Got Protection? Coverage for Cyber-Risk Under Traditional Insurance Policies

(As published in the Los Angeles Daily Journal October 24, 2012)

Although much attention is now focused on the new insurance products which are specifically designed to cover cyber-risks, companies whose property or business operations are impaired by reason of such events also ought to consult their traditional insurance policies. Such policies may often provide unforeseen benefits.

Theft of customer information by computer hackers

A company which is victimized by computer hackers may face a variety of losses and legal risks. For example, in a recent case where private customer and credit card information were stolen, the company incurred substantial financial losses, including nearly $ 4 million in remediation-related expenses, such as costs associated with charge backs, card reissuance, account monitoring and fines imposed by the credit card companies. *Retail Ventures, Inc., et al. vs. National Union Fire Insurance Company of Pittsburgh, Pa,* 691 F.3d 821 (6th Cir. 2012).

In that case the company successfully obtained reimbursement of these expenses through a "Blanket Crime Policy", which contained an endorsement for "Computer & Funds Transfer Fraud Coverage". The carrier denied coverage contending that the crime policy was effectively a "fidelity bond", a form of insurance which provides only first-party coverage. The Sixth Circuit rejected that characterization and found that the insurer was responsible for reimbursing the company for its losses in connection with the theft of customer information.

Companies victimized by computer hackers will also face liability from customers (whose personal information has been compromised) and also from financial institutions (who may be obligated to replace their customers' cards and reimburse them for fraudulent transactions). Two recent cases address this scenario. *Anderson, et al. vs. Hannaford Brothers Co*., 659 F.3d 151 (1st Cir. 2011) (class action by store customers whose electronic payment data was stolen by hacker brought action against store owner); *In Re Heartland Payment Systems, Inc. Customer Data Security Breach Litigation*, 834 F.Supp.2d 566 (S.D. Texas 2011) (credit card issuer banks and credit cardholders brought suit against processor of credit card transactions whose computer systems had been compromised by hackers).

Although neither case addressed the insurance coverage for the underlying losses, there are at least two potential sources of coverage.

First, the personal injury coverage contained in standard CGL policy might provide coverage for claims of customers where the gravamen of the claim is one for "invasion of privacy". In this regard, two recent cases have found that coverage under a CGL policy for "invasion of privacy" would apply in circumstances analogous to a data breach. See, e.g., *Creative Hospitality Ventures, Inc. vs. United States Liability Ins. Co*., 655 F.Supp.2d 1316 (S.D. Fla. 2009) (violation of right of privacy, and hence "personal and advertising injury' coverage under CGL policy triggered, where vendor failed to redact customer credit card information from receipts),

subsequently reversed in part, 444 Fed.Appx. 370 (11th Cir. 2011); *Netscape Communications Corp. vs. Federal Ins. Co*., 343 F.Appx. 271 (9th Cir. 2009) (tracking by internet service provider of customers' online activity violated customers' right of privacy and hence constituted a "personal injury offense," thereby triggering coverage under the policy).

Second, a D & O policy might provide coverage for suits against a company arising from a data breach where the policy provides entity coverage. Thus, "[w]here entity coverage [under a D&O policy] is broad, it may encompass liabilities for privacy breaches and cyber risks." *Proskauer on Privacy*, § 17:2.3 at p. 17-15.

A third source of legal risk would be claims by a company's shareholders against the company's directors and officers for failing to accurately disclose its cybersecurity risks. In this regard, the SEC issued a written guidance on this subject in October, 2011. See http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. The emerging obligation on the part of company's directors and officers to include in its securities filings an assessment of a company's cybersecurity risk means that SEC enforcement actions and shareholder suits based on alleged inadequate disclosure in this area will inevitably follow.

In the event that company officers or directors are sued in connection with data breaches, the primary vehicle for handling such suits would be conventional D & O policies: "this type of insurance may be applicable in limited circumstances where an officer or director is sued directly in connection with a privacy breach – perhaps for lack of supervision or personal involvement in dissemination of confidential information". *Proskauer, op. cit*., § 17:2.3[A] at p. 17-15.

