Insurance Updates

Legal and practical perspectives on insurance issues impacting businesses.

CYBER LIABILITY AND INSURANCE

NATURE OF THE CLAIMS

The recent hacking of the Target computer network may lead some to think cyber liability is basically a system hacking problem that is confined to large corporations. Both assumptions would be both incorrect and potentially risky if they lead small and mid-sized companies and professional service providers to ignore the risk or assume it is covered with basic computer and data security programs. In 2011, there were 414 reported security breaches that exposed 23 million confidential records.

Not all of those involved large companies. A study by the Secret Service and Verizon Communications found that 72% of all data breaches occurred in small and midsized businesses. In addition to hacking into a computer, loss of confidential data has occurred as a result of a rogue employee, a lost lap top, a stolen server or mere negligence of an employee. A Symantec survey found that 65% of all small businesses reported the loss of at least one mobile device during the course of a year. The devices included cell phones, smart phones, lap tops and notebooks. As businesses go increasingly wireless and mobile, the risk related to the loss of mobile devices can only increase.

Also, cyber liability involves more than the loss of private or confidential information. The functioning of individual computers or entire computer networks may be impaired or even destroyed as a result of a malicious act, negligence or something as basic as a power outage. The resulting damages may arise in the form of third party claims and lawsuits, first party loss from resulting business interruption or damage one's own computer system. The fact that the cyber event causing damage may arise from many different causes and resulting liabilities or damages take different forms can make the assessment of one's risk difficult.

Businesses manage their risks by the procedures they employ and the insurance they obtain. A 2012 survey by the Chubb Insurance Company found that 65% of public companies did not carry specific cyber liability insurance, even though a majority of companies viewed cyber risk as a major problem. These facts suggest that either many companies, presumably after some analysis, feel that they can adequately manage the cyber risk and do not need to incur the expense of insurance or that they found the insurance coverage offered to be inadequate, at least for the premium being charged. This note will attempt to let its readers better understand the relationship between insurance and cyber liabilities so they can make reasoned decisions on how to manage their cyber risks.

THE COST OF SECURITY BREACHES

A 2012 report by NetDiligence covering insurance payouts for cyber liability and data breach claims found that the average cost of a breach covered and paid by insurance was $3.7 million, with a majority devoted to legal damages. The business sectors suffering the most breaches were healthcare and financial services. The Ponemon Institute's 2010 report on the costs of security breaches, which was not limited to costs covered and paid by insurance, found that the average cost of $5.5 million per breach and $194 per record. The reason the Ponemon Institute's reported average loss is higher is probably because it includes internal costs to the business that may not be covered by insurance.

The NetDiligence report compared 2011 and 2012 loss data and found that while the number of records lost to breach decreased in 2012 the average cost per breach rose steeply from $2.4 million to $3.7 million. While the data is limited, if this is indicative of a trend it would signal greater risk for the smaller businesses that may not have millions of records but may also lack the financial resources to respond to a data breach.

The components of the loss reported by NetDiligence are forensics, notification of impacted parties, call center services, legal representation and providing credit monitoring. The loss figures do not include business interruption or third party damage claims arising from the breach. Not all cyber liability policies necessarily cover these later damages. It is important when considering cyber liability insurance to clearly understand what is and is not covered under the policy.

LOOKING FOR INSURANCE COVERAGE UNDER EXISTING POLICIES

Parties who have suffered some form of loss related to their data systems and did not have a specific cyber liability insurance have sought to find coverage under existing insurance policies. While these efforts appear to have had only marginal success based on reported cases, any business that suffers a cyber-loss should have all its insurance coverages thoroughly analyzed by a well-qualified professional. A broker may have general knowledge and understanding but would not necessarily have a handle on existing case law and how a successful legal argument could be mounted. A good example of this comes from fight for coverage for environmental losses. General liability policies prior to 1986 contained an exclusion that provided that there was no coverage unless the discharge of the pollutant was "sudden and accidental." The insurance industry thought "sudden" must necessarily have a temporal meaning indicating something happening over a short period of time. Courts across the country disagreed and held that "sudden" could mean "unexpected or unintended," and as a result billions of dollars of insurance coverage was found for long term, slow leaks from waste sites.

