SCHENCK PRICE SMITH & KING, LLP
ATTORNEYS AT LAW
~ Founded 1912 ~

CLIENT ALERT

June 18, 2012

CYBER RISKS AND INSURANCE ISSUES

By: John M. Bowens, Esq.

According to published reports, Twitter has 175 million accounts and gathers 300,000 new users a day. Facebook has approximately 800 million accounts, 50% of whom log on every day. The ubiquitous presence of social media in our private lives is matched byte for byte in our professional lives.

It is virtually impossible for any business to survive without heavy, and in some cases total, reliance upon computer driven data. Much to the dismay of file cabinet manufacturers, customer lists, financial materials, inventory records, correspondence, and every other type of business information is now maintained as cyber data. The unwanted companion to the tremendous benefits of computers is the exposure to "cyber risks."

According to the Norton.com 2011 Cyber Crime Report, the total cost of cyber crime for the past year was $388 billion, consisting of $114 billion in hard costs and $274 billion in lost time. In 2010, the Identity Theft Resource Center calculated that 16 million confidential records were improperly accessed as a result of breaches in computer security. The IBM 2011 midyear report on Cyber risks detailed a review of the Fortune 500 companies and 178 popular websites and found that 40% of them were vulnerable to a cyber attack.

Recent news accounts of the victims of such attacks show that even the most sophisticated organizations are not immune. In April of 2011, Sony advised a congressional committee that its Playstation system had been hacked and information on 77 million customers compromised. That number has since risen to close to 100 million accounts. Sony originally estimated the costs associated with this attack at approximately $200 million dollars but that number is likely to rise significantly. Sony is now in a court battle with its insurance carrier Zurich over coverage for 55 class action suits which have been brought as a result of the cyber breach.

The resolution of the Sony/Zurich suit will turn on the court's determination as to whether a traditional comprehensive general liability ("CGL") insurance policy will provide coverage for liabilities flowing from a cyber attack. Other such lawsuits will undoubtedly be brought around the country as the economic bite of cyber crimes and mishaps are felt by insureds and insurers alike. Given the history of other insurance battles, it is likely that there will be differing views from courts around the country as to what is and what is not covered.

Closely related to the third party liability question, is whether first party policies will provide coverage for the out-of-pocket expenses an insured incurs as a result of a cyber loss. Even where there is no direct damage to a client, and thus no liability concerns, See, Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. N.J. 2011), costs will nevertheless be incurred for notification to clients of the breach. Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have adopted laws requiring notification to be promptly sent to persons whose confidential information has been obtained by a computer hacker.

Subsection (a) of the New Jersey statute provides:

> Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.

N.J.S.A. § 56:8-163.

The costs faced in complying with this statute in a case like Sony's could be astronomical and do not include the ancillary costs of repairing any damage to the system and the prevention of future attacks.

The tension between cyber risks and insurance policies drafted before they were even contemplated was addressed, to a limited degree by the Insurance Services Office ("ISO") in 2001. ISO prepared and made available to insurers an exclusion which provided:

> 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 equipments.

This exclusion applies to third party claims. Its presence or absence in a policy, however, may not be decisive in the ultimate disposition of a claim. Insurance companies view traditional policy language as not providing coverage for cyber losses. Accordingly, many now offer "Cyber Insurance" to cover these risks. As the following discussion will illustrate, courts have reached divergent views for coverage for cyber claims.

TRADITIONAL INSURANCE POLICIES

A. First Party Coverage Issues.

Although the precise language may differ among policies, a first party insurance policy ordinarily provides coverage for "direct physical loss of or damage to or loss of use of covered property." Courts have reached diametrically opposed conclusions as to the meaning of this language.

The focal point of cases to date has been the meaning of the term "direct physical loss." In Port Auth. v. Affiliated FM Ins. Co., 311 F.3d 226,233-234 (3d Cir. 2002) the Court of Appeals for the Third Circuit reviewed a claim by the Port Authority for coverage for costs associated with removing asbestos from the structure of several buildings which it owned. The Port Authority conceded that there was no imminent danger of contamination from the presence of the asbestos. As a threshold matter, the court pointed out that there is an inherent difference between first and third party polices which should be reflected in the courts determination of the meaning of policy terms. Specifically, the Court found that:

> the difference between first and third-party insurance affects a court's interpretation of the policy language. Unlike liability policies, where the public interest in compensation for injured third-parties is a strong factor, in a first-party policy, the extent to which insured persons may protect themselves is a matter that rests in their own determination and judgment. As a result, the relationship between the insurer and insured and the incidence of property damage in first-party matters are generally determined by reliance on traditional contract principles.