A computer virus disables a company's operations or results in the loss of data.

The majority position is that electronically stored data does not constitute "property" for purposes of property or business interruption coverage. See, e.g., *Ward General Insurance Services, Inc. v. Employers Fire Insurance Co*., 114 Cal.App.4th 548 (2003). Nevertheless, there are some cases which have found coverage for business interruption or data loss caused by a computer virus.

The key issue in this area is often whether the loss of such data constitutes "direct physical loss or damage to property" within the meaning of traditional property or business interruption policies.

The courts have split on this issue, a minority finding that the destruction or impairment of electronic data is sufficient to constitute "direct physical loss of or damage to property." This split means that coverage under traditional first-party policies for the loss of computer data may depend on the jurisdiction involved and the particular policy form that is used.

Examples of instances where coverage was found under traditional first-party policies for the loss of computer data include these:

A company was insured under a property damage policy which insured against certain business interruption and service interruption losses. As a result of a power outage, the company's computer systems were rendered inoperable. The company made a claim under its policy, which

its carrier denied. The Court held for the policyholder, holding that "physical damage" is not restricted to the physical destruction or harm of computer circuitry but also includes loss of access, loss of use and loss of functionality. See *American Guaranty and Liability Inc. Co. v. Ingram Micro*, 2000 WL 726789 (D. AZ. 2000).

The operator of a medical clinic was insured under an "All Risks" property insurance policy which included business interruption coverage. As a result of a hurricane and consequent electrical and telephone outages, the clinic's computer system became corrupted, resulting in a loss of data. Although the carrier denied the operator's claim, the Court granted summary judgment to the operator, holding that the corruption of the policyholder's computer constituted a "direct physical loss of or damage to property" within the meaning of the policy. See *Southeast Mental Health Center, Inc. v. Pacific Insurance Company, Ltd*., 439 F.Supp 831 (W.D. Tenn. 2006).

An employment agency had a business insurance policy which, in addition to traditional coverages, also provided that the carrier would reimburse the agency for lost information stored "on electronic or magnetic data". The agency's computer system malfunctioned as a result of a "hacker" having injected a virus into the system. The carrier denied the claim, but the Court held for the policyholder, finding that the personal property losses sustained by the policy-holder were "physical" as a matter of law. See *Lambrecht and Associates v. State Farm Lloyds*, 119 S.W.3d 16 (Tex.App. 2003).

Importantly, the courts in other jurisdictions have reached different results. This split in appellate authority means that insureds need to scrutinize their policy forms and understand the applicable law in the jurisdiction where they conduct business.

Claims for misappropriation of another's computer data

This scenario arises when a company hires an employee who was formerly with a competitor. The new employee brings computer files from a competitor which are then downloaded to a new employer's system. The competitor then brings a claim for IP theft and trade secret infringement and thereafter learns through discovery that some of its data resides on the new employer's computer network.

Although some cases outside of California take a different view, the majority position is that claims for trade secret misappropriation or IP theft will not be covered under a standard CGL policy. See *S.B.C.C., Inc. v. St. Paul Fire & Marine Insurance Co*., 186 Cal. App. 4th 383 (2010).

However, the outcome may be different under a D & O policy. See *Acacia Research Corp. vs. National Union Fire Insurance Co. of Pittsbugh, PA*, 2008 WL 4179206 (C.D.Cal. February 8, 2008), where the court concluded that the scope of the insuring clause providing for coverage for "wrongful acts" was broad enough to require the D & O carrier to reimburse the company and its officer for defense fees and the settlement paid in an IP theft/trade secrets case. Similarly, in *MedAssets, Inc. vs. Federal Insurance Co.*, 705 F.Supp.2d 1368 (N.D.Ga. 2010), the court concluded that a claim alleging misappropriation of confidential information against insured company was covered under the company's D & O policy.