MEALEY'S™
Emerging Insurance Disputes

Cyber Insurance: What Are You Buying?

by
James M. Westerlind

Arent Fox LLP

A commentary article reprinted from the January 7, 2016 issue of Mealey's Emerging Insurance Disputes

LexisNexis®

Commentary

Cyber Insurance: What Are You Buying?

By
James M. Westerlind

[Editor's Note: James Westerlind is Counsel at Arent Fox LLP and an insurance lawyer who has become focused on cyber risk and cyber insurance coverage issues. If you have any questions, please feel free to contact the author by telephone at (212)457-5462, by email at james.westerlind@arentfox.com, or by mail at 1675 Broadway, New York, NY 10019. Any commentary or opinions do not reflect the opinions of Arent Fox LLP or LexisNexis, Mealey's. *Responses are welcome.]*

Much has been said and written about cyber risks recently. It is a hot topic at seminars, in publications, and before state and federal legislatures. And for good reason. With cyber attacks like those experienced by Anthem, Target, Sony, eBay, Chase, Home Depot, Neiman Marcus, Michael's, CVS, the Wall Street Journal, the NYSE, and even the federal government — including the White House, the Department of Energy and the Office of Personnel Management — it is no surprise that the subject has gained widespread attention. Add to it our heightened concerns over terrorism and the magnitude of the potential harm of a cyber attack increases exponentially.

Cyber security is no longer simply the responsibility of a company's IT professionals and risk managers. It is also a key obligation of the board of directors. The board members' fiduciary duties to the company's shareholders and investors include the active oversight of the company's enterprise risk management ("ERM") function. Luis A. Aguilar, the Commissioner of the SEC, made this duty clear in a speech that he made at the NYSE last year: "there can be little doubt that cyber-risk also must be considered as part of a board's overall risk oversight."

The risk does not only lie with large public companies. Any company that handles personal identifiable information, protected health information or credit card information for customers (which includes nearly every small to mid-sized company) has exposure to a data breach. The large cyber security breaches that we typically read about in the news often involved point-of-sale attacks, where some form of malware was implanted onto a retailer's credit card processing system to collect credit card information from consumers as they swipe their credit card at the register for their purchase. Card skimmers have been used by the "bad guys" at ATM machines, gas pumps, department stores and local grocery stores.

And, if such a breach or unauthorized disclosure occurs, the company likely has an obligation to comply with state and/or federal notification rules and regulations. Forty-seven states have enacted data breach notification laws to date, requiring a company that has, or has reason to believe that it has, experienced a data breach to inform authorities and consumers if personal identifiable information has been, or may have been, stolen or compromised. Notification must be prompt. For example, Vermont's breach notification statute, Vt. Stat. tit. 9, § 2435, requires a company that has experienced a data breach to provide a preliminary description of the breach to the State's Attorney General within 14 business days following discovery or notification.

In the U.S., the liability cost per compromised record was approximately $217. eBay's data breach in May 2014 exposed 233 million records. There are a number of websites where you can calculate the estimated cost of a data breach to your company. *See, e.g.*, http://www.privacyrisksadvisors.com/data-breach-toolkit/data-breach-calculators/.

Thankfully, many of the insurance policies now available to address cyber risks have been designed to help alleviate both liability and response costs. While the exposure to companies from liability to consumers for a data breach could be substantial at the end of the day, the costs and expenses that such companies experience in investigating the event, notifying consumers and rectifying the problem can be substantial as well. And these upfront costs and expenses are incurred very quickly after a data breach is discovered. Moreover, many small-to-mid-sized companies do not have the expertise and infrastructure in place to deal with a data breach and the notice requirements imposed by law.