The Court went on to favorably cite to a definition of physical damage to property as "a distinct, demonstrable, and physical alteration" of its structure. Id at 235. (Citation omitted.) The Court concluded that since the presence of the asbestos in the buildings did not render them unusable, thus there was no physical loss and no first party coverage available to the Port Authority. While this definition seems straightforward, its application to cyber data has provoked starkly differing interpretations.

In American Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., 2000 U.S. Dist. LEXIS 7299, (D. Ariz. 2000), the district court considered a claim by the insured for data losses which occurred after a power outage. The court analyzed the meaning of "physical loss" under a business interruption policy and concluded that the loss of data did, in fact, constitute physical loss to the computer system and was covered under the policy. Southeast Mental Health Ctr., Inc. v. Pac. Ins. Co., 439 F. Supp. 2d 831 (W.D. Tenn. 2006). Cf. Wakefern Food Corp. v. Liberty Mut. Fire Ins. Co., 406 N.J. Super. 524 (App.Div. 2009)(Electrical grid was "physically damaged" because it was out of service for several days.)

In Ward General Ins. Services, Inc. v. Employers Fire Ins. Co., 114 Cal. App. 4th 548 (Cal. App. 4th Dist. 2003), the intermediate California appellate court addressed a claim by an insurance agency for the costs associated with the reprogramming of its computer system after a "crash" during a changeover of the system which resulted in the loss of significant data. The Court summarized the claim and coverage question presented as:

> [t]he risk encountered in this case was a negligent computer operator, or, perhaps, a defective computer program. Unless the harm suffered, i.e., the loss of electronically stored data without loss or damage of the storage media, is determined to be a physical loss,' we cannot say that the risk encountered in this case, a negligent operator, constitutes a risk of direct physical loss. We do not understand that a computer operator, sitting at a keyboard

> pressing keys or moving a mouse, presents any other relevant type of risk. Thus, under either an ordinary or a strained interpretation of the phrase 'direct physical loss of or damage to Covered Property,' coverage for plaintiff's claim under the [insurance policy] depends on whether the loss of electronically stored data, without loss or damage of the storage media, constitutes a 'direct physical loss.'

Id at 554.

In concluding that the loss was not covered, the Court reasoned:

> A 'database' is a 'large collection of data organized esp. for rapid search and retrieval (as by a computer).' (Merriam-Webster's Collegiate Dict. (10th ed. 1993) p. 293.) "Data" is defined, quite simply, as factual or numerical "information." (*Ibid.*) Thus, the loss of a database is the loss of organized information, in this case, the loss of client names, addresses, policy renewal dates, etc.
>
> We fail to see how *information*, *qua* information, can be said to have a material existence, be formed out of tangible matter, or be perceptible to the sense of touch. To be sure, information is stored in a physical medium, such as a magnetic disc or tape, or even as papers in three-ring binders or a file cabinet, but the information itself remains intangible. Here, the loss suffered by plaintiff was a loss of information, i.e., the *sequence* of ones and zeroes stored by aligning small domains of magnetic material on the computer's hard drive in a machine readable manner. Plaintiff did not lose the tangible material of the storage medium. Rather, plaintiff lost the stored *information*. The sequence of ones and zeros can be altered, rearranged, or erased, without losing or damaging the tangible material of the storage medium.

Id at 556. See, GTE Corp. v. Allendale Mut. Ins. Co., 372 F.3d 598 (3d Cir. 2004) (No "physical loss" where computer system had to be upgraded in anticipation of Y2K concerns.)

While it seems clear that damage to a computer system itself, by a covered peril, would qualify for first party coverage, there are no guarantees that a loss of cyber data would be treated the same way. Ancillary costs, such as notification to clients or customers would almost certainly not be covered by traditional policies, at least under first party policy provisions.

B. Third Party Coverage Issues.

The standard CGL policy provides coverage for legal liability of the insured caused by an "occurrence" resulting in property damage (or bodily injury) during the policy period. An "occurrence" is regularly defined as "an accident, including exposure to conditions." Property damage is ordinarily defined as "physical damage to or destruction of tangible property, including loss of its use."

