BY DENNIS M. CUSACK

Safety Net

New insurance coverage for information-technology risks

Farella Braun + Martel

THE INCREASINGLY "WIRED" NATURE OF global commerce as well as the persistent ingenuity of hackers have companies scrambling to protect themselves against liability claims arising from lost or stolen data. The first line of defense is usually technology to prevent data loss. Another response is for general counsel to allocate risk through contractual indemnity provisions. A third solution is insurance coverage. This article explores the new insurance policies being introduced to cover risks that standard general liability and errors and omissions policies do not adequately address.

NETWORK SECURITY LIABILITY COVERAGE

Companies face increasing risks from lapses in systems designed to protect computer data: lost or stolen laptops, unauthorized access of personal information, or system

EXECUTIVE SUMMARY

Companies are increasingly preoccupied by the threat of data security breaches, invasion of privacy, and Internet-related intellectual property claims. However, new insurance products addressing these risks add a layer of protection beyond technology and contractual indemnity solutions. General counsel, IT directors, and risk managers must become knowledgeable about these products, and tailor them to their company's specific needs.

disruptions from malware. Such incidents may give rise to claims by consumers alleging actual or feared identity theft; by banks to recover the costs of reopening credit card accounts; and by vendors, clients, and business partners for the costs of disrupted operations, or disclosure of trade secrets.

One notable example occurred in 2006 when hackers stole millions of T.J. Maxx customers' credit card numbers over many months before the company detected the breach. T.J. Maxx also waited more than a month after it discovered the theft before publicly announcing it. Lawsuits were filed by the banks that had to reissue credit cards and by consumers alleging identity theft. Losses were recently estimated at more than $250 million.

Social Security and credit card numbers are not the only targets. Hackers recently stole personal background information from résumés in a Monster.com database. They then used the names of high schools and previous employers to mount targeted "phishing" campaigns, hoping to implant malware that would then collect passwords and credit card numbers.

In the face of increasing concern over data security, Congress and state legislatures have responded in a variety of ways. At the federal level, the Gramm-Leach-Bliley Financial Institutions Act, and the Health Insurance Portability and Accountability Act, protect financial records and personal health information, respectively, from disclosure. California and other states have passed laws outlining protections for personal information and requiring public disclosure of data security breaches. A Minnesota law imposes strict liability for data security breaches for failure to meet the Payment Card Industry security standards.

Many insurers now offer "network security liability coverage" to address these potential risks. Coverage typically extends to liability arising from: unauthorized access to a database (hacking); identity theft; inability to gain authorized access to data; denial or disruption of service attacks; and inadvertent transmission of malicious code. These policies also have exclusions such as federal or state agency claims (for example, by the Federal Trade Commission for a company's failure to comply with its promises to safeguard consumer data); computer failure because of fire, explosion, or electrical disruption; misappropriation of trade secrets; contractual liability (the obligation to indemnify another for their liability, unless you would be liable anyway); and emotional distress damages, such as fear of identity theft.

Stolen laptops or system disruptions may give rise to claims by consumers, banks, and clients.

PRIVACY LIABILITY COVERAGE

Privacy liability policies provide some overlapping coverage with network security liability policies; however, insurers have separately packaged certain protections under this label. This coverage addresses the risks of the improper disclosure of personal information when it results from company mistakes other than security lapses leading to theft of data. The risks encompassed by these policies include: transfer of data to third parties in violation of privacy policies, failure to control how data is used by those authorized to receive it, and other public disclosures of private information. One notable example of these risks is the FTC's action against ChoicePoint. The data broker was selling data to customers without adequately verifying that they were legitimate, and some customers were identity-theft operations. The FTC levied $15 million in fines and enjoined the company to better safeguard information.

Privacy liability coverage may extend to: invasion of privacy claims (identity theft and other public disclosure of private information); trespass and eavesdropping claims; breach of a company's privacy policy; and breach of statutes and regulations regarding control and use of personally identifiable information.

Policy exclusions may include: federal or state agency claims; the collection of private information (such as with cookies); claims that the company's published privacy notification is unclear or inadequate; claims that the integrity of private information properly collected has been compromised; and trade secret claims.

