

Data Security Insurance for Cyber-Related Losses

By Joshua Gold



Joshua Gold

Data security breaches continue to mount, and no institution or individual is immune. Defense contractors, video game companies, universities and other organizations have recently experienced serious data thefts and attacks by hackers. The problem is so acute that even firms specializing in computer security have been attacked. While there are many things an organization can do to minimize both the risk and severity of a cyber attack, this article focuses on business insurance policies that may cover a cyber-related loss and how to protect those insurance coverage rights.

Insurance In the Event of a Cyber Loss

If a company suffers a loss or faces liability due to a data breach, step one is to figure out which of its insurance policies might provide insurance coverage for the loss. One or more often-purchased commercial policies may respond to a data breach loss and provide partial or complete insurance coverage for the loss suffered. Insurance policies to be checked include the following: property insurance policies (including those promising business interruption insurance coverage), liability insurance policies (including E&O, D&O, general liability and umbrella insurance), crime insurance policies (including financial institution bonds, computer crime policies and fidelity insurance), and business owner "package" policies (which may include two or more of the above-mentioned insurance coverages).

Which Policies Apply?

Figuring out which policies provide coverage for a cyber-related loss is not always easy. In some cases there may be overlapping coverage, where two or more policies combine to cover different aspects of the loss; or overlapping coverage denials, where multiple insurance companies assert that none of the insurance policies they sold cover the claim, given the presence of conditions or exclusions that the insurance company argues preclude coverage.

Depending upon the nature and scope of a data breach, a policyholder could face an array of losses and claims: lawsuits seeking damages for invasion of privacy, negligence, violation of federal statutes governing the handling of customer, employee or health information, lawsuits over the misappropriation of sensitive or secret business information, investigations by governmental authorities and, potentially, other claims. Policyholders may also experience business interruptions if they must shut down certain online systems or websites in order to contain (or determine the method of) the attack. Other costs may be incurred after informing customers and third parties of data breaches pursuant to state notification laws, establishing call centers

“The problem is so acute that even firms specializing in computer security have been attacked.”

“Data Security Insurance” continued p2



"Data Security Insurance" continued from p1

and providing guidance to those affected by the data breach.

Insuring Data Security with New Insurance Products

While some policyholders have secured insurance coverage for losses arising from computer fraud or theft under existing insurance policies, some have also purchased newer standalone insurance products to protect against the peril of data security breaches. Some of this more recent coverage is quite valuable, but it should never be thought of as "customer friendly." Internet suite insurance products, or "modules," are often confusing and unclear as to the true scope of insurance coverage.

Thus, policy terms should be closely scrutinized. For example, recent network security policies commonly include clauses that purport to condition coverage on the absence of errors or omissions in the data security measures employed by the policyholder. One policy clause purports to exclude coverage for any allegation that the policyholder knew about a "shortcoming in security" prior to the policy inception. Another exclusionary clause seeks to bar coverage for any allegation that the policyholder failed to "take reasonable steps" to design,

maintain and upgrade computer security at the company. Another clause, sometimes included in newer policy forms marketed to insure against data breaches, seeks to bar coverage where it is alleged that the policyholder used security software that has not been "proven successful" or has incomplete test results.

Such policy clauses are not only vague but also may be exploited by insurance companies arguing that the policyholder was somehow derelict in safeguarding computer data from hackers, among other coverage defenses. The risk of overly broad interpretations of exclusions is especially problematic in the context of computers, where the pace of technological developments (both good and bad) is rapid. Further exacerbating the risk is the reality that computer security is always playing catch-up and is never 100 percent ironclad. As such, these types of policy exclusions can be traps since it is not terribly difficult for a plaintiff to allege against the policyholder following a data breach that they somehow did not take enough security measures to protect data from disclosure.

