The Metropolitan
Corporate Counsel®
National Edition
www.metrocorpcounsel.com
Volume 22, No. 9 September 2014

10 Tips For Enhancing Insurance Recoveries For Cyber Claims

Joshua Gold

ANDERSON KILL

The Massive & Ever-Increasing Risk

2014 has seen one massive data breach after another, affecting industries and organizations of every type. One recent report indicated an Eastern European cyber-crime gang by itself has hacked 1.2 billion username and password combinations. Another report indicated that there are more than 350 million stolen credit card credentials available for purchase in underworld markets. And tellingly, identity theft continued to be the number one consumer complaint tracked by the Federal Trade Commission.

Understandably, most insurance and risk management effort with regard to cybersecurity has focused on the immediate losses occasioned by data breaches. These include paying for the almost instant costs of state notification law compliance, forensic investigation, call centers, and defense of class action suits predicated on violation of privacy rights. But there are other areas of data breach-related losses that are expensive and should be addressed through insurance coverage where possible. Most policyholders will want insurance coverage to respond to inquiries, suits and formal investigations by regulators and law enforcement following a breach. Many policyholders will also want to have coverage for the reimbursement of fraudulent account charges if credit card, banking or brokerage accounts are pilfered.

Joshua Gold

A Market In Flux

Businesses and other organizations will in turn need to figure out their insurance needs and options. This is easier said than done, because the cyber insurance market remains in a state of flux. The marketplace has expanded greatly for dedicated cyber insurance policies covering both "first-party" risks (e.g., breach notification costs) and "third-party" risks (e.g., class action litigation defense and indemnity), with lots of different insurance companies all over the world getting in on the action.

But be careful – there is little uniformity in the insurance products, and many of the policy forms are almost incomprehensible. Complicating matters, many different types of insurance policies have historically provided some measure of coverage for cyber-related perils. All-risk property policies, general liability policies, and crime insurance policies often contained (and often still contain) some level of insurance coverage for computer-related losses. Business package policies also occasionally cover data losses and other related perils. Nonetheless, policyholders need to take a careful inventory of coverage as the insurance industry has added exclusions to attempt to push claims toward other insurance products.

With these factors in mind, below is our list of 10 tips for policyholders to consider in maximizing the chance of an insurance recovery from cyber-related losses.

1. Make sure your insurance matches the way you conduct online business and process data. For example, there are insurance coverage implications if you use cloud computing or other computer vendors for hosting and processing data. Many of the cyber risk insurance policies available today can be tailored to reflect the fact that the policyholder may delegate to third parties data management and hosting.

2. Do not rule out coverage for a claim under traditional business policies. If a cyber loss occurs, consider D&O, E&O, property, crime and GL insurance coverage depending on the claim against your company or the form of loss. We have had success in securing coverage under traditional lines of coverage such as E&O, crime and GL coverage.

There are also insurance policies that are something more than so-called "traditional" commercial insurance policies and something less than "cyber insurance." For example, in a case hot off the presses at the time of this writing, a policyholder won coverage for defense costs from a class action suit where the policyholder had allegedly allowed online access to sensitive health information of patients. *Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, LLC.* The insurance companies argued that although they covered electronic publications of information, there was no "publication" merely because the health information was searchable and accessible online. The federal district court presiding over the case rejected the insurance company's arguments and held that it had to defend its policyholder for the class action suit. The court rejected the argument that actual access of the sensitive data had to be shown and ruled instead that: "the issue is not whether a third party accessed the information because the definition of "publication" does not hinge on third-party access."

3. Avoid cyber insurance policy terms that condition coverage on the policyholder having employed "reasonable" data security measures. These clauses are so vague and subjective that they are bound to lead to

Joshua Gold *is a Shareholder in the New York office of Anderson Kill. Mr. Gold is also Chair of the firm's Cyber Insurance Recovery Group. He regularly represents policyholders in insurance coverage matters and disputes concerning contractual liability, arbitration, time element insurance, electronic data, marine, and other property-casualty insurance coverage issues.*

Please email the author at jgold@andersonkill.com with questions about this article.

coverage fights. Further, given the lightning speed of technological innovation and amorphous nature of cyber risks, a cybersecurity practice that was reasonable just months ago may look reckless with the benefit of hindsight and the passage of time.

4. If you possess or process consumer or business credit card information, make sure that you have insurance coverage for fraudulent card charges and credit card brand assessments and fines; these can be large exposures when there is a significant data breach.