A basic insurance coverage principle that parties should keep in mind is that the duty to provide a defense is more easily triggered than the ultimate duty to provide indemnity for a given loss. Generally, a mere possibility that some small amount of indemnity coverage may be owed for a claim is enough to trigger the duty to defend. Having an insurance company provide a defense not only saves the insured those defense costs but can also serve to reduce ultimate indemnity costs when plaintiff attorneys know that the defendant cannot easily be forced to settle simply to avoid defense costs.

The essential point is that if confronted with a cyber-liability loss tender the claim to the insurance company. All the insurance company can do is to deny the claim. In tendering the claim, the insured should have a strategy and take care in how the initial tender is framed and how any follow up may be pursued.

Most businesses carry some form of commercial general liability ("CGL") coverage, either as a separate policy or as part of a business owner's protection policy. A CGL policy offers coverage for third party claims for loss or damage to property. More specifically, the CGL policies provide coverage for loss or damage to "tangible" property. The issue in the cyber liability context is whether software and data that may be lost, stolen or hacked constitutes "tangible" property. Since data and information may be the most valuable asset of a business, it may seem counter intuitive that this valuable asset would not be considered property for purposes of insurance coverage.

Courts are not unanimous in what constitutes "tangible" property for purposes of deciding whether a CGL insurance policy applies. While more cases currently support the insurer position that tangible property does not include software and data, there will almost certainly be more case law developed on this issue. The basic position taken by insurance companies is that "tangible" means something that can be recognized by the senses of touch, sight or smell. see: *American Online Inc. v. St. Paul Mercury Insurance Company,* 347 F.3d 89 (4th Cir. 2003); *Ward General Insurance Services v. The Employers Fire Insurance Co.,* 7 Cal Rptr. 3d 844 (Cal. App.2003).

In the case of *Carlon v. Delaget,* 2012 WL 1954146 (W.D. Wis. 2012), the defendant was a money manager for the plaintiff and virus planted into the money manager's data system allowed a hacker to withdraw money from Carlon's account. The Federal District Court held that the money loss was not tangible property. The Court acknowledged that money can be tangible but it need not be, and the electronic transfer of funds out of the account did not constitute tangible property. The Court held that to be "tangible" the property must be susceptible to physical injury.

The Federal District Court in Arizona took a broader view of what constituted physical damage under an insurance policy. *American Guarantee Liability Insurance Co. v. Ingram Micro Inc., 2000 WL 726789* (D.C. Arz. 2000). In that case a basic power outage caused the insured's computer network to go down for eight hours and caused a permanent loss of certain custom software configurations. Ingram relied heavily on its computer network and sought coverage for loss of profits. The Court found that the system was inoperable and could not be used for a period of eight hours constituted physical damage. Limiting the concept of "physical damage" to something that could be observed through the senses would be "archaic" according to this Court.

In the case of *Eyeblaster Inc. v. Federal Insurance Company,* 613 F.3d 797 (8th Cir. 2010), it was alleged that Eyeblaster's website caused injury to an individual's computer, software and data. The insurance policy's definition of tangible property specifically excluded software, data and other information. However, the policy provided for a "loss of use" of property. The Court found that there was coverage because there was no evidence that the party's computer could be

fully restored after the alleged viral infection. Thus, there was "loss of use" and insurance coverage was owed.

The practical teaching of these cases is that the tangible property language in most CGL policies may provide a basis for insurance companies to deny cyber-liability claims, there may be ways to defeat such denials and gain coverage, at least with respect to defense costs. If a cyber-liability event arises, it is important to not only have the company's general liability coverage closely analyzed but also to pay attention to how the loss is described and framed in the initial tender.