MEDIA LIABILITY COVERAGE

Companies formerly relied on some coverage for certain intellectual property risks, such as copyright, trademark, and unfair competition claims, through the "advertising injury" coverage in the standard general liability policy. But over the past 20 years, insurers have gradually narrowed this standard

EXPERT ADVICE

INSURANCE TIPS

Companies pursuing insurance solutions should reflect on several factors before choosing a policy. Here are a few to consider:

- Identify potential risks, such as data security breaches, privacy violations, and Internet-related intellectual property risks.
- Work with the company's risk manager and broker to identify a choice of insurance products.
- Participate actively in the insurance-application process. Coordinate with the IT director to ensure the application and attachments are accurate.
- Study the proposed policy forms to clarify what is covered and propose language changes as needed.
- Consider requiring that vendors and other business partners also obtain network-security, privacy, or media-liability insurance.

INSURANCE

coverage to almost nothing (only limited coverage for copyright infringement in an "advertisement" is now included). Any company with a significant advertising or publishing presence on the Internet may find even this coverage removed by endorsement.

Insurers now offer separate "media liability" coverage for those risks associated with advertising and publishing. This includes companies directly doing business over the Internet, or providing services for online businesses. Although the Internet is the main focus of the coverage, it may also extend to other media. Coverage includes claims for infringement of copyright and trademark, unfair competition, defamation, and invasion of privacy. Still excluded are claims for trade secret misappropriation, antitrust, patent infringement, and negligence in providing professional services.

POLICY SCOPE

All of these policies may be offered, as a company's risk profile warrants, in different combinations of modules in a package policy, or even as stand-alone coverages. They are generally offered as "claims made" coverage. This means that the policy will respond only to claims that are first made during the policy period, regardless of when the incident occurred. The policy may further provide that the claim must be reported to the insurer within the policy period, or by some other deadline. Premiums, limits of liability, and deductibles vary widely, depending on both the risk being insured and on the insurer. In addition, the language in these policies is not standard. For example, some network-security and privacy-liability policies cover emotional distress damages; others do not. Moreover, one insurer's policy contains an exclusion for claims arising out of security shortcomings a client knew of or "ought reasonably to have known about." This phrase raises doubts about whether the policy covers anything at all.

Quotes for the same coverage may differ by tens or even hundreds of thousands of dollars. This wide disparity reflects how new these coverages are, and the limited experience insurers have for calculating risk and thus pricing. However, the fluidity of policy forms also creates an opportunity. Companies may be able to negotiate changes to the language to clarify intent, in order to avoid disputes later. Coverage may also be tailored to more closely suit a company's risks. One element that remains common, though, is that unlike a standard general liability policy, defense costs incurred on any claim will erode the policy's limits of liability.

Companies may be able to negotiate changes to language to clarify intent and avoid disputes later.

General counsel, therefore, must carefully review the policy forms before making a purchase. In this area, reliance on the company's broker is not sufficient to identify issues and traps for the unwary.

THE APPLICATION PROCESS

When these policies were first introduced, insurers often required companies to undergo an independent audit of the company's network-security systems as part of the application process. Most insurers are now willing to rely on the company's own information and audits. Nonetheless, the application process remains a significant challenge, requiring the input of the company's CFO, risk manager, IT director, and general counsel. The lengthy application forms require detailed answers about the company's information technology practices and past experiences. Unlike other areas of coverage, such as general liability or directors and officers policies, insurers generally will not accept an application submitted on another insurer's form. Insurers also will require that you submit substantial additional written materials, which will be deemed incorporated into the application.

All of this creates a greater risk that the insurer will raise a rescission defense when a claim arises later. The complex application process for these new specialized coverages only increases the risk that information may be omitted that an insurer will later argue was material to its underwriting. General counsel therefore need to be actively involved in the process, making sure that requested information is provided and that, if questions are unclear, they are clarified before the application process is completed. Savvy risk managers will also insist on a policy term—an "unintentional errors and omissions clause"—that precludes the insurer from rescinding unless it can show that the company committed intentional fraud in the application.

IT directors, risk managers, and general counsel should become knowledgeable about these new ways to protect a company's assets, and participate actively in their purchase.

DENNIS M. CUSACK is a partner at Farella Braun + Martel in San Francisco and is a member of the Insurance Coverage Group. He represents companies and individuals seeking insurance coverage under technology errors and omissions, general liability, directors and officers, employment practices liability, and property policies. His practice includes litigation, arbitration, appeals, and mediation of disputes.
dcusack@fbm.com

"Partner Advisory, Insurance" originally published in the Winter, 2008 issue of *8-K*.