CLM CLAIMS & LITIGATION MANAGEMENT ALLIANCE™

ADVANCING ETHICS, COOPERATION AND EDUCATION

CLM 2015 New York Conference
December 3, 2015 in New York City

Tea Leaves and Coverage: Emerging Coverage Issues In Cyber Litigation

I. Cyber Liability

A. Sources of Cyber Exposure for Data Breaches

Malicious attacks remain a significant source of cyber liability exposure in the context of security data breaches, network security events, and the loss of personally identifiable information ("PII"). According to Ponemon Institute's 2014 Cost of Data Breach Study (United States), 44% of reported network breach events were caused by malicious attacks. What may surprise some is that 31% of network security events were caused by employee negligence. Employee negligence may include lost laptops or smart phones containing corporate data, weak passwords and the transfer of unencrypted files, working from home on unsecure (or less secure) servers, and poor waste management. While third-party attacks remain a significant source for cyber exposure, corporate personnel behavior is becoming an increasingly significant source for data breaches. It is also becoming an area of focus for underwriting cyber risks.

B. Sources of Cyber Liability From Data Breaches

Litigation remains a significant source of cyber liability, both in terms of defense costs and legal liability. Typical class action lawsuits involve putative classes comprised of members of the breach-victim's customer base. More recently, such as in class action lawsuits filed against Sony Pictures and Uber, lawsuits also involve putative classes of the breach-victim's current or former employees. Typical claims alleged in these lawsuits include invasion of privacy (based both in the common law and state constitutions), breach of data protection statutes, such as the California Consumer Records Act, increased risk of identity theft, failure to comply with "industry standards," negligence, costs incurred in lost time for protecting one's credit, and costs incurred from subscribing to third-party credit monitoring services.

47 different states, have notification statutes that require a breach-victim to notify either persons whose information was compromised in a data breach, or the state's Attorney's General office, or both, upon the discovery of a network security event and loss of PII. Some federal statutes have notification requirements, such as the Health Insurance Portability and Accountability Act.

Deadlines for providing notification, as well as whom to notify, depends upon a myriad of issues, not the least of which is what jurisdictions are affected (many of the states' statutes

differ), whose information was compromised in the data breach, whether the compromised information was encrypted, whether there is a perceived likelihood of harm (although not every statute has this trigger), and whether the breach-victim owned the lost data. Deadlines can be days, not weeks or months. Many class action lawsuits also now allege failure to comply with notification statutes, terms of either the timing of the notification or its manner or form as an independent basis of liability.

Federal agencies are becoming more involved with network security breach events. The Federal Trade Commission considers it a violation of Section 5 of the Federal Trade Commission Act if a company fails to comply with the network security measures procedures it advertises or discloses to the public.

II. Types of Cyber Coverage: CGL Policies

A. Coverage B – "Oral or Written Publication, In Any Manner, of Material that Violates a Person's Right of Privacy."

If the history of cyber insurance coverage were divided into chapters, Chapter One would be "personal and advertising injury" under Coverage B of commercial general liability ("CGL") policies. Coverage B of CGL policies defines "personal and advertising injury" as injury arising out of certain enumerated offenses, including "oral or written publication, in any manner, of material that violates a person's right of privacy." In the non-cyber context, courts around the country have struggled with the meaning of the terms "publication" and "right of privacy." While the latter term has not received much, if any, attention in the context of network security events, the issue of the meaning of "publication" has garnered attention from the courts.

In the non-cyber context, courts have attributed different meanings to the term "publication" within the "personal and advertising injury" offense for "oral or written publication, in any manner, of material that violates a person's right of privacy." The issue is whether the term "publication" requires widespread dissemination (the standard for invasion of privacy claims), or dissemination to a third person only (the standard for defamation)? Does the word require dissemination at all? Some courts have required that material must be distributed to the public at large. Other courts require only a disclosure to a third party, and not widespread dissemination. Some courts have gone so far as to eschew the requirement that the information be disseminated at all.

