A Desk Guide to Data Protection and Breach Response - Part 3

February 27, 2014 Leslie Thorne, Micah Skidmore

PRACTICES Healthcare Transactions and Regulatory, Privacy and Cybersecurity, Energy, Power and Natural Resources, Social Media, Finance, Government and Public Policy, Government Contracts, Healthcare and Life Sciences, Insurance Recovery, Intellectual Property

Insurance Coverage for Cyber Attacks: What Do You Need in a Cyber Liability Policy?

With more and more businesses suffering costly data breaches and cyber attacks, companies should utilize every tool they have to shift the potentially enormous expenses associated with those breaches and attacks. That?s where insurance comes in. Companies can potentially shift some expenses under the traditional business policies - such as general liability, commercial property, crime/fidelity, and errors and omissions - but they are increasingly looking to specialized ?cyber liability? policies for more fulsome coverage.

Cyber attacks come in myriad forms. Depending on the type of attack, trade secrets, personal customer or employee information, or even entire computer systems may be compromised. While every policy is different, cyber liability policies typically protect the insured against its own direct losses (first party coverage) as well as their liability for the losses of others (third party coverage). Depending on the policy, cyber insurance may cover:

- Forensic investigation and system restoration;
- Defense and indemnity costs associated with litigation resulting from the loss of personal information or other sensitive data;
- Defense costs and penalties associated with regulatory investigations;
- Notification costs and credit monitoring for affected customers and employees;
- Losses attributable to the theft of the policyholder-company?s own data (including transfer of funds);
- Business interruption costs attributable to a cyber attack;
- Costs required to investigate threats of cyber-extortion and payments to extortionists; and
- Crisis management costs, such as the hiring of public relations firms.

It is critical to carefully review the particular provisions of each cyber liability policy with a broker and coverage counsel. Unlike many traditional policies, cyber liability policies differ significantly because they are not (yet) based on a standard form.

The first rule in choosing the right policy is to match the company?s unique risks to the risks covered by the policy. Coverage needs vary significantly depending on the type of organization, the type and amount of personal information it holds, and many other factors. A credit card company, for instance, may have vastly different needs than a hospital system or a utility company. Likewise, companies with a public profile may have a much greater need for extortion coverage or crisis management coverage than a smaller, lesser known business. Companies that fail to thoroughly understand their own needs often inadvertently purchase policies that (1) have gaps in coverage and/or (2) include unnecessary coverage.

While companies should work closely with their brokers and counsel to choose the right policy, would-be policyholders should particularly watch out for:

- **Provisions identifying who is an ?insured? under the policy.** Typically, the policyholder would want to include both the organization itself and any other individuals or entities (including independent contractors or other third parties) responsible for the organization?s network security.
- **Sublimits.** Some policies, despite providing significant overall coverage, cap the amount they will pay for certain categories of liability, such as notification costs.
- **Who gets to choose the lawyers, PR firms, investigators, or credit monitoring companies.** Some polices require that the policyholder use the carrier?s approved vendors.
- **Late retroactive dates.** Policyholders should negotiate early retroactive dates, meaning the policy will cover breaches that occurred long before the policy was purchased, but were not discovered until after coverage took effect.
- **Exclusions for Payment Card Industry (PCI) breaches.** If your organization suffers a breach involving customers? credit card numbers, this type of exclusion could be catastrophic.
- **Provisions that exclude or limit coverage for regulatory actions.** Regulatory agencies such as the Federal Trade Commission and the HHS Office for Civil Rights are becoming increasingly aggressive in pursuing data security-related actions (see our coverage of increasing SEC scrutiny of cybersecurity disclosures **here** and our article regarding a recent lawsuit by the California Attorney General claiming unnecessary delay in disclosing a breach **here**). Companies that could be subject to regulatory actions should avoid policies that have these exclusions.
- **Provisions that exclude fines and penalties.** Depending on the organization?s specific needs, it may need coverage for penalties assessed under the Health Insurance Portability and Accountability Act of 1996 (?HIPAA?), the Gramm-Leach Bliley Act (?GLBA?), the Health Information Technology for Economic and Clinical Health (?HITECH?) Act, and other similar state and federal laws.
- **Provisions that exclude coverage for third party vendors.** If the company uses third parties to gather, store, or process data, these exclusions could obviously present serious problems.
- **Exclusions barring coverage if the insured ?should have known or anticipated? the breach.** Such provisions often lead to coverage disputes as to who should have known what and when.
- **War exclusions.** These exclusions bar coverage for losses arising from ?acts of foreign enemies.? Many cyber attackers are foreign nationals and some allegedly act at the behest of foreign governments.
- **Exclusions for the misappropriation of trade secrets or other intellectual property.** Some policies exclude coverage for damages stemming from a cyber-attacker?s misappropriation of trade secrets. Such exclusions need to be tailored to avoid unintended consequences.
- **Exclusions for claims alleging unsolicited electronic dissemination of faxes, emails or other communications.** Such exclusions should be modified to specifically except claims based on distributed denial of service (?DDoS?) attacks perpetrated using the insured?s systems.
- **Insured vs. insured exclusions.** Given the potential for employee claims alleging the disclosure of personal information, exclusions barring claims brought by one insured against another can be problematic.

- **Breach of contract exclusions.** Carriers may invoke these exclusions when a customer sues based on an alleged breach of his personal information, arguing that the insured held the information under a service contract.
- **Exclusions for loss of information on unencrypted devices.** With many employees carrying sensitive information on their home computers and handheld devices, companies should consider the potential risk associated with the portable nature of certain information.

Every policyholder is unique, meaning some of these issues may not be important to a particular policyholder. But by being aware of these and similar concerns, policyholders and their brokers will be able to negotiate the policy that best meets their needs and minimize coverage disputes when claims arise.

In earlier installments of our special series, A Desk Guide to Data Protection and Breach Response, we discussed

- ***data protection and compliance issues* and**
- ***developing a data security plan*.**

In future installments, we will discuss how best to investigate and respond to a data breach, regulatory actions, fallout litigation, and how to maximize insurance recovery after a loss. For additional information on any of these subjects, please contact a member of the Haynes Boone Privacy and Data Breach Group.