insuranceday
www.insuranceday.com

Protecting against cyber risk: a primer on cyber insurance

As the number of high-profile data breaches grows, US companies are looking to insurance solutions

Thomas Bentz
Holland & Knight

There has been no shortage of stories about massive data breaches this year. From Target to The Home Depot, it seems like a new cyber event is reported nearly every week. As these stories continue to grow in number, corporate America has started to explore ways to insure against this risk.

Cyber insurance is a relatively new concept. The first policies did not appear until the late 1990s and there have been constant changes to the forms and the protections offered ever since. Today, there are close to 25 insurers that offer some type of cyber risk coverage. However, the coverage provided varies wildly between different insurers. In addition, the market is in flux, with new coverage and new forms appearing nearly as often as new cyber claims are being reported.

Because there is so much difference in the coverage, it is imperative insureds understand what coverage they need, what coverage is being offered and what risks they will need to self-insure against even after they purchase coverage. It cannot be stressed enough that comparisons of cyber policies based on price alone are nearly meaningless for this line of coverage.

Cyber insurance policies are typically split into first- and third-party coverage.

First-party coverages

Forensic investigation coverage pays the insured for costs and expenses related to determining whether a cyber attack has occurred, how it occurred and how to stop the attack/loss of data.

Data loss and restoration coverage covers physical damages to computers (and related items), including the costs of retrieving and restoring data, hardware, software or other information damaged or destroyed in a cyber attack.

Network business interruption coverage covers lost income and operating expenses due to a material interruption or suspension of an insured's business caused by a network security failure.

Cyber extortion coverage protects against hackers who attempt to extort money by threatening to release sensitive information/data if a ransom is not paid, as well as for hackers who attempt to hold a network or data on the network hostage.

Theft and fraud coverage covers losses related to the loss or destruction of the insured's data as a result of criminal or fraudulent cyber attacks.

Third-party losses

Notification costs/credit monitoring costs covers costs related to notifying customers and others about the cyber event, as well as mandatory credit/fraud monitoring expenses. Recent estimates benchmark this cost at close to $188 per record.

Litigation expenses covers defense costs, judgments, settlements and related liabilities caused by plaintiffs who bring suit against the insured for various theories of recovery arising from the data breach.

Defence of regulatory proceedings covers defence costs to prepare for and defend against regulatory proceedings including legal, technical and forensic work. Some policies also cover certain fines and penalties that may be assessed against the insureds, as well as costs related to responding to government inquires about the cyber event.

Crisis management costs covers crisis management and public relations expenses to assist in managing and mitigating a cyber event.

Online defamation and copyright and trademark infringement covers costs related to claims of defamation, copyright and trademark infringement.

Many policies today also offer IT assessment services, training and compliance forums and even sample policies to respond to a data breach. Some insurers also offer a suite of expert consultants to assist with crisis management, legal responses and forensic work.

It is important to remember cyber policies are not the only place where an insured might find coverage for a cyber event. Depending on the losses and/or allegations, several other types of insurance policies may also respond to a cyber-related claim.

Directors' and officers' (D&O) liability: one of the largest potential exposures in the wake of a cyber event has turned out to be derivative actions against the board of directors for failure to exercise proper business judgment in preparing for or dealing with a cyber event. These types of derivative claims can be covered under a D&O policy. Other third-party claims against the directors and officers of the insured company may also be covered by a D&O policy;

Commercial general liability (CGL): many CGL policies offer at least some coverage for a cyber event. For example, they may cover invasion of privacy or privacy/confidentiality allegations. Earlier this year, however, the standard CGL form was changed to add an exclusion for cyber events. This may limit the amount of coverage available under a CGL policy;

Fiduciary liability: certain provisions of the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act require prompt notice of a cyber event and provide for penalties in the event of a data security breach. A strong fiduciary liability policy may respond to some of the notice expenses as well as certain penalties from a cyber event; and

Other lines: some other lines of coverage may also provide some limited protections against a cyber event including employment practices liability, crime coverage and technology errors and omissions coverage. Arguments can be made for coverage in each of these types of policies depending on the nature of the claim and the scope of the coverage purchased.

Co-ordinating cover

One of the most difficult things about a cyber event is co-ordinating the various types of coverages. Co-ordinating limits, retentions/deductibles and other coverage requirements can be difficult. In addition, because multiple types of policies may apply, there may be problems co-ordinating defence counsel (different insurers may not approve of a firm required by another insurer or there may be disagreement between insurers about "reasonable" hourly rates). The "claims-made" natures of many of these policies also can present problems for insureds in the event of a claim. Insureds are well advised to co-ordinate their coverage in advance.

Cyber insurance is still evolving. Insureds must take the time to learn what cover they need and what cover they have to ensure they are adequately protected. In addition, insureds should have a plan in place to deal with the complexity of having multiple lines of cover that may apply to a single cyber event. A little preparation can avoid significant problems with the coverage in the event of a claim. ■

Thomas Bentz leads Holland & Knight's D&O and management liability insurance team