

# Finding Insurance Coverage for Data Breaches and Other Cyber Crimes

by Joshua Gold

Very recently, we obtained for a policyholder-client an insurance recovery when the United States Court of Appeals for the Sixth Circuit rejected AIG's denial of insurance coverage for the losses that resulted when the policyholder suffered a data breach at the hands of a computer hacker.

The Sixth Circuit's decision underscores a couple of important insurance coverage points involving computer hacking claims: 1) policyholders should resist the routine insurance company claims handling tactic of applying unduly narrow interpretations of insuring clauses, including the "direct loss" clause to crime insurance and fidelity bond insurance policies; and 2) when a loss occurs, policyholders are well advised to consider whether more than one policy covers their losses.

### **Maintaining Broad Coverage in an Era of Narrow Underwriting**

As for the first point, unfortunately for policyholders, insurance companies for many years now have been trying to get away from insurance that is "all-risk" or "comprehensive" in scope. Computer risk exposures (under both liability and property policies) are but the latest peril that the insurance industry has tried to push into stand-alone specialty policies or specific insurance policy endorsements to more conventional policies. However, just because the insuring clause for computer risks is placed into a specialized computer policy does not mean the coverage is narrow in scope for the online computer risk. In the Sixth Circuit case mentioned above, the insurance company had sought to deny coverage by arguing for a narrow interpretation of the insuring clause and a broad interpretation of the policy exclusions. Fortunately, both those claims handling tactics are disfavored under the law of most states.

As for claims that implicate two or more insurance policy types, policyholders should make sure that they provide prompt notice to all potentially relevant insurance companies. Data security breaches implicate a host of risks and also a bunch of potential losses associated with those risks that may be covered under both liability insurance policies and property policies (as well as policies that may provide hybrid coverage

between the two). Indeed, with the use of cloud computing, social media, and an ever increasing volume of electronically captured information, businesses are unquestionably exposed to an increasing threat of severe data security breaches.

In the Sixth Circuit case referenced above, the policyholder received defense cost coverage from its general liability insurance company for certain class actions which were filed as a consequence of the data breach. In addition, the policyholder was able to recover for the bulk of its other losses suffered as a result of the data breach, including, among other things, fraudulent credit card charges, credit monitoring expenses, customer call centers, FTC compliance costs, and costs for re-establishing compromised checking accounts.

Given the as yet many unresolved legal issues, businesses need to think carefully about the implications of their data appearing in an ever expanding number of public and semi-public repositories.

### **Potential Coverage from Many Insurance Lines**

When information does get wrongly accessed and misused, policyholders may find insurance coverage from a variety of sources for breaches of online security and invasion of privacy claims. Many forms of liability insurance protect against invasion of privacy claims. Should a policyholder be confronted by such a claim, umbrella insurance, general liability insurance, errors and omissions policies and other stand-alone specialty insurance policies should be checked for potential coverage. More proactively, if an insurance portfolio review reveals that those provisions have been written out of the businesses' portfolio of insurance, the broker should be enlisted to get those increasingly important coverages back in. If these provisions cannot be written back into existing policies, then stand-alone insurance policies specifically designed to cover online risks should be explored with the insurance broker.

Media and publishers' policies also have historically contained protection from online risk exposures. These policies, including media errors and omissions insurance coverage, may provide the insurance coverage framework for valuable protection to businesses of all types.

### **Other Risk Management Strategies**

Beyond insurance, other risk management strategies can be effective in minimizing the risk of online data security breaches. While the risk cannot be eliminated, it may be ameliorated by employing a few common sense principles in an organized and systematic approach. State of the art encryption and firewall software is a must. Also, business protocols should be adopted that regulate the manner in which data is used both outside of and inside the office. Given the data capacity of laptop computer hard drives, mobile devices, cloud computing and social media, it is critical that information contained in these places be protected as thoroughly as the business would protect the servers and desktops on its premises. All mobile devices should be password protected. Information within the organization should be ranked in terms of sensitivity, and internal access limited based upon actual business needs. Last, for those businesses dabbling with or embracing social media sites as part of their business strategy, care

should be taken as to the extent of the information posted or uploaded to those sites, as it could lead to information being exposed to many more eyes than originally intended. Additionally, companies must have clear written guidance as to the permissible and impermissible use of social media when the business makes a decision to embrace such marketing.

While no data security plan or approach will ever be watertight, a combination of smart data-handling procedures and quality insurance coverage can lessen the blow of unauthorized or unintended uses of business-related data. Furthermore, prudent risk management mandates that policyholders have a clear inventory of their insurance assets and take proactive steps to preserve their coverage rights under all potentially applicable insurance policies when claims surface.

---

*Joshua Gold is a shareholder in the New York office of Anderson Kill & Olick, P.C.*

# **RISK MANAGEMENT**