Data Security Insurance for Cyber-Related Losses

by Joshua Gold, J.D.

Editor's note: This article originally appeared in Anderson Kill's *Policyholder Advisor* newsletter, Volume 20, Number 3, and is reprinted with permission.

```
error_reporting(E_ALL ^ E_NOTICE);
POST /DataRetrieve HTTP/1.1
Host: 192.168.1.1
Content-Type: application/soap+xml; charset=utf-8
Content-Length: 3932
<?xml version="1.0"?>
<soap:Envelope soap:encodingStyle="">
<soap:Body xmlns:m="http://192.168.1.1/loc">
<m:SecurityArray>
<m:PasswordIn>******</m:PasswordIn>
</m:SecurityArray>   var method = (("https:" == document.location.protocol)
                     topSecure var ("https://ssl." : "http://www.");)
                     document.write(unescape("script '" + gaVaHost + "xa.js' type='text/xml));
</soap:Body>         var pageTracker = _gat._getSecure("cd998dsxd");
                     webSecurity._analyze();
                     webSecurity._trackLocation();
</soap:Envelope>     </script>
```

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 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 table 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.

"Further exacerbating the risk is the reality that computer security is always playing catch-up and is never 100 percent ironclad."

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. ■