Buying Cyber Insurance Protection in a Fast-Evolving Market

By Joshua Gold and Cort T. Malone

The authors explain that before purchasing such insurance, it is important that companies examine what coverage they have under traditional insurance policies and identify where potential coverage gaps might exist.

The Cyber Hits Just Keep Coming

Joshua Gold

As if anyone needed a reminder about the cyber risks facing virtually every individual and every business, there has been a rash of recent data breaches – all very serious in nature. These risks – and the fact that they are trending up, not down – underscore the fact that smart cyber risk management is essential. As part of risk management for cyber security, it is critical that businesses figure out what their insurance needs are. This is easier said than done, because the cyber insurance market continues to change in many significant ways. The insurance marketplace has expanded greatly for dedicated cyber insurance policies for both "first-party" risks (e.g., breach notification costs) and "third-party" risks (e.g., class action litigation defense and indemnity).

The Department of Homeland Security and lawmakers have issued warnings recently regarding the need for businesses to do a better job of minding the store when it comes to data security. Indeed, it was reported that lawmakers recently asked the United States Securities and Exchange Commission to beef-up disclosure responsibilities about cyber risks and preparedness for the benefit of investors. This prodding is important as attacks against U.S.-based corporations rise – not just for data theft but also for data destruction and alteration.

Cyber thieves recently stole $45 million from ATMs in a coordinated plot spanning numerous countries. But it is not just money that cyber thieves crave. A recent report indicated that computer hackers in Asia accessed and copied several U.S. weapons designs. Other cyber attacks have sought to degrade data or shut down key infrastructure altogether.

Cort T. Malone

A few months ago, a survey indicated that about 30 percent of corporate general counsel believe that their companies are unprepared to deal with a serious data breach. That's a sobering figure that should cause in-house lawyers, risk managers and IT departments to stop and think about their own company's preparedness for such issues. While data security presents daunting challenges for most, there are basic steps that businesses can pursue to protect against the worst cyber perils. A smart blend of careful contracting, insurance coverage, due diligence, and follow-up with employees can assist greatly in reducing the risks associated with data security breaches. Below, we focus on the insurance issues.

Joshua Gold is a shareholder in the New York office of Anderson Kill & Olick, P.C. Mr. Gold regularly represents policyholders in insurance coverage matters and disputes concerning liability, arbitration, time element insurance, electronic data, and other property-casualty insurance coverage issues. Cort T. Malone, a member of the Editorial Advisory Board for ***FC&S Legal: The Insurance Coverage Law Center***, is a shareholder in the Stamford, Connecticut, office of Anderson Kill. Mr. Malone's practice focuses on insurance recovery and corporate and commercial litigation. The authors can be reached at jgold@andersonkill.com and cmalone@andersonkill.com, respectively.

Risk Management through Insurance

Breaches in data security can lead to a slew of different losses. In the wake of a cyber incident, significant expenses can be incurred in defending class action litigations, indemnifying those who have a stake in disclosed information, and responding to state attorneys general, the Federal Trade Commission, and the Securities and Exchange Commission. Also, costs can be significant in investigating cyber breaches and complying with notification laws. Cyber incidents can also affect profitability when an incident interrupts business and systems need to be taken off-line or security needs to be re-developed.

It is not unusual for a computer security breach to cost a company millions of dollars in loss and exposure. A severe breach can lead to catastrophic losses in the eight and nine figure ranges. Risk transfer through insurance can therefore be quite valuable.

Over the years, many different types of insurance policies have provided some measure of protection for cyber-related perils. Several years ago, many of the broker-form all-risk property policies defined "physical loss or damage" in their insuring grants to include destruction, distortion and corruption of computer data, programming and hardware. General liability policies also contained broader advertising and personal injury coverage sections which could and did cover domain name disputes and breach of privacy class-action litigation arising from a computer hack. Crime insurance policies often contained insurance coverage for computer fraud losses. Business package policies also occasionally covered data losses and other related perils.

In recent years, however, the insurance industry has added new and broader exclusions to avoid claims under many business insurance policies. The industry aims to require the purchase of cyber-specific first and third-party insurance policies for those policyholders seeking to insure the risk. There is a good deal of variation between insurance companies' products right now, so policyholders are well advised to pick carefully.

The good news is that the insurance market for policyholders shopping for cyber specialty policies is more competitive than it ever has been and this means more flexibility and coverage options than was the case five years ago. Despite this, insurance policies and terms are still unnecessarily complicated, and businesses would be well advised to closely examine proffered policies to determine whether grand promises of coverage are undermined by fine print stuck in the exclusions, definitions and conditions sections of the insurance policy.