In the cyber context, courts have focused their attention upon the accessibility of the information at issue. If there is no evidence that the data is accessible, such as if encrypted data tapes were lost, some courts have determined that regardless of the precise definition of publication, access is a necessary prerequisite to the communication or disclosure of personal information. Thus, there can be no "publication."

On the other end of the spectrum, if the information was accessible but was never accessed, some courts have rejected the contention that the absence of anyone actually accessing the information means that there has been no "publication." These courts have held that a publication occurs when information is placed before the public, not when a member of

the public reads the information placed before it. Some courts also have held that the mere access to information by a hacker constitutes a "publication." No court has addressed the phrase "publication, *in any manner*" in the context of a network security event.

B. Coverage A – "Property Damage"

Coverage A of CGL policies provides coverage for all sums the insured becomes obligated to pay as damages because of "property damage." "Property damage" is defined in part as "loss of use of tangible property that is not physically injured." Financial institutions have begun to sue retailer breach-victims for losses they have incurred through forgiveness of fraudulent charges and, perhaps more relevant for purposes of insurance coverage, the need to replace deactivated debit/credit cards. Would claims for those costs constitute loss of use of tangible property that is not physically injured to satisfy the definition for "property damage"? This issue has not been addressed by the courts. Some believe that it does.

A counter-argument to the position, however, is that most, if not all CGL policies state within the definition for "property damage" that "[f]or the purposes of this insurance, electronic data is not tangible property." The Electronic Data exclusion also may be implicated. One may argue that, for purposes of coverage, it is the deactivated electronic data on the debit/credit cards that causes any loss or damage, *not* the plastic cards themselves. Whether this coverage issue will be the subject of litigation is unclear.

C. Access/Disclosure of Confidential/Personal Information Exclusion

The Access or Disclosure of Confidential or Personal Information and Data-Related Liability exclusion is new. The exclusion should effectively end potential windows of coverage in CGL policies for Network Security Data Events. For Coverage B, the data disclosure exclusion applies to prohibit coverage for "'personal and advertising injury' arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, . . . financial information, credit card information, health information or any other type of nonpublic information." The exclusion applies "even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of any access to or disclosure of any person's or organization's confidential or – personal information." A near verbatim exclusion exists for Coverage A.

The exclusion has not yet been tested by the courts. Nor can it be said that every CGL policy currently issued includes this endorsement – some older policy forms still may be in use. This endorsement should shut the window for data breach coverage under CGL policies. But for those who believe that the window inescapably will shut quickly, heed this warning: Many industry analysts believed the same thing about the TCPA exclusion for junk fax litigation.

III. Cyber Insurance

A. Network Security Coverage

Cyber insurance policy forms are a lot like snowflakes. At first glance, they look very similar. Indeed, to the non-discerning eye, they may even look the same. However, a careful examination of the policies reveals they are all quite different, whether because they have been drafted by different insurers, they are intended to cover slightly varying forms of risk, or are subject to different evaluations when determining to underwrite cyber risks.

Network Security Coverage in cyber insurance comes in varying forms, but every coverage form is intended to provide third-party liability coverage for three essential events: the failure to prevent unauthorized access to a computer system; the failure to prevent the transmission of a virus or malware; and the failure to ensure authorized access into a computer system. Coverage for liability from unauthorized access to a computer or hacking event – usually is the most prominent coverage sought. As discussed below, the terms of these coverage forms, however, can have a significant impact on the scope of the network security coverage.

A second important and related form of coverage is for first-party costs, sometimes referred to as Crisis Management coverage. Generally, this coverage is intended to provide first-party coverage to the breach-victim for costs, including legal expenses incurred when addressing a network security event, including costs, incurred for complying with state and federal notification statutes, computer forensics work required to identify the source of the breach, the information taken, and steps necessary to patch the breach. Sometimes, coverage also will include costs for public relations, efforts, and call centers to enable third parties, whose PII has been compromised, to contact the breach-victim. Some Crisis Management coverage forms also may offer coverage for regulatory enforcement actions; although, many cyber insurance forms require that such coverage to be purchased separately, to the extent it is if available at all.

