CYB Cyber Liability

Q&A

What is Security Breach Response Coverage?
This first-party coverage reimburses an Insured for certain costs incurred due to a security breach of personal, nonpublic information of their customers or employees. Examples include:

The hiring of a public relations consultant to help avert or mitigate damage to the Insured's brand
IT forensics, customer notification and 1st Party legal expenses to determine the Insured's obligations under applicable Privacy Regulations. Credit monitoring expenses for affected customers

What is "PCI-DSS Assessment" coverage?
The Payment Card Industry Data Security Standard (PCI-DSS) was established in 2006 through a collaboration of the major credit card brands as a means of bringing standardized security best practices for the secure processing of credit card transactions. The coverage provides for fines and penalties assessed by this governing body.

Are notification costs covered on an individual basis or on a limit basis?
Trick question! It depends on the carrier. Some carriers such as Beazley provide notification expense on a per individual loss basis, while other carriers provide this expense coverage with an aggregate limit loss.

Claims-Made form or Occurrence form?
Cyber in general is on a claims-made form.

How much cyber liability insurance should I buy?
The first step in the process of deciding what limit of insurance you want to buy is conducting an exposure analysis, including data analysis where possible. Part of the work here is understanding which parts of your exposures are insurance and which parts are not. For example, there is an abundance of "breach calculators" that purport to help companies understand the cost of a major exposure event, but many of these calculators are over-inclusive if you are thinking about your insurance exposure. We recommend talking through your exposures with a trusted advisor, and using third-party data where available and relevant.

Is it difficult to obtain cyber liability insurance?
It is not difficult, but the application process involves some work. There is an information-gathering phase that is likely to involve questions for not only your IT and network security teams, but also for finance and legal. It is a good idea to pick one person to quarterback the entire process.

Insurance carriers will want to know how robust your systems are, what your ability is to detect a potential problem, and how quickly you can resume operations after a security incident. After the first round of questions, carriers may well come back with more questions.

In the end, you may have several different quotes from various carriers. You will want to work with your skilled insurance broker, and in some cases outside counsel, to compare the various options your broker has been able to negotiate on your behalf.

These scenarios are not intended to be interpreted as coverage positions. Coverage for any given claim is based upon its facts and the specific terms and conditions of the policy.

CYB Cyber Liability

Q&A

Why would you want cyber insurance?

As an enterprise, you have data to protect. If that data includes credit card information, personal health information (PHI) and/or data that would be considered private by its owners, then the breach or loss of that information could result in substantial costs to the company, including remediation, compliance penalties and loss of business or corporate reputation damage. Even for organizations that keep a contingency fund, the costs can quickly become overwhelming.

Essentially, cyber insurance provides protection for the enterprise from the following types of specific costs:

- **Cost per record breached:** The Ponemon Institute calculated that a company can expect to pay approximately $214 per breached record.
- **Breach notification:** Simple mailings to affected customers can run around $1 to $3 per person.
- **Customer credit monitoring:** Credit monitoring offered as a remedy to affected customers can run around $20 to $100 per person per year.
- **Post-breach forensics:** Forensic examinations can result in extensive costs, from thousands to hundreds of thousands of dollars.

While each one of these actions has a cost, it is also important to remember that the costs associated with repairing a damaged reputation may be prohibitively expensive as well. Therefore, a cyber insurance policy may be of superior benefit to a company susceptible to suffering a data breach both financially, as well as managerially, for the peace of mind it can offer the CEO and board of directors should a breach occur

Suppose a company already has a General Liability or other traditional business policy (D&O, E&O, Crime, etc.). Do any of these coverages offer protection against cyber losses?

E&O policies can include Cyber Liability coverage. The remaining lines of insurance typically do not cover any type of Cyber related loss.