

By Steve Schoenberger, VP & Technology Liability Practice Leader

A Brief Overview of Insurable Cyber Risk

Insurable cyber loss is broadly categorized in two parts: damage to your system and third party liability. Damage to your system is often referred to as first-party loss and includes damage, loss or corruption of data and software arising out of non-tangible events such as virus, hack, power surge or programming error. Insurance is provided to cover your costs to research, reconstruct or recreate the lost or damaged data. Insurance coverage is also available for any loss of income arising from the preceding damage. It is important to note that the loss of income provided by cyber policies is not just a loss of income generated directly by online sales, but also includes subsequent offline business loss, such as the loss of billable hours at a law firm. A third type of first-party cyber loss is additional operating expense, which could include the additional cost associated with temporary manual work-arounds, the setting-up of hot-sites, and other expenses associated with maintaining routine operations.

Cyber liability loss includes injury arising out of “content” or information either made available for public viewing on a website, secured deep in a corporate database or distributed through email. Typical infringement claims arising out of website content include libel, defamation, and trademark or copyright infringement. An even greater source of cyber liability is the unauthorized access of confidential information, be it client data, trade secrets, personal health records or financial information. Most organizations have some type of information that, if released, could lead to third party claims; the most obvious is employee and credit card information. However, every company connected to the Internet will have the potential for liabilities arising out of intentional or unintentional network harm to a third party due to virus transmission, a DDOS attack where they are a host or some other malicious use from or through their system. The requirements of many state and federal regulations such as HIPAA, GLBA and SOX have heightened the awareness of potential plaintiffs and, in some cases, creating a standard duty of care against which a civil suit could be based.

Short History

Standard insurance policy language was developed long before the IT revolution. Prior to the late 1990s, there was a minimal amount of language designed to expressly include or exclude coverage for cyber risk. As more and more companies began to rely on their information infrastructure, underwriters were hit with a wave of new claim activity arising from unanticipated sources. Manufacturers and retailers were being sued for torts that were originally associated with advertisers such as trademark, copyright and libel arising out of things like deep linking, framing and metatags. Companies began to file claims against property policies for first-party data loss and software damage. Underwriters either paid the claims because the policy language was indefensible or litigated the intent. In 2000, *Ingram Micro v. American Guaranty*, Ingram Micro successfully argued that physical damage covered by a property policy included harm to circuitry and subsequent loss of use of that property.

Mason & Mason Technology Insurance Services, Inc.

458 South Avenue | Whitman, MA 02382 | T: (+1) 781-447-5531 | F: (+1) 781-447-7230 | www.masoninsure.com

Two years later, *AOL v. St. Paul Mercury Insurance*, St. Paul successfully argued that the programming damage AOL caused to computer owners using AOL 5.0 was not tangible property damage and therefore not eligible for coverage under a general liability program. The issue of whether or not data damage is tangible physical damage or not has been at the core of coverage disputes regarding data and software damage.

Since around the year 2000, the trend in the courts and in the insurance community at large has been an acceptance that the standard property and liability insurance programs are NOT designed to respond to typical cyber claims. The addition of specific cyber exclusions on standard package programs and the offering of express coverage through endorsements or stand-alone policies have strengthened the insurers' arguments against coverage in core insurance programs.

The push to create a new insurance market for cyber coverage came to head around 2000 with about half a dozen insurers aggressively marketing distinct programs. The expectation was that a new marketplace would quickly develop as it had for employment practices in the early 1990s and pollution liability in the 1980s. Stand-alone employment practice and pollution policies became very popular when express exclusions were added to standard general liability programs.

The market for express cyber coverage is showing signs of life specifically in the areas of healthcare and banking due, in large part, to the sensitivity of the information and the increasing reliance on information technology. However, the general consensus is that the market has been slow to develop. The big push for cyber coverage roughly coincided with a hardening of the insurance marketplace. Underwriters were offering a new line of coverage while insurance buyers were trying to find ways to cut their insurance costs. It is hard for CFO or risk managers to think about adding a new line of coverage when they are thinking about reducing limits or dropping coverage on core insurance programs. In addition to poor timing, unlike pollution and employment practices liability, cyber risk for most of us is more ephemeral and the probability and costs are not nearly as well understood. When a building burns or people die from pollution or government officials are sued for harassment, the public is well aware and the cases are sensational. When a company has its security breached and suffers financial loss, the last thing it wants to do is augment the harm with a lot of publicity. Better to keep quite than alert the competition and open the company to further litigation.

A general lack of understanding on both the buyer's and seller's side has also hampered the growth of the market. Quantification of the risk has proven difficult, especially on the first-party side. In addition, corporate risk managers generally do not have the technical understanding to access the value of risk transfer; and most insurance brokers are in the same boat. Policy language, especially on the first-party side, is new and requires much more time and effort for both the insurance broker and buyer to complete a thorough analysis and understand the coverage options. To date, few companies have successfully integrated IT into the corporate insurance decision process. While many executives today will agree that non-tangible information assets are more important than their physical assets, few have yet ventured into insurance for their non-tangible assets, although the focus is changing for at least some industries.

Mason & Mason Technology Insurance Services, Inc.

458 South Avenue | Whitman, MA 02382 | T: (+1) 781-447-5531 | F: (+1) 781-447-7230 | www.masoninsure.com

Shortcomings of Traditional Products

Traditional property policies are designed to protect tangible property against tangible property perils such as fire, flood and earthquake. Typical property policies also require a tangible property loss before they will pay any business interruption or extra expense loss. To ensure that non-tangible data claims are not paid, many insurers have also added explicit exclusions pertaining to non-tangible assets, such as data information stored in electronic format. Traditional crime policies, also built around insurance for tangible property, often exclude the theft of information such as trade secrets.

Most general liability programs also share the same tangible/non-tangible property damage issue. General liability programs are typically drafted to respond to tangible property damage. Many general liability programs also have a narrow scope of coverage for “advertising and personal injury,” but it is now common to see language designed to specifically exclude cyber related activities such as chat rooms and banner ads.

Errors and omissions or professional liability programs purchased by software or other service companies may provide coverage for some third-party cyber liabilities, but the policy should be carefully reviewed, and it is unlikely to protect against all of the liabilities previously discussed. There is often language that effectively excludes claims arising out of security breaches, the release of confidential information or acts by rogue employees. In addition, errors and omissions coverage is generally limited to claims arising out of the delivery of a specific service. Errors and omissions coverage may not respond to claims arising out of a network unrelated to the delivery of a product or a service, such as the spread of a virus to an affiliate or supplier.

Steve Schoenberger is the VP and Technology Liability Practice Leader at Mason & Mason Technology Insurance Services Inc. Prior to joining Mason & Mason, he managed AIG’s Technology & Professional Liability underwriting for the Boston Region. Steve works with a broad range of life science and technology companies from pre-funded to mid-cap public companies and can be reached at sschoenberger@masoninsure.com or 781-447-5531 x140.

Mason & Mason Technology Insurance Services, Inc.

458 South Avenue | Whitman, MA 02382 | T: (+1) 781-447-5531 | F: (+1) 781-447-7230 | www.masoninsure.com