B. Coverage Issues for Network Security Coverage

1. Unauthorized Access

The term "unauthorized access," or a very similar term, is a central component to network security coverage. Yet few, if any, cyber insurance coverage forms define it. What does "unauthorized access" mean? Does it mean hacking from outside sources: presumably, few would argue against such an interpretation. However, does it also involve officers or employees inside the company who use their access to sensitive information in an unauthorized manner for illicit purposes? The topic has garnered considerable attention in the context of the meaning of the phrase "exceeds authorized access" under the Computer Fraud and Abuse Act ("CFAA"), the preeminent federal anti-hacking statute. Relatively recent developments in case law have significantly altered the courts' view of the scope of the phrase.

The CFAA, 18 U.S.C. § 1030(a)(4), provides that whomever "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value … shall be punished." The statute defines "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *See* 18 U.S.C. § 1030(e)(6).

The first courts to address the meaning of the phrase held that the phrase "exceeds authorization" could apply to officers or employees who used their corporate positions to access data in an unauthorized manner. These courts focused on a breach of agency test: if the employee's actions breached his or her fiduciary duty to the employer, the acts were unauthorized. Other courts employ an intended use analysis. They hold that if the actor has reason to know that the intended use of the data exceeds norms of company authorization, such as to engage in an illicit activity, the actions are unauthorized.

More recently, many courts have rejected these approaches. Instead, the phrase "exceeds authorized access" under the CFAA is limited to violations of restrictions on access to information, and not restrictions on the information's use. If a person otherwise is permitted access to information, accessing that information, even for illicit purposes and in breach of any duty owed to the company, does not satisfy the definition of "exceeds authorized access" to implicate liability under the CFAA. In the context of cyber liability coverage, one court adopted a similar position, holding that the phrase "fraudulent entry" into a computer system was limited to instances of outside hackers, not fraudulent content submitted by authorized users.

2. Insured's Acts or System

Some Network Security Coverage forms define the scope of the insured risk by the insured and its computer system. Specifically, some coverage forms define a covered act or loss as one caused by an error or omission of an insured under the policy, as opposed to an error or omission committed by a third party. Other policy forms may limit the meaning of the network to those systems owned and operated by the policyholder. To be clear, there is nothing wrong about that. However, these limitations in coverage should be discussed between insurer and policyholder to ensure that each party has a firm understanding of the scope of the insurance contract.

In the alternative, a policyholder or insurer may wish to enter into an insurance contract that defines a covered network security event as a failure to protect confidential information, or the failure to prevent an unauthorized access into a computer system without qualifying the identity of the negligent actor or the ownership of the system involved.

3. Terrorism Exclusion

With the increased of cyber espionage and state-sponsored hacking, terrorism exclusions have become much more significant the perhaps first anticipated for defining the scope of Network Security Coverage. A typical terrorism exclusion may prohibit coverage for loss arising from:

any act or threatened act of terrorism, including but not limited to the use of force or violence, of any person(s) or group(s) of persons whether acting alone or on behalf of or in connection with any organization or government, committed for political, religious, ideological or similar purposes including the intention to influence any government and/or to put the public, or any section of the public, in fear.

Thus, the exclusion could apply to any network security event caused by an organization acting for political, religious, ideological or similar purposes. This exclusion has a potentially broad scope that may bar coverage for hacking committed by a foreign government or an organization purportedly acting on behalf of a foreign government. It could apply to an event caused by Anonymous or other hack'tivists. Could it apply to a disgruntled employee who takes action against an employer for political or religious reasons, or similar purposes? Perhaps. Courts have not addressed the issue.

IV. Trends

A. Litigation – Article III Standing

For a time, Article III standing presented a significant defense for breach victims who were later sued in putative class action lawsuits comprised of consumers whose information was compromised. Standing derives from Article III of the U.S. Constitution, which limits the powers of the federal judiciary to the resolution of "cases" and "controversies. To maintain a lawsuit, every plaintiff must plead and ultimately prove that he or she has suffered sufficient injury to satisfy the "case or controversy" requirement. At the pleading stage, a plaintiff must allege an injury-in-fact that is concrete and particularized, as well as actual or imminent; that the injury is fairly traceable to the challenged action of the defendant; and that the injury can be remedied by a favorable ruling. If the plaintiff cannot satisfy this criteria, the claim must be dismissed.

