Connecticut Law Tribune
FEBRUARY 14, 2011
VOL. 37, NO. 7 • $10.00
An ALM Publication
CTLAWTRIBUNE.COM

Insurance Coverage For The Computer Age

Cyber-security policies needed to deal with data loss and theft

By SABRINA HOULTON

Business losses resulting from data breaches, computer system malfunction, employees' Internet usage, computer viruses, and other risks relating to information technology infrastructure and activities have grown exponentially with the evolution of the Internet and the ability to collect, store, and use electronic data on a mass scale.

For many years, companies had traditional insurance policies written before or without regard to the computer age. Now numerous insurers explicitly exclude IT-related risks and offer separate, specific cyber-security insurance.

The need for such coverage is clear. Larry Clinton, president of the Internet Security Alliance, reports that "some estimates now place the economic loss from known cyber thefts at more than $300 million per day." A study of data breaches from 2009 by the Ponemon Institute calculates the cost of a data breach at over $200 per affected individual, with the average total cost at over $6 million per event.

Traditional Insurance Enough?

The insurance coverage questions involving e-commerce and electronically stored data raise a host of novel issues for the courts to decide. There is one common legal question, however, that consistently pervades these decisions: whether a loss of such data constitutes a physical harm sufficient to trigger coverage under traditional policies. The answers offered by the courts are inconsistent.

Several courts concluded that a loss of electronic data does not amount to a loss of property and, therefore, traditional general liability and commercial liability policies do not offer coverage. For example, in *America Online Inc. v. St. Paul Mercury Insurance Co.*, the court considered whether claims from customers that AOL's Version 5.0 had damaged their computer data, software, and systems were covered under AOL's general liability policy. 207 F. Supp. 2d 459 (E.D. Va. 2002).

The policy covered "property damage," defined as "physical damage to tangible property of others, including all resulting loss of use of that property; or loss of use of tangible property of others that isn't physically damaged." The court held that "[c]omputer data, software, and systems do not have or possess physical form and are therefore not tangible property as understood by the Policy."

On appeal, the 4th Circuit affirmed the decision, holding: "The insurance policy in this case covers liability for 'physical damage to tangible property,' not damage to data and software, i.e., the abstract ideas, logic, instructions, and information." *America Online Inc. v. St. Paul Mercury Insurance Co.*., 347 F.3d 89, 96 (4th Circuit, 2003).

Despite this clear statement, earlier in the same year – 2003 – the 4th Circuit held in a different case that loss of data resulting from a disgruntled employee hacking into a company's databases constituted "damage to its property, specifically, damage to the computers." *NMS Services Inc. v. The Hartford*, 62 Fed. Appx. 511, 2003 U.S. App. LEXIS 7442, at *7 (4th Circuit, April 21, 2003).

The California Court of Appeal in *Greco & Traficante v. Fidelity & Guaranty Insurance Co.* (an unpublished 2009 decision) considered the claim of a law firm that mistakenly underreported its bills as part of a settlement, and thereby failed to collect some $57,000 owed to it, as a result of a glitch in its billing software.


Sabrina Houlton

Because the law firm could not prove that the glitch was the result of a physical loss, the court held that there was no coverage under the "Electronic Data Processing Systems" provisions in its policy that covered "risks of direct physical loss."

Other decisions have also found that electronic data is not tangible property and, therefore, is not covered under a property liability policy or a general liability policy.

In *American Guarantee & Liability Insurance v. Ingram Micro Inc.*, however, the U.S. District Court in Arizona in 2000 reached a very different conclusion. Ingram, which was a wholesaler of "microcomputer products," suffered a power outage that resulted in a loss of "all of the programming information" from its system to track customers, production, and daily transactions. As a result, the company suffered a significant business interruption and financial harm. The court found coverage, holding that "'physical damage' is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of

Sabrina Houlton is an associate in Wiggin and Dana's Privacy and Information Security, Insurance, and Litigation practices.

Insurance Coverage & BAD FAITH LITIGATION

use, and loss of functionality."

