Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Insurance Coverage For Cyber-Risky Business

Law360, New York (February 21, 2012, 1:39 PM ET) -- The U.S. Securities and Exchange Commission (SEC) recently issued guidance for public companies about their disclosure obligations for cyber-security risks and cyber incidents. The SEC strongly advised companies to consider disclosure of specific cyber risk factors, potential related costs and a "description of relevant insurance coverage."

The SEC's guidance will undoubtedly draw increased executive-level attention to the types of insurance that coverage companies maintain — if any — for cyber-security events, such as the loss of private customer information through a data breach. Insurance companies may see increased inquiries from public company clients looking to fill coverage gaps prior to their next quarterly filing.

Although industry data demonstrates that the market for stand-alone cyber-security insurance policies continues to expand, these independent policies appear to be the exception rather than the rule.

Instead, as recent court decisions demonstrate, companies continue to seek to rely on their commercial general liability (CGL) policies in an effort to cover cyber-security related losses. Contemporary CGL policies, however, typically do not, by design, provide coverage for certain critical cyber risks.

The Loss of Computer Data May Not Constitute Covered Property Damage

Take, for example, the situation in which an accident — or the nefarious actions of a third party — cause the loss of sensitive and valuable computer data. Many insureds have sought coverage for this type of loss by filing a "property damage" claim under Coverage A of their CGL policies.

Historically, this approach has earned mixed results. For example, in American Guaranty & Liab. Ins. Co. v. Ingram Micro Inc. (April 19, 2000), the District of Arizona determined that the temporary deterioration of a company's computer system and loss of programming data constituted "physical damage," thereby creating coverage under the relevant policy.

By contrast, in America Online Inc. (AOL) v. St. Paul Mercury Ins. Co., 347 F. 3d 89 (2003), the Fourth Circuit Court of Appeals upheld a rejection of coverage after determining that injury to customer computer software and data — allegedly caused by the installation of AOL software — did not constitute "physical damage to tangible property," which is required under Coverage A of CGL policies.

In response to American Guaranty, and the divergence of case law, many insurance companies changed their CGL forms to eliminate the possibility that they would be ordered to cover data loss under "property damage" liability coverage.

For example, in 2001, the Insurance Services Office (ISO) amended its CGL form to clarify that "electronic data is not tangible property." In 2004, ISO again amended its CGL form to expressly exclude from property damage coverage any "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access or inability to manipulate electronic data."

Accordingly, under most modern CGL forms, insurance companies can, and do, deny "property damage" claims relating to a third party's loss of computer data or destruction of software.

For example, in Eyeblaster Inc. v. Federal Ins. Co., 613 F.3d 797 (8th Cir. 2010), Federal denied coverage after a customer alleged that spyware from Eyeblaster's website permanently destroyed certain data on his computer, and otherwise impaired the efficient running of his computer. The Eighth Circuit Court of Appeals, relying on the "electronic data" exclusion, supported a denial of coverage for injury to the customer's data.

The court, however, refused to dismiss claims related to damages the customer alleged to have incurred for the ongoing poor operation of his computer, because those allegations allegedly fell within the CGL policy's cover for the "[l]oss of use of tangible property that is not physically injured." As a result, policyholders may seek to craft claims to describe damages related to hardware failure, as opposed to data loss.

In a case filed in February 2012 — Arch Ins. Co. v. Michaels Stores Inc., No. 12-0786 (Feb. 3, 2012, N. D. Ill.) — Arch seeks a declaration that it has no duty to defend or indemnify Michaels under its CGL policies. The underlying claims at issue in Arch allege that that Michaels allegedly failed to safeguard personal identification number (PIN) pad terminals, thereby allowing criminals to obtain and misuse customer debit and credit card information.

In its complaint, Arch relies, among other things, on the policies' "electronic data" exclusion and the updated definition of "property damage" that carves out electronic data.

In the face of standard exclusions for electronic data loss, many insurance companies offer data loss endorsements to their standard CGL policies. For example, ISO created the "Electronic Data Liability" endorsement that adds a third party's computer data and software back into the universe of items that can constitute covered "property damage."

This endorsement, however, will not provide coverage for a company's accidental loss of its own electronic data. CGL policies typically contain an "owned property exclusion" that limits coverage to the damaged property of third parties. When faced with the loss of their own data, insureds will generally need to review their first-party property insurance policies.

Data Breach Liability May Not Constitute Covered Personal and Advertising Injury Liability

When a data breach does cause injury to third parties — typically a company's customers — policyholders have increasingly tendered claims under Coverage B of standard CGL policies, which covers certain "personal and advertising injury" liabilities.

In ISO's most recent CGL form, for example, the phrase "personal injury and advertising injury" is defined as injury arising out of specified offenses, including the "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."