Data breach class action lawsuits typically assert boilerplate allegations of invasion of privacy, increased risk of identity fraud, and costs incurred from having to subscribe to third-party credit monitoring services. Some courts have held that these boilerplate assertions do not allege concrete and particularized (and actual or imminent) injury to confer standing.

Other courts, however, have found standing where there was evidence that the data thief or hacker had "deliberately" targeted the information that was compromised in the network security event. These courts distinguish decisions rejecting the presence of Article III standing on the basis that those cases involved the theft of devices in which there was no evidence that the PII had been targeted by the thief, or that the thief even had any intention or capability to access the data.

B. Emerging Coverage Issues

1. Fewer Restrictions Tying Coverage To An Insured's Error or Breach of An Insured's System

Policyholders recognize that cyber risk extends beyond the errors or omissions of their employees. The source of the Target data breach for instance, has been traced back to an employee of a Target HVAC vendor who feel victim to a phishing scam. For purposes of illustration here, it is important to note that the vendor employee was not an employee of Target. Similarly, Policyholders realize that exposure lies beyond data contained in their systems. Companies may employ cloud systems and resources, or store information offsite. More and more employees use personal smart phones for work, and they bring work home and use home computers. A network security event can take place beyond a system owned by the insured.

As a result, limitations on the scope of Network Security Coverage to the errors and omissions of an insured, or to network security events on an insured-owned system, may become less common. However, because of premium pricing, and less sophisticated corporate data protection policies, these restrictions may remain in place for policies issued in the middle and lower markets.

2. Minimal Practices and Misrepresentation

Cyber risk can involve catastrophic amounts of money. It is beyond doubt, therefore, that through underwriting when assessing the cyber risk to be insured is critical. As part of that underwriting process, an insurance carrier can be expected to investigate security measures and data protection policies employed by the applicant company. What happens if the company ultimately fails to observe those security measures or policies, or even flout minimal industry standards for securing data and its network? Would such a practice constitute a misrepresentation in the underwriting and application process? Would there be additional grounds to call coverage into question? These are the precise issues being litigated in one coverage case involving a Failure to Follow Minimum Required Practices exclusion, which prohibited coverage for loss based upon, directly or indirectly arising out of, or in any way involving:

> Any failure of an Insured to continuously implement the procedures and risk controls identified in the Insured's application for this Insurance and all related information submitted to the Insurer in conjunction with such application whether orally or in writing[.]

The insurer argued that Cottage Health had failed to maintain adequate security in its network, including the failure to "continuously implement the procedures and risk controls identified in its application"; to "regularly check and maintain security patches on its systems"; and to "enhance risk controls." (Complaint, ¶43.) The insurer also alleged in its complaint that Cottage Health's failure to maintain adequate security measures constituted a misrepresentation in its application, thereby voiding coverage. This coverage action remains in its early stages. Yet, as underwriting procedures for cyber insurance become more complex and thorough, the likelihood of intentional or unintentional misrepresentations or omissions about a company's network security could result in significant questions of coverage should a network security event take place and the security measures disclosed in the application process have not been followed.

3. Intentional Misconduct Exclusions

Network Security Coverage covers the negligence of an insured, not the intentional acts of an insured. One recent case, which perhaps received an inordinate amount of attention because it has been hailed as the first cyber insurance coverage opinion, has a simple message: even in the cyber world, intentional misconduct is not negligence. The essential facts of the case are that the insured was a vendor that held and processed third-party data of its customers. When one of its customers demanded the return of the data as part of an asset sale, the insured refused to return the data until customer satisfied certain financial demands beyond those provided for in the vendor agreement. When the costumer later sued, was sued, the insured sought coverage under a cyber insurance errors and omissions policy.

In the declaratory judgment action, the insurer argued that it had no duty to defend because the underlying lawsuit alleged intentional misconduct only. The court agreed, holding that because the underlying action did alleged that the insured knowingly withheld this information and refused to turn it over until the plaintiff met certain demand, there were no alleged errors, omissions, or negligence to implicate coverage.