Similarly, in *Southeast Mental Health Center Inc. v. Pacific Insurance Co.*, the court addressed a coverage claim made by a health center after the prescription data contained its pharmacy computer became corrupted as a result of a power outage. 439 F. Supp. 2d 831, 833 (W.D. Tenn. 2006). Relying on *Ingram*, the court held "that the corruption of the pharmacy computer constitutes 'direct physical loss or damage to property' under the business interruption policy."

In short, courts offer a mixed reading on whether e-commerce injuries or the loss or compromise of electronic data or systems qualify as physical harms sufficient to trigger coverage under traditional insurance policies.

Insurance Companies' Response

Given the varied response of the courts, both insureds and insurers are left without clear guidance on whether a traditional property or general liability policy covers damage to electronic data. In response to this uncertainty, many insurance forms now explicitly exclude electronic information unless added into the coverage through an endorsement. Other insurers have offered limited coverage.

The policy language varies enormously. Some exclude electronic data entirely. Others provide coverage for the cost of replacing or restoring lost or corrupt electronic data, or provide coverage only for replacing the blank media compromised in a data loss, while excluding the costs of recreating or replacing the data. Some policies only cover specific types of data loss, such as the damage caused by a computer virus. And still others provide coverage for electronic media and records with a broad, inclusive definition. Certain policies cover other possible damage, such as data breaches and claims related to Internet usage, with varied approaches.

In addition to the legal uncertainty that insurers face is a lack of market experience in dealing with e-commerce and electronic data risks, which makes pricing cyber-security insurance a challenge. As a result, many insurers have been hesitant to offer expansive insurance that might involve the assumption potentially limitless risk. Instead of following a more traditional model — covering a broad range of risks with the option to purchase additional coverage through endorsements — insurers tends to offer cyber-security insurance on a piecemeal basis to allow insurers to price risk more discretely.

Evaluating Cyber Insurance

As with traditional commercial policies, there are two general categories of risks covered by e-commerce insurance: first party and third party. First party insurance covers the insured's own damages, such as property insurance or business interruption insurance. Third party insurance covers risks of harm to others for which the insured might be held liable. It is critically important to consider both kinds of risk when evaluating cyber security insurance, because cyber-security insurance tends to be offered in a menu format, putting the burden on the insured to make the right selections from that menu.

The e-commerce and other electronic data risks that a business may wish to cover include

data loss caused by a power outage, hacking, an IT accident; theft; and defective hardware. Coverage might also include data breach from an accidental sharing of information; hacking; software malfunction; mishandling of data; a rogue employee; defamation or slander related to Internet postings; copyright or trademark violations related to Internet usage; extortion (disabling or threatening to disable a computer system or to destroy data if a certain payment is not made); and corporate espionage.

Additionally, businesses might wish to guard against a loss of income as a result of lost or corrupt data; service outage; damaged hardware or software. Finally, they might seek protection against third party claims, where, for example, a user sues for damage to his or her computer or data as a result of a Web site or product offered.

Businesses must guard against inadvertently purchasing insurance that is too narrow to cover the numerous risks that they may face. But they must also guard against purchasing coverage that is unnecessary because their property liability and general liability policies already cover certain IT-related risks expressly or under applicable case law.

Companies must also be attentive to exclusions of certain types of harm in cyber-security insurance policies. For example, some policies do not cover intentional violations of a company's privacy policies. As a result, if an employee fails to follow company policy, the resulting harm may not be covered.

Policies also may exclude coverage for government enforcement actions. That means that the costs associated with responding to a Federal Trade Commission investigation into a data breach, or a Department of Health and Human Services investigation into a potential violation of the Health Information Portability and Accessibility Act, may not be covered.

There is one indirect benefit to purchasing cyber-security insurance – encouraging the adoption of best data security and privacy practices. Just as a property insurer will require that property be "up-to-code" and in proper condition, a cyber-security insurer will likely require a company to implement best practices to avoid a covered event. Meeting these insurance requirements may have the unintended benefit of improving your company's IT security practices and procedures – in addition to providing coverage should something go wrong. ■