Many of the cyber risk insurance policies available in the market provide breach response coverage in addition to liability insurance. That is, they cover all or a portion of the costs and expenses that the insured company will incur in investigating the data breach (or suspected data breach), notifying authorities and consumers of the matter, and remedying the problem (including, among other things, providing coverage for public relations firms to assist the company in protecting its reputation following a data breach). Many of the cyber risk insurers maintain a panel of professionals, including lawyers, forensic IT specialists, PR firms, 1-800 call centers, etc., that are available to quickly assist the insured when it suspects that it has been the victim of a data breach and has notified the insurer. The immediate assignment by the insurer to the insured of legal counsel who specializes in dealing with data breaches and notification laws has numerous benefits to the insured, including protecting communications with vendors assigned to assist with the matter as privileged and ensuring that each person involved in the breach response process is experienced and knowledgeable. One mistake early in the breach response process could be devastating for the company, which, in most instances, is simply a victim itself.

Beazley offers a couple of different policies to protect against cyber losses, including (1) a Professional and Technology Based Services, Technology Products, Information Security & Privacy, and Multimedia and Advertising Liability Insurance Policy ("Beazley Services and Products Policy"), and (2) a Beazley Breach Response policy.

The Beazley Services and Products Policy insuring agreements include: (1) Professional and Technology Based Services Liability; (2) Technology Products Liability; (3) Information Security & Privacy Liability; (4) Privacy Notification Costs; (5) Regulatory Defense and Penalties; (6) Regulatory Defense and Penalties; and (7) PCI Fines, Expenses and Costs.

The Professional and Technology Based Services Liability insuring agreement pays for damages and claims expenses of the insured's negligent professional services (except for media activities, or work in the capacity as an accountant, architect, surveyor, health care provider, lawyer, insurance or real estate agent or broker, or civil or structural engineer) or computer and electronic services, or the unintentional breach of a contractual obligation to perform such services.

The Technology Products Liability insuring agreement pays for damages and claims expenses of the insured for negligence, the unintentional breach of a contractual obligation or copyright infringement related to its Technology Products, defined to include computer, telecommunications or related electronic products.

The Information Security & Privacy Liability insuring agreement pays for damages and claims expenses of the insured for losses arising from: (1) the unauthorized disclosure of personally identifiable information or other confidential business information in the care, custody or control of the insured, (2) failure of computer security to prevent a security breach, (3) the insured's failure to timely disclose one of the foregoing incidents as required by law, (4) the insured's failure to comply with its written privacy policies, or (5) the insured's failure to administer an identity theft prevention program or information disposal program as required by federal law.

The Privacy Notification Costs insuring agreement pays the insured for privacy notification costs incurred in complying with breach notification laws. Such costs are defined to include those arising from:

(1) computer expert services (including a computer security expert to determine the existence and cause of an actual or suspected electronic data breach; a PCI Forensic Investigator to investigate the actual or suspected compromise of credit card data; and a computer security expert to demonstrate the insured's ability to

prevent a future electronic data breach as required by a Merchant Services Agreement);

(2) legal services to determine the actions necessary to comply with breach notice laws and advise the insured in responding to credit card system operating regulation requirements for any actual or suspected compromise of credit card data;

(3) provide notification to (a) individuals who are required to be notified by law, or (b) in the insurer's discretion, individuals affected by an incident in which their personally identifiable information has been subject to disclosure in a manner which poses a significant risk of harm to those individuals;

(4) call center services (for a period of 90 days following notification or longer if required by law);

(5) public relations consultancy (up to $100,000); and

(6) credit and identity monitoring services for up to 1 year.

The Regulatory Defense and Penalties insuring agreement pays claims expenses and penalties that the insured is required to pay for a claim in a governmental regulatory proceeding arising from a violation of a privacy law.

The Multimedia and Advertising Liability insuring agreement pays for damages and claims expenses of the insured arising from its professional services, media activities and technology-based services and that are premised on claims of infringement, misappropriation, unfair competition and certain other claims.

The PCI Fines, Expenses and Costs insuring agreement indemnifies the insured for fines, penalties, reimbursements, fraud recoveries or assessments owed by the insured under the terms of a Merchant Services Agreement and resulting from the actual or alleged noncompliance with published PCI Data Security Standards and a data breach (but not including charge backs, interchange fees, discount fees or prospective service fees).