In Am. Online, Inc. v. St. Paul Mercury Ins. Co., 207 F. Supp. 2d 459, 466 (E.D. Va. 2002), AOL sought coverage from its insurer St. Paul for defense and indemnity with respect to a number of class action law suits alleging that AOL 5 caused damage to software and data on computers of its customers. The court framed the first issue before it as "whether computer data, software and systems are tangible property." AOL contended that these items were tangible property because they are "capable of being realized." The court disagreed and found that:

> … the plain and ordinary meaning of the word tangible is something that is capable of being touched or perceptible to the senses. *See* *Lucker Mfg. v. Home Ins. Co.*, 23 F.3d 808, 818 (3rd Cir. 1994) ("Tangible property is property that can be felt or touched, or property capable of being possessed or realized."). *See also* Paul M. Yost, *et al., In Search of Coverage in Cyberspace: Why the Commercial General Liability Policy Fails to Insure Lost or Corrupted Data,* 54 SMU L. REV. 2055, 2066-68 (2001) (discussing in detail various dictionary definitions of the term tangible and the word's etymology to conclude that "tangible property" is limited to corporeal items). Computer data, software, and systems do not have or possess physical form and are therefore not tangible property as understood by the Policy. *Cf.* *Lucker Mfg.*, 23 F.3d 808 at 820-821 (noting that "by making 'tangibility' the touchstone of coverage, the [insurance policy] excludes significant class of property for which liability insurance could be provided - property like system designs or computer software.").

> Computer data can be transmitted and stored in a variety of ways, but none of them renders the data capable of being touched. A "bit" on a computer disk or hard drive is not palpable. Electrical impulses that carry computer data may be observable with the aid of a computer, but they are invisible to the human eye. *See Advanced Computer Servs. v. MAI Sys. Corp.*, 845 F. Supp. 356, 363 (E.D. Va. 1994) ("electrical impulses of a program in a [Random Access Memory] are material objects, which although themselves imperceptible to the ordinary observer, can be perceived by persons with the aid of a computer."). An ordinary person understands the term "tangible" to include something she can touch, such as a chair or a book, not an imperceptible piece of data or software that can only be perceived with the help of a computer.
>
> Excluding computer data and software from the meaning of the term tangible is consistent with the only reported case that directly addresses whether such property is tangible for insurance coverage purposes. In reviewing policy language substantially similar to the case at bar, the court in *State Auto Property and Casualty Insurance Co. v. Midwest Computers & More* tackled the issue of whether an insurer owed a duty to defend a policyholder against claims alleging negligent performance of service work on a computer system causing computer data loss. 147 F. Supp. 2d 1113 (W.D. Okl. 2001). Relying on the ordinary meaning of the term "tangible," the court succinctly found that "computer data cannot be touched, held, or sensed by the human mind; it has no physical substance. It is not tangible property." 147 F. Supp. 2d 1113 at 1116. Accordingly, the court found that the insurer did not have a duty to defend against claims of data loss. *Id.*

Id at 467-468. In reaching its decision, the court specifically rejected the reasoning in Ingram, supra.

In Seagate Tech. v. St. Paul Fire & Marine Ins. Co., 11 F. Supp. 2d 1150 (N.D. Cal. 1998), Seagate sought coverage from St. Paul for a suit by one Seagate's customers, Amstrad, claiming that disk drives supplied by Seagate were defective resulting in damage to Amstrad. The St. Paul policy at issue provided coverage for property damage which was defined as "physical damage to tangible property of others, including all resulting loss of use of that property." Id at 1153. The court rejected Seagate's claim finding that while Amstrad's complaint alleged loss of customer information, loss of business and damage to Amstrad's reputation, absent was any suggestion that components of the host computer, other than the Seagate drives, suffered damage. Thus, there was no coverage. Implicit in the Court's holding is that the customer information data which was lost did not constitute "tangible" property for purposes of coverage.

CONCLUSION

Given the uncertainty with respect to coverage under a standard CGL policy for losses of cyber data, businesses which could potentially lose confidential client records or crucial operational information, need to give serious consideration to cyber insurance to protect them from potential losses. The Ponemon Institute has estimated that the cost associated with a cyber breach in 2010 averaged $214 per lost confidential record. Even for smaller companies, the loss potential associated with cyber risks can be catastrophic.