

Data Breaches Are Not Going Away

Will Your Company Be Covered for Those Risks?

By Scott Godes

When a company reports two data breaches in one month, another company reportedly is paying fines for past data breaches, and “the demand for cyber security professional[s] is high and growing” because, “[o]ver the past year cyber exploitation activity has grown more sophisticated, more targeted, and more serious,” it is clear that data breaches are problems that are not going away (*see*, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1371544,00.html; www.pcworld.com/printable/article/id,173902/printable.html; and www.defensetech.org/archives/005068.html).

In fact, “between 75[%] and 85[%] of Fortune 2000 companies have suffered a ‘material data breach.’” Worse still, just three alleged hackers allegedly stole more than 175 million data records; at an estimated cost of \$202 per lost record, and that adds up to more than \$35 billion in loss.

Because the costs of data breaches can be so astronomically high, the importance of ensuring that e-commerce and other types of firms have insurance to cover such claims cannot be overstated (*see*, www.proper-ty-casualty.com/Issues/2009/July%2020%202009/).

Scott Godes is counsel with Dickstein Shapiro’s Insurance Coverage Practice in the firm’s Washington, DC, office. He is the co-head of the firm’s Cyber Security Insurance Coverage Initiative and co-chair of the American Bar Association Computer Technology Subcommittee of the Insurance Coverage Committee of the Section of Litigation. He frequently represents corporate policyholders in insurance-coverage disputes. He can be reached at godes@dickstein-shapiro.com.

Pages/Data-Explosion-Expands-Breach-Exposure-But-Insurers-More-Open-To-Handling-Risk.aspx; www.claimsjournal.com/news/national/2009/08/17/103075.htm; and www.forbes.com/2009/01/30/security-hacking-enterprise-technology-security_0202_data_breach_print.html).

WHAT INSURANCE MIGHT APPLY TO DATA BREACHS?

If your company faces a data breach and suffers losses as a result, but your company has not purchased a specialized suite of policies marketed as cyber-security policies, then coverage nonetheless may still be available under other insurance policies.

Commercial General Liability And Business Owners Policies

The first insurance policies to consider is your company’s business-owner insurance policy (“BOP”) or commercial general-liability (“CGL”) insurance policy. BOPs and CGL policies contain grants of coverage that may apply to potential liabilities arising from data breaches.

The first coverage to examine is personal and advertising injury coverage. That coverage grant often includes invasion-of-privacy or other privacy-related claims. When analyzing whether such coverage might apply to data breach-based damages, consider the allegations in any complaint alleging a data breach. If there are allegations of invasions of privacy or other privacy violations, the personal- and advertising-injury coverage may provide a duty to defend the claims, at a minimum. Case law that should prove helpful, by analogy, exists in which courts have rejected insurer arguments “that in order to constitute a publication, the information that violates the right to privacy must be divulged to a third party.” (*Zurich Am. Ins. Co. v. Fieldstone Mortgage Co.*, No. CCB-06-2055, 2007 U.S. Dist. LEXIS 81570, at 14 (D. Md. Oct. 26, 2007);

see also, Netscape Commc’ns Corp. v. Fed. Ins. Co., No. CV-08-15120, 2009 U.S. App. LEXIS 19500 (9th Cir. Aug. 27, 2009) (interception and internal distribution of private data meets personal injury coverage for purposes of duty to defend).) Many states’ insurance-coverage laws will require the insurance company to defend the entire lawsuit against a policyholder, even if there is just one covered claim (in the form of an invasion-of-privacy allegation). (*See, e.g., Donnelly v. Transp. Ins. Co.*, 589 F.2d 761, 764-65 (4th Cir. 1978) (D.C. law).)

Beyond BOPs and CGL policies’ personal- and advertising-injury coverage, companies should consider coverage for damages because of alleged property damage. The question of whether such coverage for “property damage” extends damage to computer software and data was hotly contested in courts in the late 1990s and early 2000s, with a split of authority. For example, a Texas appellate court rejected a property insurer’s argument that damage to a policyholder’s computer system from a computer virus was not a “physical” loss.” (*Lambrecht & Assocs., Inc. v. State Farm Lloyds*, 119 S.W.3d 16, 23-25 (Tex. App. 2003).) A federal court in Arizona held that computers suffered “physical damage,” as required by the applicable all-risk first-party insurance policy, when information stored in random access memory was destroyed and the computers’ functionality was reduced. (*Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*, No. 99-185 TUC ACM, 2000 WL 726789 (D. Ariz. Apr. 18, 2000).) At least one court has ruled that the computer data in question “was physical, had an actual physical location, occupied space and was capable of being physically damaged and destroyed” such that lost data was covered under a CGL policy. (*Computer Corner, Inc. v. Fireman’s Fund Ins. Co.*, 46 P.3d 1264, 1266 (N.M. Ct. App.

2002). Yet another court, the U.S. Court of Appeals for the Fourth Circuit, has a split in its authority, having issued one opinion holding that data erased by a hacker was “direct physical loss” under the insurance policy, and another opinion holding that damage to and loss of use of customers’ data and software were not covered under a CGL policy because there was no damage to “tangible property” under the definition of “property damage” (*compare, NMS Servs., Inc. v. Hartford*, 62 F. App’x. 511, 514 (4th Cir. 2003) *with Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003)).

