Black Friday data breach at Target Corp., the retailer had to triple its already robust call center staffing and keep the call centers open around the clock as well as on Christmas, which greatly increased the total costs of the breach. Some polices do not cover the cost of restoring, recreating or recollecting data as part of event management coverage — the cost of which could vary considerably depending on the manner in which the policyholder uses the data in its business operations.

With many carriers, the extent of event management coverage is negotiable and an expert broker can provide considerable assistance in these negotiations.

Network Interruption

Most policies offer coverage for loss of business income due to a breach that results in an actual interruption or impairment of the insured's business operations. The important distinction among the policies is the duration of such coverage. For example, one policy may cover loss of business income from the time the network interruption begins until some fixed period after the interruption ends. Other policies cover loss of business income until business operations are back to normal or 60 days after the insured's system is restored, whichever comes earlier.

The cyberinsurance market is not yet mature enough to have produced case law to guide policyholders on how these policy provisions terminating coverage when operations are back to normal will be read. Some policies have a "waiting hours" period that is written into an individual policy.

The waiting hours period would require some specified number of hours to elapse once a material interruption has begun before loss of business income is covered. A policyholder may want to consider this provision carefully. Depending on the nature of a company's operations, the initial hours of network interruption may significantly impact operations and could cause a substantial business loss. Again, each policyholder will need to assess its own potential exposure to determine the appropriate time span for coverage of business losses.

Other important first-party coverages that are typically offered in cyberinsurance policies are:

- Denial of service costs to business: These costs include loss of use and resulting business interruption. Coverage can be set as a per day amount or can be tailored to a company's specific loss. For example, losses to an online retailer would likely be higher on Cyber Monday than on Memorial Day.

- Losses resulting from misappropriation of the insured's information assets or confidential business information: Under some policies, losses related to misappropriation of intellectual property, trade secrets, company records, customer lists, company credit card numbers, budgets, proposals, work papers and any other proprietary or sensitive company data that results from a data breach are covered.

- Damage to systems: This could include losses resulting from damage to the insured's computer systems resulting from the breach. Some policies include coverage for the cost of restoring lost or compromised data.

- Disclosure of information: Some policies include coverage for damages in connection with the disclosure of information to a competitor.

- Intellectual property: Coverage could include expenses related to the restoration or recreation of intellectual property, including trademarks, copyrighted material and proprietary business information, up to amortized value.

- Fines/penalties: While the civil fines themselves are usually covered, some carriers may not offer coverage for costs to investigate, defend and settle fines.

Third-Party Losses

Cyberinsurance policies can vary even more radically with respect to third-party losses. Important considerations

include the degree to which defense costs will be covered and what type of third-party damages are included in coverage.

Defense Costs and Third-Party Damages

Cyberinsurance policies usually offer some type of coverage for third-party claims based on a failure to protect confidential information. However, some also offer coverage for the insured's failure to disclose a breach in accordance with privacy laws and in violation of privacy statutes.

Given the proliferation of statutes and regulations governing data privacy, such coverage may be increasingly valuable. Some policies cover not only injury incurred by a third party due to loss of use of its own system that was a result of the cyberattack on the insured, but also injury to the third party caused by an inability to access the insured's system.

Depending on the nature of the insured's business, third-party system losses could be considerable. For instance, if a retailer could not access the database of its third-party email marketing provider, and the retailer was unable to send out advertising to its customer base in advance of an important sale, the resulting losses could be significant. Not all policies include coverage for losses resulting from reputational injury, but many offer purchase of an additional coverage section to cover those types of losses.

Other important third-party coverages that are typically offered in cyberinsurance policies are:

- Defense costs: These costs include attorney fees and expert fees for outside claims made against an insured related to a data breach.
- Media liability: This provides coverage for losses related to libel, slander, defamation and other media torts, as well as copyright, trademark and patent infringement. This can include losses resulting from information posted to social networking sites, such as Facebook Inc. and LinkedIn Corp.
- Data and personal identifiable information ("PII") loss: This covers losses or breach of a third-party's data, including the dissemination of PII. One example would be if confidential third-party information, such as Social Security numbers or passwords, was used to breach the third-party's data. Policies define PII differently in the absence of an industry-standard definition.
- Fines and penalties: These include fines that may be assessed under state privacy statutes as well as under federal privacy regulations.

The above lists are not exhaustive, but they do cover the primary offerings under policies currently in the market. Carriers may offer additional coverage, especially for companies with specialized risks. In addition to securing appropriate coverage, policyholders should confirm that this coverage is not subject to any policy exclusions.

Cyberpolicy Exclusions

As with commercial general liability policies, cyberpolicies often contain a host of exclusions. Agreement on the wording of many of these exclusions — and therefore their scope — are an important part of the negotiation process.

Possible exclusions from cyberpolicies should be carefully noted and, if feasible, negotiated. Because many of these exclusions have not been the subject of litigation, policyholders lack the benefit of judicial interpretation when assessing the boundaries of coverage. The relative lack of analysis cautions towards careful and creative evaluation of the scenarios in which exclusions may apply.

Examples of exclusions to keep in mind during negotiations include:

- Contractual liability exclusion: This exclusion typically functions to exclude coverage for any liability assumed by an insured under a contract or agreement. To the extent a third-party claim can be styled as breach of contract, this exclusion may come into play. In some cases, this exclusion can be limited to situations where, but for the contract, the policyholder would not be liable for losses. As discussed more fully below, data vendors who have contracts in place with third parties that address confidential information should pay close attention to the language of the contractual liability exclusion during the negotiation process.

- Criminal conduct exclusion: Many policies contain exclusions for criminal or fraudulent acts by the insured. Companies with call centers should carefully negotiate this exclusion, given the abundance of criminal eavesdropping statutes that could apply.

- Exclusion for unauthorized collection of customer data: Some policies contain exclusions for losses related to data whose collection was not authorized. Companies engaged in online activities, especially activities in which consumer financial data is collected, could find this exclusion at play. Indeed, for some companies, the collection of data is central to their business, and this exclusion could present a significant bar to coverage.

—By Bob Steinberg, Peter K. Rosen, Margrethe K. Kearney, Neil A. Rubin and Martha L. O'Connor, Latham & Watkins LLP

Bob Steinberg and Peter Rosen are partners and Neil Rubin is an associate in Latham & Watkins' Los Angeles office.

Martha O'Connor and Margrethe Kearney are associates in Latham & Watkins' Chicago office.