In addition to general liability policies, other types of policies may also be examined for potential coverage. In the case of *Nationwide Insurance Co. v. Central Laborers Pension Fund,* 704 F. 3d 522 (7th Cir. 2013), an employee of the accounting firm that managed financial matters for the pension fund had a CD stolen from her car that was parked in the open near where the employee lived. The CD contained private information concerning union members and the union sued the employee for damages. The employee tendered the claim under her homeowner's insurance policy. The policy excluded coverage for loss or damage to property "in the care, custody and control" of the insured. The Seventh Circuit relied on this exclusion as the basis for denying coverage. The holding does not mean that a homeowner's policy will never provide coverage, and what constitutes "care, custody and control" can be fact specific and lead to different results under different fact patterns. The case is worth noting because it demonstrates that coverage for a cyber-loss may be pursued under a variety of insurance policies, even those not directly covering the business. With the increasing reliance on, and loss of mobile data devices it would be reasonable for more cases to arise under homeowner or similar policies such as personal umbrella policies.

The case of *NMS Services, Inc. v. The Hartford*, 2003 WL 1904413 (4th Cir. 2003) involved a disgruntled employee who infected his employer's digital files and databases with a virus that caused certain of the materials to be erased. The question of coverage turned on the interpretation of the policy's employee dishonesty exclusion. This provision excluded coverage for loss or damage caused by a dishonest act of an employee. However, the exclusion by its terms did not apply to acts of destruction caused by an employee. The Court held that the erasing of the digital materials constituted "destruction" as opposed to "damage" of the digital, files and therefore the exclusion did not apply. The takeaway from the NMS Services case is that subtle difference, such as the distinction between destruction and damage, can be pivotal to the determination of whether there is coverage.

This discussion of certain case law is not intended to be an exhaustive presentation of existing law. Rather, the intent is to give the business person a sense of the potential for finding coverage, and the need for a careful and studied analysis of existing policies. Also important is the need to present the claim in the form that enhances the prospect for finding coverage. A company facing a cyber-liability event would be advised to get appropriate counsel immediately and before the claim is even tendered to an insurance company.

A BRIEF ANALYSIS OF CYBER-LIABILITY INSURANCE POLIICIES

Many insurance companies offer some form of cyber-liability insurance coverage. While there are some basic similarities with most policies, there may also be differences that may be important to the particular cyber risk profile of a company. As with all insurance, the policy should be carefully reviewed before binding. In preparation of this note, the authors have reviewed the basic policy forms provided by Beazley and Chartis, as well as various pieces written by brokers describing the cyber-liability insurance available. The intent is to provide the reader with a starting point for understanding and potentially analyzing cyber-liability insurance policies.

The first point is that the policies are a bit complex and lengthy. For example, the Beazley policy is 27 pages of "insurance speak." Even for an attorney who has drafted insurance policies and reviewed hundreds of others, sorting through the terms of the cyber-liability policies takes some time and effort. The review process will be more efficient if the company starts by outlining its cyber risks and the types of claims, losses and damages that might reasonably be expected to flow from a cyber-loss event.

A starting point is to recognize that the cyber-liability policies provide two distinct forms of coverage: first party and third party coverage. The first party coverage defines what losses sustained directly by the insured are or are not covered. The third party coverage defines the nature of third party claims are covered. Under the Beazley policy form both first and third party coverage is provided on a "Claims Made and Reported" basis. By comparison, the first party coverage under the Chartis policy is written on a "Discovery" basis and the third party coverage is written on a Claims Made and Reported basis.

Generally speaking, under a Claims Made policy, coverage is triggered when a formal demand in the form of a written demand or suit is received. Under a Discovery policy, coverage is triggered when, in effect, a security breach or other cyber event is first discovered, even though no claim has been made. The distinction between Claims Made and Discovery coverage can be important. For example, the loss of a lap top might be a security failure triggering an obligation to notify the insurer under a policy triggered on a Discovery basis. Such a potentially common event might not require reporting under a Claims Made policy. (However, it might still be prudent to provide notice under a "claims made" policy form). Also, suspected breaches that may be reported to the company under a whistle blowing program may need to be reported more promptly to an insurer under a Discovery policy as opposed to a Claims Made policy. An insured needs to understand when coverage is triggered under its insurance policy and how that relates to reporting requirements.