The insurance industry has made changes to the standard-form CGL policy language, and certain policy forms sold since the early part of the decade contain language addressing whether data, software and other electronic information are “tangible property.” Insurers may argue that such language limits the application of general-liability coverage to cyber-security claims. Even with the new policy language, however, the issue is far from settled — coverage may depend on the facts of the claim and the type of policy involved. Moreover, endorsements may change the coverage significantly. What the CGL’s standard-form insuring agreements sought to limit might be revised by policy endorsements that broaden coverage. For example, some policies may contain data-breach endorsements or other endorsements that amend the definition of property damage to include loss of or damage to electronic data. Thus, it is critical to review the endorsements to the policy closely; there may be endorsements that have made coverage for such claims available.

(For more on endorsements as mentioned immediately above, *see*, Claire Wilkinson, “Is Your Company Prepared for a Data Breach?”, *Insurance Information Institute 20* (2006), available at http://server.iii.org/yy_obj_data/binary/761998_1_0/Data_Privacy.doc, which discusses the Insurance Services Office Inc.’s (“ISO”) endorsement for “electronic data liability.” *See also*, Jerry Trupin, “Address the Electronic Data Liability Coverage Gap,” *IRMI Update*, Oct. 8, 2009, at www.irmi.com/newsletters/irmiupdates/2009/0215-risk-management.aspx#subject1, asserting that ISO Electronic Data Liability endorsement CG 04 37 12 04 provides coverage to lost or damaged data resulting from the physical injury to tangible property.)

Other Sources of Coverage

After analyzing the company’s CGL policy or the third-party liability section of the company’s BOP, it is worthwhile to analyze the remaining coverages that are in place for the company. For example, check the company’s crime policy. A broadly written insuring agreement may provide coverage for hacking, data breaches and the theft of consumer data. Crime policies may also contain endorsements for computer fraud, computer theft or other data extraction. One major property and casualty insurer has sold crime policies with computer-fraud endorsements that may cover data breaches and other cyber-security losses.

It also is worthwhile to consider other policies that the company has in place. Review all risk/first-party property policies and coverages closely; there have been court cases holding that damage to data and electronic information is covered under such policies. First-party policies (often the first coverage grant in a BOP) may also provide coverage for the business-interruption losses and extra expenses incurred because of a cyber-security loss. Moreover, a first-party policy may provide coverage for losses arising from a third party’s cyber security-based business interruption (so-called “contingent business interruption”). For an overview of contingent business-interruption insurance coverage, *see*, Scott N. Godes, “Ensuring Contingent Business Interruption Coverage”, *Law360*, Apr. 8, 2009, <http://insurance.law360.com/articles/94765>.

As another example, the company’s error and omissions (“E&O”) coverage, including all endorsements, may provide coverage for alleged errors and omissions, depending on the nature of the allegations made against the company and the scope of coverage purchased. Also consider the nature of allegations against the company and other individual defendants after a claim has been made and/or complaints have been filed. To the extent that directors or officers are named, D&O coverage may apply. In those matters in which there are attempts at extortion or ransom, such as was alleged against one Fortune 200 company and a Virginia State Web site with health records, kidnap and ransom

policies may provide coverage. Other policies, such as employment-related practices policies or data-processing policies, may provide coverage as well, depending on the particular facts of the claim. (*See*, Complaint, *Amburgy v. Express Scripts, Inc.*, No. 09-705 (E.D. Mo. Filed May 8, 2009) and *Business Wire*, “Cyber Secure Institute Analyzes Virginia Health Database, UC-Berkeley Hacks,” *Dark Reading*, May 26, 2009, www.darkreading.com/database_security/security/privacy/showArticle.jhtml?articleID=217700176: “Last month, hackers attempted to extort \$10 million after breaking into a Virginia State [W]eb site used by pharmacists to track prescription drug abuse. The records of more than 8 million patients were deleted and a ransom note was put on the Virginia Prescription Monitoring Program’s homepage, demanding \$10 million dollars [sic] in exchange for the return of the records.”)

What Other Sources of Recovery May Be Available?

Finally, investigate the company’s contracts with vendors, partners or other service providers to determine whether any indemnity agreements may include cyber-security liability. Also determine whether the company is an additional insured under any other insurance policies, such as those held by vendors, customers or clients, to determine whether there may be coverage under those terms.

CONCLUSION

With the continual upgrading of technology such that ever-growing amounts of data can be held on servers in a single location or individual hard drives, the temptation for cyber thieves to try to steal such data will not disappear soon. Data breaches, therefore, are a real and growing threat to companies. Insurance was designed to alleviate such financial risks, and companies would be well advised to analyze their policies to ensure that they will be covered for such potential liabilities and damage.

Reprinted with permission from the December 2009 edition of the LAW JOURNAL NEWSLETTERS. © 2009 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877.257.3382 or reprints@alm.com. #055081-11-09-02