Apr 11 2013

Posted By: Mark F. Foley

Practice Area: Information Technology, Data Privacy and Security & Insurance Coverage and Risk Management

A recent *Digital Lex* column discussed a Wisconsin Court of Appeals decision holding that traditional Comprehensive General Liability Insurance for "advertising injury" covered third party claims for intellectual property theft in the form of former employees starting a new company competing with their former employer by duplicating a web based system for matching buyers and sellers of goods. *See* Digital Lex: Insurance for Technology Theft in the World of E-Commerce, Jan. 16, 2013.

This kind of theft is only one of the many forms of cyber related risk companies face. Every CEO, CFO, and CIO should be assessing cyber risks to the enterprise and considering whether to insure or self-insure against the potential costs and losses resulting from a major data security breach. The market for cyber insurance has matured dramatically in the last half decade to where there are now many kinds of policies available for both third party claims and first party losses.

Third-party coverage insures against claims by third parties for losses they suffer on account of the assured's acts or omissions. Third party cyber-related coverage is presently available for at least a half dozen types of risks.

- **Directors' and officers' errors and omissions** has been available for many decades to cover risks that have nothing to do with the cyber world per se. In assessing whether and how much to have of this insurance, the company should consider the possibility of claims based on allegations of securities fraud or failure to properly disclose and manage risks and breach of fiduciary duty in protecting the enterprise against foreseeable cyber security and related risks. Even an executive's seemingly innocuous Tweets can create potential liability for securities law violations. *See*: Protect Your CEO's Tweets and Posts from SEC Enforcement Action.
- **Professional liability/product liability** has also existed for many years. Today, claims may relate to custom developed software, off the shelf software products, cloud data storage, software as a service, or software embedded in products that, when they fail, cause property damage, personal injury, or consequential and incidental damages.
- **Disclosure injury** coverage is for lawsuits alleging unauthorized access to or dissemination of the plaintiff's private information. To date, such lawsuits have not generated large numbers in terms of damage claims by individual data subjects. The greater risk is for class action lawsuits or claims extending to negligence in handling outsourced data processing and data storage services.
- **Content injury** coverage is intended to protect against suits arising from intellectual property infringement, trademark infringement, and copyright infringement.
- **Reputational injury** insurance is designed to cover claims for disparagement of products or services, libel, slander, defamation, and invasion of privacy.
- **Conduit injury** coverage is for claims arising from system security failures that result in harm to third-party systems.
- **Impaired-access injury** is similar, but different, applying to claims arising from system security failure resulting in your customer's systems being unavailable.

First-party coverage is available to cover your own losses and expenses for the following circumstances that may be related to a cyber security breach.

- **E-business interruption** is for e-commerce sites that go down, act erratically, or have data corrupted. It is a variant of traditional "business interruption" insurance.
- **E-theft and e-communication** policies cover losses that arise from the interruption of communications systems and networks outside of your company's own system.
- **E-threat**, including the cost of a professional negotiator and ransom payment to protect against extortion attempts.
- **E-vandalism expense** coverage is for attacks that seek to damage but not necessarily to extort economic advantage. A critical coverage question is whether the policy applies to vandalism was caused by employees as well as third persons.
- **Advertising injury** coverage is often part of a standard comprehensive general liability policy. It may apply where stolen data or electronic systems are used by a competitor to offer products or services to customers and prospects through an electronic platform.
- **Privacy notification** insurance covers U.S. mail, email, and media notification expenses as well as the cost of providing credit-monitoring services for customers affected by your data security breach. A critical coverage issue is whether the policy applies even when state law doesn't require notification.
- **Crisis management** coverage may include the cost of public relations consultants.

These are only general descriptions of the types of coverage available. Every policy must be examined closely to be sure the risks you face are included. The biggest problem for businesses looking for insurance coverage is to fully understand what is not covered.

Too often, the close scrutiny of policy coverage does not occur until after a claim is made. This makes misunderstanding and disappointment a distinct, and potentially costly, risk. Even sophisticated companies stumble. In 2011, SONY suffered a series of cyber security breaches affecting data in its online gaming systems. The SONY's insurer said the company did not have a cyber insurance policy, that SONY's existing policies only covered tangible property damage, not cyber incidents, and therefore the insurer would not provide any coverage for the company's loss nearly $200 million loss. SONY spokespersons contested these statements, expressing their belief that at least some of the losses were covered. *See, Insurance Against Cyber Attacks Expected to Boom*, New York Times online, December 23, 2011.

You, your insurance advisers, and your legal counsel should make a careful investigation of what your company needs, what coverages are offered, what a specific policy does and does not cover, and how to self insure potential losses outside of your coverage limits.

---

von Briesen & Roper Legal Update is a periodic publication of von Briesen & Roper, s.c. It is intended for general information purposes for the community and highlights recent changes and developments in the legal area. This publication does not constitute legal advice, and the reader should consult legal counsel to determine how this information applies to any specific situation.