2016 CLM Annual Conference
April 6-8, 2016
Orlando, FL

New Developments in Intellectual Property, Media and Cyber Coverage Issues

I. Introduction to Coverage for Cyber Events

Key Terminology

To understand a discussion of cyber events, it is essential to know the key terms typically used by the industry to describe such events. The following are some of the central terms:

- Data Breach—disclosure of sensitive information to an unauthorized party.
- Security Incident—an event that compromises the confidentiality and integrity of data (distinct from Data Breach in that a Security Incident does not require the disclosure of the information, just that it be compromised).
- PII—Personally Identifiable Information, such as name, address, social security number, date of birth, or anything else that would identify an individual.
- PHI—Protected Health Information, such as health status, health care, payment information linked to an individual, medical records, medical payment history, and similar information.
- FII—Financially Identifiable Information, such as credit card numbers of bank account information.
- DDoS—Distributed Denial of Service, which involves an attempt to make a network resource unavailable to users. This often targets sites and services on high profile web servers like banks, credit card payment gateways, and retailers.

Framework of a Cyber Event, Common Types, and Industries at Risk

Cyber events take many forms, and the actions, impact, and motivations vary widely from event to event. Due to the number of recent high profile cases in the news over the

past few years, most people think of cyber events as malicious third party hacks that steal data. However, cyber risk goes far beyond that. Actions leading to a cyber event can be as simple as the theft of a PC from the home of an employee that provides the thief with access to the network key and/or data to an entire company. Similarly, a cyber event does not have to be intentionally caused at all. Some of the most harmful events in recent years have been caused by human or mechanical errors that lead to information being compromised, destroyed, and/or leaked to the public.

Similarly, the harm caused by a cyber event can present in a number of ways. Most frequently, the only impact that gets attention is what happens to the comprimised data, whether it is stolen, deleted, or corrupted. However, the insurable loss goes beyond that. Cyber events frequently lead to significant business interruption claims, as whole systems can go down for a substantial length of time, bringing a company's operations to a halt, or at least causing a significant slowdown. Similarly, there can be actual property damage, both in the form of computers and software destroyed or, in some cases, where collateral property is damaged through a malfunctioning network (like water damage caused by fire sprinklers being improperly triggered). Also, cyber events cause significant intangible damage, particularly to the reputation of the injured company. For instance, customers will be slow to return to a company that leaked customer credit card information or health information, and business could suffer for years. When looking at a single event, therefore, it is essential to consider all aspects of that event, and not just look to the obvious harm.

Finally, the motivations leading to cyber events, assuming that those events were intentionally caused at all, can take many forms, and can be therefore difficult to predict. The classic motivation, of course, is greed, such as in the theft of credit card information or other financial data. However, some of the most harmful breaches have been motivated by social or political activism, or just a hacker seeing if she was skilled enough to pull it off. Also, it bears mentioning in the current political climate that more sinister motivations may be on the rise. Cyber espionage is becoming more common, particularly as used by countries like China and Russia. Similarly, there is a growing concern that terrorist groups like ISIS will use cyber terrorism to cause widespread, and difficult to trace or prevent, damage. Given the many sources of the threat, therefore, it is unsurprising that cyber events become more and more common every year, and that they are a risk that will not be going away, or even diminishing, anytime soon.

Any company that relies upon a computer network—which is to say virtually any company—is at risk for a cyber event. However, some companies are particularly popular targets because of the information that they keep on those networks. Specifically, the healthcare, financial services, retail, professional services, technology, education, non-profit, entertainment, hospitality, and telecommunications industries are the most highly exposed industries for cyber event. These industries are the most vulnerable because they handle large quantities of sensitive information, and, all too often, do not have the necessary defenses to protect against cyber events.

Coverage for Cyber Events

Traditional Policies

While cyber events are becoming increasingly common, many insureds still have not purchased insurance for these events, as cyber insurance is still an emerging industry with only a limited number of products on the market. A number of companies, therefore, will try to obtain coverage for these events through their traditional policies. These policies can have significant limitations responding to cyber events, however, as such events are not their intended purpose.

CGL Policies

Probably the most common traditional policy that insureds turn to after a cyber event is their commercial general liability (CGL) policy. Coverage under CGL policies for cyber events is a complex topic with too many nuances to discuss here, but there are a few general principles that can guide coverage in most situations. Courts nationwide are currently divided on whether electronic data is "tangible property" covered by Coverage A of a standard CGL policy (though they are generally agreed that the tangible property storing the data will be covered). Under Coverage B, some types of cyber events may be covered as an advertising injury, such as when the insured itself makes a publication of sensitive data. However, if the publication was done by a third party as part of a malicious attack, most CGL policies will not provide coverage.

Property Policies

While insureds less frequently turn to them, property policies can offer coverage for cyber events, though a common exclusion typically prevents this. Specifically, many policies have exclusions for losses related to electronic data, and such exclusions will generally bar coverage for a cyber event. However, these exclusions are not universally part of property policies, and, without this exclusion, coverage is possible. As noted above, courts nationwide are divided on whether electronic data is "tangible property." Depending on the jurisdiction, a court may find that damage to electronic data is covered as damage to tangible property. This could also lead to coverage for business interruption. Further, cyber events frequently cause traditional, physical property damage that is covered by property policies. For instance, computers and other technological equipment may be damaged in a third party hack or even an unintentional IT error. In other cases, network breaches and hacks can cause even greater property damage. For instance, a malicious hack of a public utility could cause an explosion if it compromised natural gas lines, or a hack of a hydroelectric dam could cause a flood. Just because these events were caused by a cyber event does not affect coverage under a traditional property policy.