Insurance Coverage Issues

As always, mind that fine print. Insurance companies often contest claims on the basis of hard-to-digest exclusionary language. It's important both to use due diligence to avoid buying policies with the most broadly written exclusions and to be prepared to push back if coverage is denied on the basis of overly broad interpretations of such exclusions.

Below are a few issues to work out with underwriters at point of purchase – not point of claim.

Exclusions for Terrorism, Hostilities

Many cyber insurance policies contain exclusions for terrorism, "hostilities (whether war is declared or not)" and claims arising from "acts of foreign enemies." Given that many cyber attacks and breaches are believed to originate in foreign countries and some of those are further believed to be at the direction of foreign governments, policyholders must decide whether such exclusions make the cyber coverage unsuitable for their needs. This question may be especially germane if the policyholder is in a key infrastructure industry, defense industry or technology sector. Policyholders need to measure the policy terms they are presented with against the coverage they need before binding coverage.

Exclusions for Contractual Liability

Some cyber insurance policies purport to exclude coverage for "any guarantee, warranty, contractual term or liability assumed or accepted by an Insured under any contract or agreement." Exclusions of this type have been misused a good deal by certain insurance companies in the past to contest valid claims. "Contractual liability" exclusions are particularly problematic in the cyber insurance realm because many policyholders that may experience a data breach will have contractual relationships with merchant banks, credit card companies, investors, and other business partners. In such situations, insurance companies may try to argue that such exclusions bar coverage otherwise available under the cyber policy. Some insurance companies will also argue that breach of contract damages do not constitute a covered "loss."

Even if the cyber insurance policy provides a carve-out from the exclusion for scenarios in which the policyholder may have liability absent the contract relationship and terms, policyholders are still regularly forced to refute creative arguments about legal doctrines that are not supposed to apply to determinations over insurance coverage. These types of exclusions therefore need

to be either eliminated or greatly narrowed in their potential application so as to avoid unwelcome disputes over coverage when it is needed most.

Unauthorized Collection of Data Exclusions

Some cyber insurance policies contain exclusions for the "unauthorized" collection or gathering of information. For policyholders engaged in some forms of online business activity, such an exclusion can be problematic. For instance, it was reported last month that the FTC warned several data brokerage firms that their practices of gathering and selling consumer information potentially violates the Fair Credit Reporting Act. Other companies have been accused of having kept consumer credit card transaction data for too long after the transaction was complete. Policyholders that gather information for consumer transactions, marketing purposes, or as part of their core business model must gauge how an exclusion for unauthorized collection might be used by an insurance company to evade insurance coverage for a claim.

Pollution Exclusions

Cyber insurance policies may also contain exclusions for "pollutants." Again, depending upon the industry that the policyholder is in, such an exclusion may be problematic or lead to an unnecessary dispute over the scope of coverage for a claim. Given that cyber attacks are increasingly aimed at key infrastructure, it is possible that a cyber attack could implicate "pollutants." Insurance companies have been very aggressive over the years in urging a broad application of pollution exclusions to go far beyond industrial polluters. Accordingly, depending upon the policyholder's industry, imposition of an exclusion for "pollutants" may require a conversation at your underwriting meetings.

Violation of Statute, Rule, Law, or Consumer Protection Law

Some cyber policies have exclusions that seek to restrict or void coverage where the policyholder has violated a statute, rule, law or order of a regulatory agency. There are many variations of such exclusions and it is important that your insurance broker either eliminate such exclusions or at least find a policy that has the most palatable one available. It is not uncommon after a serious data breach or cyber attack that regulators and others assert that the policyholder's data handling and conduct violated state or federal law.

Untested Policy Language

Policyholders need to stay vigilant as they seek out the best insurance solution available to them to transfer the risk of cyber liabilities and losses. Almost all of the cyber insurance policy terms and forms are untested in court. That is likely to change in the future as more of this insurance is purchased and insurance companies start taking a harder line on claims.

While policyholders will have numerous grounds to counter the policy exclusions cited above should a claim dispute arise over them, it is better not to have the dispute in the first place. Accordingly, policyholders should be diligent in securing the most favorable insurance terms they can. It is also important to steer clear of foreign law and foreign mandatory arbitration clauses that sometimes creep into cyber insurance policies. Those clauses are not inserted in the insurance policies by accident.

Conclusion

There are now more options than ever to protect against cyber losses via dedicated specialty insurance. Before purchasing such insurance, however, it is important to examine what coverage the business has under its traditional insurance policies and identify where potential coverage gaps might exist. Make sure as well that coverage will be available – whether under cyber policies, business package policies, errors and omissions policies, or crime bonds/policies – when cloud computing services are used. Most insurance coverage can readily be adapted to expressly cover cloud computing risks. Bottom line is that the insurance coverage should match the cyber exposure of the policyholder so that coverage is as comprehensive and protective as possible. That's the point of insurance, after all.