This provision is the covered "offense" on which policyholders most frequently rely in data breach claims. For example, if a doctor's misplacement of her iPhone results in the release of patient health data, a hospital may be the recipient of lawsuits alleging a variety of tort claims, including negligent failure to maintain adequate network security.

For several reasons, however, "personal injury" coverage may not be available for data breach liability under standard CGL policies.

First, a data breach may not constitute "publication" of private material. Insurers may argue that the word "publication" requires a communication that is both intentional and widespread. When the doctor leaves behind her iPhone in a taxi, she does not intend to publish health information to the taxi driver, who retrieves the iPhone. Arguably, it is not a publication "offense" covered under standard CGL forms.

By contrast, a hospital's intentional posting of documents on its website that accidently contain pieces of patient health data may constitute "publication."

The case law on the issue is mixed, as two recent cases demonstrate. In Norfolk & Dedham Mut. Fire Ins. Co. v. Cleary Consultants Inc., 81 Mass. App. Ct. 40 (Dec. 16, 2011), the Massachusetts Court of Appeals determined that an insured's alleged transmittal of an employee's private information to her co-workers could constitute "publication" under a standard CGL policy.

By contrast, in Creative Hosp. Ventures Inc. v. E.T. Ltd. Inc., 2011 U.S. App. 19990 (Sept. 30 2011), the Eleventh Circuit Court of Appeals found that the issuance of a receipt containing sensitive credit card information to a customer did not constitute publication, because it did not involve "dissemination of information to the general public" — although the court did stress that the customer was the one who received his own personal financial information.

Second, whether a data breach constitutes a violation of privacy may depend on the nature of the information allegedly disclosed. In Valley Forge Ins. Co. v. Swiderski Elecs. Inc., 223 Ill. 2d 352 (2006), the Illinois Supreme Court held that the "right of privacy" in a standard CGL policy "connotes both an interest in seclusion and an interest in the secrecy of personal information."

Health care information, social security numbers and credit card numbers likely will qualify as personal information whose public release would invoke a person's right of privacy. Coverage questions may arise, however, when a data breach causes the release of questionably private information, such as a customer's purchase history or an employee's salary information.

Third, the "personal and advertising injury" section of standard CGL forms contains a number of exclusions that may impact the availability of coverage for data breaches. For example, many CGL policies, including ISO's most recent form, exclude cover for personal and advertising injury liability incurred by policyholders that are in the advertising, broadcasting or Internet service provider businesses.

In addition, many CGL policies, including ISO's most recent form, exclude coverage for injuries "arising directly or indirectly" from an action that violates or is alleged to violate "any statute, ordinance or regulation ... that prohibits or limits the sending, transmitting, communicating or distribution of material or information."

For example, in Creative Hospitality Ventures Inc. v. United States Liab. Ins. Co., 655 F. Supp. 2d 1316 (S.D. Fla. 2009), adopted in relevant part by 655 F. Supp. 2d 1316, a federal magistrate judge excluded coverage when a policyholder was alleged to have disclosed customer credit card information in violation of the federal Fair and Accurate Transaction Act.

By its terms, however, the exclusion is not limited to intentional actions that violate the law. By accidently misplacing a laptop containing customer social security numbers, a policyholder may distribute personal information, albeit by mistake, in violation of state data privacy regulations.

Additionally, the exclusion does not appear limited to statutory violations committed by the policyholder; in fact, most CGL policies contain a separate exclusion for damages arising out of criminal actions committed by the insured. Instead, the "distribution of material in violation of statutes" exclusion precludes coverage for damages associated with a third party's criminal transmittal of private information that leads to claims against the policyholder.

For example, if a computer hacker enters a company's network and then retrieves customer information to engage in identity theft, the hacker may have violated a criminal statute prohibiting the transmittal of stolen financial information. An insurer could seek to rely on these alleged criminal violations to exclude coverage for the aggrieved customers' lawsuits against the policyholder.

In Arch Insurance Co. v. Michaels Stores Inc., No. 12-0786 (Feb. 3, 2012, N. D. Ill.), Arch appears to have taken this position by denying coverage under the "distribution of material in violation of statutes" exclusion for damages stemming from a criminal's hacking of its policyholder's debit card terminals.

As courts continue to highlight the absence of coverage for data loss under standard CGL policies, and as the SEC focuses on disclosure of cyber-security risk information, the market for stand-alone cyber-security policies continues to grow.

Companies may be increasingly attracted to products that more clearly address third-party liability, while also unambiguously covering the potential for significant first-party costs of responding to a data breach, such as investigative expenses, notification costs, business reputation loss and government fines. Companies that choose not to purchase these types of available policies likely will be left without coverage for certain key cyber risks.

--By Jean-Paul Jaillet, Choate Hall & Stewart LLP

J.P. Jaillet is a partner in the insurance and reinsurance and major commercial litigation groups in Choate's Boston office.