Another basic point to understand is what is and is not covered under a cyber-liability policy. Under the first party coverage, the policies generally cover the items referred to in the NetDiligence study: forensic reviews to understand the nature and source of the problem; some degree of public relations support (the Beazley policy limits this to $10,000); the cost of notification and credit monitoring. The policies may or may not cover costs to restore or repair the company's data network. The policies generally do not cover lost profits, business interruption, coupons and other customer relations activities and internal costs associated with a data breach. Executives at a company may reasonably be most concerned about what a security breach will mean to the income and profits of the company and simply assume that

any cyber-liability policy would insure this exposure. Executives should be aware that the reality is to the contrary.

The policies may vary significantly in terms of what third party coverage is provided. For example, the Chartis policy covers punitive damages and "any monetary amounts and Insured is required by law or has agreed to by settlement to deposit into a consumer redress fund." This is a fairly broad grant of third party coverage. The Beazley coverage grant may be somewhat narrower in this regard. It covers damages from unauthorized disclosure or private information, regulatory defense and penalties and website liabilities such as slander and infringement on intellectual property.

Instructive of the type of coverage issues that are likely to arise under the cyber-liability policies is an apparent conflict between the Chartis broad grant of coverage under the third party liability section for any monetary amounts required to be put in a consumer redress fund ant the exclusion for damages to Property, defined as tangible property. Does the exclusion overrule the "any monetary amounts" if part of the consumer redress fund is aimed at paying for property damage? If so, then apparently "any" does not really mean "any."

The Beazley policy also excludes coverage for property damage. However, because its coverage grant language is more narrow than the "any monetary amounts" language in the Chartis policy, the same potential conflict that exists under the Chartis policy would probably not be found to exist under the Beazley policy.

As discussed in connection with coverage cases under CGL policies, whether the term property damage covers data loss can be an important issue. Under the Chartis policy, Property Damage is defined to mean tangible property and further defined that tangible property does not include electronic data. Therefore, when the policy excludes claims for "property damage" it is not excluding coverage for the loss of electronic data. A convoluted way to get to the point that damages for the loss of electronic data could be covered.

The Beazley policy gets to basically the same coverage point with respect to loss of data but gets there differently. The coverage grant specifically covers alteration, corruption or destruction to a Data Asset. The policy defines property damage to mean physical injury to tangible property and does not mention data. Therefore, when the policy excludes coverage for property damage, it would reasonably be read to only exclude injury to tangible property and not reduce the coverage grant covering damage to Data Assets.

The purpose here is not to analyze all the potential coverage issues that may arise under a cyber-liability insurance policy. There will undoubtedly be many issues, and those issues will be driven by the particular facts of the case and the language of the particular policy involved. The examples here are cited simply to make the reader aware of the type of issues that may arise and how insurance policies may need to be analyzed. The interpretation of an insurance policy under a given set of facts is not always an easy task. Over the last 30 years the field of insurance coverage has become something of a niche specialty in the legal profession, and probably for good reasons. A company dealing with a cyber-liability insurance coverage issue would be well served to call upon a member of this niche practice area.

The authors are pleased to receive comments, criticisms or questions.

Don Jernberg has focused on insurance coverage issues for over 35 years. He has litigated over 75 insurance coverage cases across the country, provided numerous coverage analysis and opinions, and authored over 30 articles in the areas of insurance and dispute resolution. He has also been called upon by insurance companies to draft policies, ranging from pet health insurance to complex lender liability policies. He has been retained as an expert on insurance matters and was qualified as an expert witness on certain insurance issues in the Circuit Court of Cook County. He may be contacted at djernberg@jernberglaw.com or 847-259-0953.

Jennifer Mozwecz represents corporations and individuals in intellectual property, corporate transactions and commercial litigation matters. She represents and counsels clients in the technology sector on their corporate and intellectual property matters. She is also authorized to practice before the United States Patent and Trademark Office. She may be contacted at jmozwecz@srmlaw.com or 312-564-5757.