D&O Policies

Directors and officers (D&O) policies are also becoming increasingly important for cyber events. As security options are becoming more available and an industry standard for protecting against cyber events is emerging, companies are exposed to breach of fiduciary duty claims if they fail to implement adequate security measures to protect

against a cyber event. For instance, this was one of the claims in the litigation arising out of the Target data breach, where customer credit card information was leaked. D&O policies may provide coverage against such claims.

Employment Practices Liability

Employment practices liability policies may also be triggered by some cyber events. If confidential employee information is breached in such an event, an employment practices liability policy could provide coverage for any subsequent employee lawsuits against the employer for negligence.

Hospital Professional Liability

Similarly, hospital professional liability policies can be triggered by cyber events involving breaches of Public Health Information (PHI). These policies can provide crisis management coverage, as well as coverage for HIPAA fines imposed as a result of the breach.

Cyber Policies

Because of the limitations of traditional policies in responding to a cyber event, there is a growing market for cyber policies that provide coverage more narrowly tailored for such losses. As these policies are new, the coverage offered from product to product still varies more than that offered in the more traditional policies. However, the core coverages are generally the same, and an understanding of these coverages will become increasingly important as cyber events continue to become more common.

A cyber policy is any policy that covers one of three general categories of loss. First, they cover the damage to the insured's own physical assets caused by a cyber event, including data, which a traditional policy would not consider to be tangible property. Second, they cover business interruption caused by damage to the insured's assets or by lack or impairment of external services. Third, they cover third party liabilities (operating much like a CGL policy would) caused by a cyber event, like privacy claims, intellectual property claims, virus transmission, and other third party injury. Some cyber policies also provide coverage for cyber extortion events, like investigative costs and even extortion money that is paid on a credible threat.

II. Discussion of Coverage Available for Specific Fact Patterns

Understanding coverage in the abstract is always difficult. The following fact patterns bring the coverage issues presented by a cyber event to life. Our discussion will center around what coverage is available for these different events.

Claim Scenario #1: Privacy Class Action

This claim arose from a privacy class action against the Insured, which is a company that provides free software to consumers in exchange for their agreement to allow the Insured

to install its monitoring software on their computer. The Insured's software collects data about a user's internet habits, including number of emails and instant messages, types of purchases, amounts of purchases, and vendor sites. The software anonymizes the data on the local machine and sends it to the Insured's "holding facility" for further review and anonymization. The data is then aggregated and sold to various customers of the Insured. The class action alleged that the data was not being anonymized before being transmitted and provided to the Insured's customers. The Court granted the plaintiff's motion for certification of a class of 12 million people—an unprecedented number for a privacy class action.

Claim Scenario #2: Hack of a Major Entertainment Company

This claim arose from a malicious third party hack of the Insured, which is a major entertainment company. The attack disabled and effectively destroyed the majority of the company's computer system, and leaked a significant amount of information to the public, including PII, PHI, and FII of thousands of the Insured's employees and sensitive emails of key executives. The attack also leaked unreleased movies belonging to the Insured for free streaming, significantly damaging the Insured's expected profits on those movies. The Insured faces litigation from the employees whose information was compromised, in addition to its own property damage and business interruption caused by the attack.

Claim Scenario #3: Defamation/Disparagement Litigation

This claim involved litigation between the Insured, a national provider of information and technology services, and Plaintiff after discussions to acquire and/or merge these entities failed. Following these discussions, three of Plaintiff's employees left to join the Insured. Plaintiff filed suit claiming breach of non-disclosure and confidentiality agreements, misappropriation of trade secrets, disparagement and defamation. The suit named several directors and officers of the Insured, although the claims against the D&Os did not survive a motion to dismiss.

Claim Scenario #4: Steel Mill Explosion

This claim arose from a malicious third party attack on the operating system of the Insured, a steel mill. Hackers infiltrated the Insured's business network and took over the controls at the mill. As a result, the Insured was unable to shut down a blast furnace when necessary to prevent overheating, leading to a massive explosion and significant property damage.

Claim Scenario #5 – Fraudulent Wire Transfer

This matter arises from a series of electronic wire transfer payment orders purporting to be from Plaintiff and processed by the Insured on two separate dates. On the first date, the Insured received three such orders which it processed. Four days later, the Insured received nine electronic payment orders which it disapproved on the basis that the orders collectively exceeded plaintiff's wire transfer limit. The Insured contacted the plaintiff

regarding the orders for the two dates and was advised that the plaintiff had no knowledge of any of the payment orders, had not authorized the orders, and had not sent them. Of the twelve fraudulent payment orders that were received from plaintiff, the Insured was able to prevent nine from being sent and two from being executed. One payment in the amount of $500,000 was outstanding.

Claim Scenario #6 – Bodily Injury Claim

The Insured installed train track sensors for City Metro Transit Authority ("Transit Authority"). The sensors were primarily to provide historical metrics of rail use and times so that Transit Authority could improve train schedules, but also provided certain real time relays of information to control centers. Co-defendant provided rail sensors specifically designed to alert engineers and control of pending impacts incidents of rail cars. As a result of sensor failure and human error a collision occurred during rush hour between a speeding car and one parked at a station. The collision received wide spread press coverage as a result of 19 deaths and serious injuries to over 50 people. Bodily injury and wrongful death suits subsequently followed. While the Insured had excellent merit defenses to the claims, the rules of contribution in State would make them equally liable to plaintiffs along with co-defendants in the event that they were found to have any responsibility for the incident.

Claim Scenario #7 – Leak of Pharmacy Customer Information

The Insured is a major pharmacy chain. Two of its employees worked together to steal sensitive personal information from thousands of the Insured's customers, including confidential medical information and PII, to fraudulently obtain credit and credit cards. The Insured has fired the two employees to blame, but is now facing a class action from the customers whose information was compromised, alleging both ordinary negligence and breach of fiduciary duties.