5. If you do business with individual consumers and obtain their personal identifying information, make sure you have coverage (including attorney fees coverage) for the inevitable expenses of responding to informal inquiries and formal proceedings that ensue from state attorneys general, the FTC, and others when a breach occurs (often implicating residents of several states).

6. Make sure that your insurance covers breaches arising from mobile devices that may or may not be connected to the company's computer network. More and more employees can access systems through tablets, smart phones, and PCs. The ever-growing size of hard drives and ubiquity of portable drives mean that some employees may create security risks, even when the device is not logged onto the company servers.

7. Complete insurance applications carefully, including D&O applications. Underwriters will be focusing more and more on computer risk areas, and insurance application responses often are used against policyholders to contest insurance claims.

In this environment, added care must go into reviewing all D&O insurance policy terms and endorsements (including those contained in the primary, excess layer and Side A policy forms) at inception and renewals. It is likely that some insurance companies will try to insert exclusions into D&O policies just as they do into other policies (even into dedicated cyber policies). Many of these terms are vague and destined to lead to disagreements over their effect on the scope of insurance coverage for a cyber-related claim.

Given the steady barrage of daunting headlines over data breaches and data breach-related lawsuits against officers and directors filed this year, some D&O underwriters will no doubt inquire via insurance applications into their customers' cybersecurity awareness and preventive measures. As with all questions on insurance applications, it is vital to address these questions carefully.

Also, make sure that you are careful with your D&O insurance reporting of claims and circumstances after an incident. Many a legal battle has broken out with insurance companies arguing over claim notice provisions, first inception date clauses, retroactive dates, and so on. If all that fails, an insurance company may still argue "known risk," "known loss" and "policy rescission," even if the positions are beyond frivolous.

8. Avoid cyber insurance policies with broad or vague exclusions, including contractual liability exclusions. Contractual liability claims often are made in conjunction with statutory claims, negligence claims, and other forms of relief.

Even if such exclusions are present in your insurance, they may not apply, or if they are applicable, they may only apply to a small portion of the overall loss. Note that the law of most states holds that exclusions are to be construed narrowly. For example, in a recent case, *Bank of Rhode Island v. Progressive Cas. Ins. Co*., the court rejected an insurance company's argument that breach of contract damages against the policyholder-bank were not covered, finding that the tort and breach of contract damages against it were "indivisible." The court also had to address the insurance company's arguments over whether coverage was barred by an Internet services exclusion. The court held that despite the presence of the "Internet services exclusion," the policy's allocation clause would likely lead to a finding of coverage for "significant" portions of the damages awarded in the underlying suit against the policyholder. Since the effect of exclusions (including breach of contract exclusions) on a loss is a recurring insurance company defense in many D&O, E&O and even general liability insurance cases, the above decision and cases like it are obviously useful to policyholders.

9. If you are buying or renewing specialty cyber insurance policies, make sure that you are working with a very good and experienced broker. Because there is not presently uniformity of product in the cyber insurance marketplace, lots of terms are open for negotiation. A good broker can help get you the best coverage.

10. Provide notice to your insurance companies quickly after a breach. Early in the process of responding to a breach, the meter will be running on costs. When you have a breach situation, every second counts, and you undoubtedly will incur costs quickly for computer forensics, attorneys and other consultants. Providing proper notices and advising of these costs promptly can increase the odds of recovering these costs from your insurance companies.

* * *

About Anderson Kill's Cyber Insurance Recovery Group

Anderson Kill is a national full-service law firm best known for its work in insurance recovery. The firm represents policyholders only in insurance coverage disputes, with no ties to insurance companies and no conflicts of interest. Anderson Kill's Cyber Insurance Recovery attorneys have successfully represented retailers, financial services companies, professional services and engineering firms, entertainment companies, telecommunications companies, and technology manufacturers seeking insurance recovery for losses stemming from alleged data breaches, hacker-induced file corruption, data privacy violations, software and hardware malfunctions. The Cyber Insurance Recovery Group is chaired by Joshua Gold, http://www.andersonkill.com/attorneysprofile.asp?id=2378, who has helped to recover more than $1.5 billion for corporate policyholders in insurance coverage disputes. Mr. Gold has represented clients in diverse industries pursuing insurance claims for cyber-related losses and has published widely in insurance and legal journals on cyber insurance coverage issues. For more information about Anderson Kill's Cyber Insurance Recovery Group, please visit http://www.andersonkill.com/Cyber-Insurance-Recovery.