The Beazley Breach Response policy insuring agreements include: (1) Information Security & Privacy Liability; (2) Privacy Breach Response Services; (3) Regulatory Defense and Penalties; (4) Website Media Content Liability; and (5) PCI Fines, Expenses and Costs. Theses insuring agreements are, for the most part, substantially similar to many of the insuring agreements in the Beazley Services and Products Policy. The Privacy Breach Response Services insuring agreement in the Beazley Breach Response policy, however, provides more services by Beazley and its vendors to the insured in responding to a breach event.

Coverage under the Privacy Breach Response insuring agreement is triggered by an incident (or reasonably suspected incident) arising from (1) a theft, loss or unauthorized disclosure of personally identifiable information or confidential business information, or (2) a failure of computer security to prevent a security breach. If coverage is triggered, the insured is entitled to Privacy Breach Response Services from Beazley, which phrase is defined to include:

(1) Computer expert services (including a computer security expert to determine the existence and cause of an actual or suspected electronic data breach; a PCI Forensic Investigator to investigate actual or suspected compromise of credit card data; and a computer security expert to demonstrate the insured's ability to prevent a future electronic data breach as required by a Merchant Services Agreement) in accordance with the terms and conditions set forth in an Information Packet provided to the insured with the policy and provided by a service provider selected by the insured;

(2) Legal services to determine the actions necessary to comply with breach notice laws; to provide necessary legal advice to the insured in responding to an actual or reasonably suspected theft, loss or unauthorized disclosure of personally identifiable information; and advise the insured in responding to credit card system operating regulation requirements for any actual or suspected compromise of credit card data. Legal services are provided in accordance with the terms and conditions set forth in the Information Packet and are to be provided by an attorney selected by the insured;

(3) Notification services provided by a service provider selected by the insurer in consultation

with the insured from a list provided in the Information Packet to (a) individuals who are required to be notified by law, and (b) in Beazley's discretion, individuals affected by an incident in which their personally identifiable information has been subject to disclosure in a manner which poses a significant risk of harm to those individuals;

(4) Call center services, which means the provision of a call center to answer calls during standard business hours for a period of 90 days following notification (or longer if required by law) of an incident for which notification services are provided. Such notification will include a toll free telephone number for recipients to call, and call center employees will answer questions about the incident and provide information required by HIPAA/Health Information Technology for Economic and Clinical Health Act ("HITECH") media notice or other applicable law. Call Center services will include up to 10,000 calls per day, and be provided by a service provider selected by Beazley in consultation with the insured from a list provided in the Information Packet;

(5) Breach resolution and mitigation services, meaning credit monitoring, identity monitoring or another solution selected from the products listed in the Information Packet and offered to notified individuals;

(6) Public relations and crisis management expenses, meaning the following costs approved in advance by Beazley and related to mitigating the harm to the insured's reputation or potential loss covered by the policy resulting from (a) a theft, loss or unauthorized disclosure of personally identifiable information or confidential business information, (b) a failure of computer security to prevent a security breach, or (c) the actual or imminent publication in the media of a covered claim:

(i) costs incurred by a public relations or crisis management consultant;

(ii) costs incurred to inform the general public about the incident (limited to $100,000);

(iii) costs for voluntary notifications to customers or patients;

(iv) costs for government mandated notices;

(v) costs to restore healthcare records of notified individuals whose personally identifiable information was compromised; and

(vi) other costs approved in advance by Beazley.

Privacy Breach Response Services also includes assistance from the BBR Services Team and access to educational and loss control information at no charge.

If you have any questions, please feel free to contact James Westerlind at Arent Fox LLP by telephone (212-457-5462), email (james.westerlind@arentfox.com), or mail (1675 Broadway, New York, NY 10019). ■

MEALEY'S: EMERGING INSURANCE DISPUTES
edited by Jennifer Hans
The Report is produced twice monthly by

1600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA
Telephone: (215)564-1788 1-800-MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com
Web site: http://www.lexisnexis.com/mealeys
ISSN 1087-139X