Furthermore, some policies may attempt to limit insurance coverage if the data breach occurs when a computer is not actively connected to a network. For instance, will the insurance policy provide coverage for a laptop that is stolen from a car, hotel room or conference room where it is unconnected to the policyholder's network? Some insurance policy forms are either vague about this or actually purport to exclude computer hardware that is not actively tied to a network by omitting such devices from the policy's definitions. A stolen laptop storing sensitive information can pose just as many problems for a policyholder as a hacked network. Moreover, with the advent of tablet computers and handheld devices that have high-capacity memories and comparatively limited security, policyholders need insurance policies that protect against the risks inherent in these small, data-laden devices.

The risk of
overly broad
interpretations
of exclusions
is especially
problematic . . .

TO REGISTER
seminars@andersonkill.com
(212) 278-1400

15th
ANNUAL POLICYHOLDER
ADVISOR CONFERENCE

ANDERSON KILL & OLICK, P.C.
**Maximizing
Your Insurance Recovery**

Sentry Midtown East
730 Third Avenue
New York, NY
andersonkill.com/events.asp

October 13, 2011
Registration: 8:30 am - 9 am
Seminar: 9 am - 5 pm
Networking Reception: 5 pm - 6:30 pm



Other exclusions that should be avoided are those that seek to bar coverage for dealing with the Federal Trade Commission, state attorneys general or other governmental entities. Policyholders can incur substantial expenses in addressing enforcement actions, inquiries, investigations and other matters that may result after a data breach has taken place. Also to be avoided are exclusions that seek to bar coverage where the policyholder actively acquires customer information. For a host of business applications, policyholders may seek out and store customer information. Should that data get hacked, loss and liability may ensue. If the policyholder is looking to insure this risk, it is vital that the insurance policy not contain a vague or unduly broad exclusion that ends up gutting the very coverage sought.

Accordingly, policyholders should steer toward selecting insurance policy forms that are devoid of as many coverage exclusions (aka the fine print) as possible. Data security measures coupled with risk transfer in the form of insurance coverage can further a policyholder's risk management strategies and serve as a financial buffer when the data genie does escape the bottle.▲

Joshua Gold is a shareholder in the New York office of the law firm of Anderson Kill & Olick, P.C. Mr. Gold regularly represents policyholders, including gaming and hospitality businesses, software companies and retailers in insurance coverage matters and disputes concerning liability, arbitration, time element insurance, electronic data and other property-casualty insurance coverage issues.

(212) 278-1886

jgold@andersonkill.com



Be carbon conscious

...
Please consider
switching your
subscription to email.

By switching to email, you will receive our timely **Client Alerts** that are sent by email only. It's easy, send your mailing and email address to andersonkill@andersonkill.com.

To subscribe to Anderson Kill Newsletters and Alerts, please visit www.andersonkill.com/publications_subscribe.asp. To unsubscribe, please email unsubscribe@andersonkill.com.

Water, Water Everywhere . . . But is it Covered?

By Finley Harckham

The ubiquity of floodwater this spring in this country and in Japan should serve as a warning to businesses that do not have flood insurance to consider getting it. Flood insurance will protect a company's own property, and they also protect its profits when its customers or suppliers suffer flood damage. Fortunately, even businesses without flood insurance that were recently damaged when the Army Corps of Engineers opened flood gates in Louisiana may be covered.

Many American businesses have prepared insurance claims for lost profits resulting from the tsunami in Japan, only to have their insurance company deny coverage because they do not have flood or earthquake insurance. The claims are made under the contingent business interruption coverage found in many commercial property policies, which insure against lost income resulting from damage to the property of suppliers or customers. One requirement of that insurance is that the damage would have been covered if it had happened to the policyholder's own property. Businesses which do not have flood or earthquake insurance for their own property are probably not covered for losses arising out of the disaster in Japan.

