SandRun Risk
STRATEGIC | COLLABORATIVE | INNOVATIVE

Insurance Coverage for Cyber-Risk Claims

by

Lori L. Siwik
Founder and Managing Partner
SandRun Risk

and

Wendy Cressman
Senior Consultant
SandRun Risk

Data breaches have resulted in hundreds of millions of data records being illegally assessed. Home Depot, Target, Sony, Kmart, Apple's iCloud, First Commonwealth Bank, and P.F. Chang's are just a few of the companies that recently reported a data breach. According to Business Insurance[1], the number of cyber security incidents has increased 48% this year to 4.8 million. That is equivalent to 177,339 attacks per day. With more and more companies using technology to manage their daily business activities, it is becoming easier for criminals and non-criminals to get access to sensitive information like social security numbers, bank account information, credit card numbers and intellectual property information.

Data breach notification laws have been enacted in every state, but the requirements vary per state. These data breach notification laws are triggered when there has been a breach of personal information, which is not uniformly defined in the statutes. Companies should interpret the laws broadly and err on the side of caution when dealing with a data breach.

Companies that suffer a data breach incur significant costs including but not limited to, forensic investigation costs, breach notification costs, credit monitoring costs, crisis management costs, lost business, and legal/litigation costs. To protect themselves, companies can purchase a

[1] "*Cyber Security Incident Reports Increased 48% This Year*", Business Insurance, September 30, 2014, reported by Judy Greenwald.

specialty insurance policy referred to as "Cyber Coverage." This insurance is usually claims made and can be very expensive, although the costs have come down as more carriers entered the market. It is important that companies review the policy wording carefully to make sure that it meets their business needs. Some policies are better written than others. Cyber policies can provide coverage for first-party (cyber crime) coverage as well as third-party (cyber liability) coverage. They can provide coverage for direct loss and legal liability with resulting consequential loss caused by cyber security breaches. Depending on the policy, there is an ability to insure notification costs, credit monitoring and other direct expenses covered if there is a data breach EVEN if there is never a liability claim. Regulatory fines and penalties are endorsable. Some insurance carriers provide crisis management, a call center, and other services to the policyholder when cyber coverage is purchased.

Alternatively, when faced with a data breach, many companies look to their commercial general liability ("CGL") policies for coverage. CGL policies provide that they "will pay those sums that the insured becomes legally obligated to pay as damages because of 'bodily injury' or 'property damage' to which this insurance applies. "Property damage" is often defined as "physical injury to tangible property, including all resulting loss of use of that property" and "loss of use of tangible property that is not physically injured." Many courts find that data does not amount to "tangible property" because computer information lacks physical substance. *See Ward General Servs. Inc. v. Employers Fire Ins. Co.*, 114 Cal. App. 4th 548, 556-57 (Cal. App. 4 Dist. 2003) (where a computer crash, due at least in large part to human operator error, resulted in data loss, the court held that there was no physical loss or damage. The court held that data loss was simply a "loss of organized information . . . (such as client names and addresses). . . ." concluding that such information "cannot be said to have a material existence, be formed of tangible matter, or be perceptible to the sense of touch"). *See also America Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89,93-98 (4th Cir. 2003); *AFLAC, Inc. v. Chubb & Sons, Inc.*, 581 S.E.2d 317, 319 (Ga. Ct. App. 2003). *But See NMS Services, Inc. v. The Hartford*, 62 Fed. Appx. 511, 514 (4th Cir. 2003) *concurring opinion of Judge Widener.* Other cases reached a different conclusion when that data was actually lost to the owner and not simply stolen. *See Southeast Mental Health Center, Inc., v. Pacific Ins. Co.*, 439 F.Supp.2d 831, 837-39 (W.D. Tenn. 2006); *Lambrecht & Associates, Inc. v. State Farm Lloyds*, 119 S.W. 3d 16, 25 (Tex. App. 2003).

To address court decisions finding coverage under the CGL policies for data breaches, the insurance industry, through the Insurance Services Office ("ISO"), have taken actions to remove cyber coverage from CGL policies. In 2013, ISO introduced an *optional* endorsement that deleted the invasion of privacy related offense (oral or written publication, in any manner, of material that violates a person's right of privacy) from the definition of personal and advertising

injury applicable under Coverage B of the ISO coverage form.[2] Thereafter, ISO introduced several other endorsements that further exclude coverage for data breaches. These endorsements have been approved by insurance regulators in 45 states and became effective May 1, 2014. Each of the ISO endorsements broadly excludes data-related losses as well as those arising from the access or disclosure of confidential or personal information of a person or company. The endorsements exclude damages claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred. In addition to the exclusions, several insurance carriers have revised the definition of "property damage" in the CGL policies to state:

> For the purposes of this insurance, electronic data is not tangible property. As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

Policyholders can expect a fight with their general liability insurance carriers over coverage for cyber risks. There have been a number of lawsuits in the news involving whether CGL policies provide coverage for cyber breaches. For instance, Travelers Indemnity Company of Connecticut recently filed suit against P.F. Chang's seeking a judicial declaration that its CGL policy does not provide coverage for the data breach suffered by P.F. Chang's. In February 2014, a New York State Supreme Court judge held that Zurich American Insurance Company does not have to provide coverage to Sony Corporation of America for the 2011 hacking of the PlayStation Network. Sony has appealed that ruling. In August 2013 Liberty Mutual Insurance Company filed suit against its insured, Schnuck Markets Inc., claiming that it does not owe coverage for the data breach suffered by Schnuck Markets. That litigation was resolved by settlement.

When faced with a data breach, cyber policies and CGL policies are just two of the sources of coverage to evaluate. Depending upon the circumstances, policyholders should also review their commercial property policies, crime policies, directors & officers' liability policies and their errors and omissions or professional liability policies. It may take a while for some insurance carriers to include the exclusions and other language in their policies to limit coverage for cyber breaches. Should a cyber-breach occur, it is worth reviewing the various policies to see what coverage, if any, may be available.

[2] July 18, 2014 Insurance Journal – ISO Comments on the CGL Endorsements for Data Breach Liability Exclusions.