However, not having flood insurance does not necessarily mean there is no coverage in every instance when property is inundated by water. In Southeast Missouri and Louisiana, the Army Corps of Engineers deliberately opened floodgates and breached levees, inundating lightly populated areas in an apparently successful bid to relieve pressure on the Mississippi River to forestall flooding in New Orleans, Baton Rouge and other densely populated areas. Thus, in a sense, some areas have been subjected to man-made flooding, and would have been spared absent human action. Indeed, property owners claiming to represent more than 60,000 acres in the floodway have sued the federal government, claiming that an intentional breach to the Bird Point levee violated their Fifth Amendment rights, prohibiting the government from seizing property without just compensation.

"Water, Water Everywhere" continued p4



"Water, Water Everywhere" continued from p3

Whatever constitutional questions it raises, the intentional release of water will also have insurance implications. The distinction between water damage caused by the deliberate act of government authorities, and that which results solely from the wrath of Mother Nature may provide a lifeline for some businesses when they argue against the application of flood exclusions in their property policies.

In the wake of Hurricane Katrina, policyholders argued against the application of flood exclusions on the ground that the proximate cause of damage was human negligence, not storm surge. Those arguments were rejected by the United States Court of Appeals for the Fifth Circuit on the grounds that even if human folly played a role, there was a storm surge which fell squarely within flood exclusions in many policies. The court also predicted that under Louisiana law the so-called anti-concurrent causation clauses found in most policies would be enforced to bar coverage as long as an excluded flood occurred at any step in the causal chain-reaction leading to a loss.

In an attempt to avoid the same fate as the victims of Katrina, businesses without flood insurance that have suffered from the recent flooding may be able to argue that the damage was caused *solely* by intentional human conduct, and therefore falls outside the scope of exclusions. This will be an issue of first impression for the courts in Louisiana, Missouri and neighboring

states, but policyholders and insurance companies alike will be able to find support in cases from other jurisdictions addressing analogous situations. For example, some courts have held that a flood and surface water exclusion does not apply to damage caused by a backed-up storm sewer system, even where the problem resulted from excessive rainfall, reasoning that water loses its character as surface water when it is channeled through a pipe. Victims of deliberate flooding could likewise argue that the river water does not take on the character of floodwater once it has been channeled and deliberately disposed of in an area that would not otherwise have flooded. On the other hand, a recent, unreported Massachusetts superior court decision held that a flood exclusion barred coverage when a municipality intentionally released water from a dam.

Although the extent of coverage for flood-related losses is often uncertain, policyholders should carefully consider the language of their policies and the circumstances of their losses, and not simply accept a denial of coverage. ▲

Finley Harckham is a senior shareholder in Anderson Kill's New York office. Mr. Harckham regularly represents corporate policyholders in insurance coverage matters. He has successfully litigated, arbitrated and settled hundreds of complex coverage claims, including those involving business interruption, property loss, directors and officers liability, professional liability and general liability claims.

(212) 278-1543

fharcckham@andersonkill.com

IRS Circular 230 Disclosure: To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. federal tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing, or recommending to another party any transaction or matter addressed herein.

AKO Policyholder Advisor

Anderson Kill Policyholder Advisor is published bimonthly by Anderson Kill & Olick, P.C. The newsletter informs clients, friends and fellow professionals of developments in insurance coverage law. The articles appearing in the **Anderson Kill Policyholder Advisor** do not constitute legal advice or opinion. Such advice and opinion are provided by the firm only upon engagement with respect to specific factual situations. If you require more information, legal advice or an opinion with respect to a specific situation, please contact our editorial board:

Editorial

Mark Garbowski, Editor-in-Chief

(212) 278-1169 or mgarbowski@andersonkill.com

Finley T. Harckham, International Editor

(212) 278-1543 or fharcckham@andersonkill.com

The firm has offices in New York, NY, Newark, NJ, Philadelphia, PA, Stamford, CT, Ventura, CA, Washington, DC.

Insurance Recovery Group Chairs

Robert M. Horkovich, Chair

(212) 278-1322 or rhorkovich@andersonkill.com

William G. Passannante, Co-Chair

(212) 278-1328 or wpassannante@andersonkill.com