CLM 2016 New York Conference
December 1, 2016
New York, NY

Cyber Claims and Coverage Update

I. Summary of cyber policy coverages

Coverages One Should Expect to See

There are over 70 form policies in the currently in the cyber insurance marketplace. Although this may be the case, there are certain core 1st and 3rd party coverages that are part of most cyber policies. Those coverages include expenses for privacy notification, crisis management, rewards and ransoms, data restoration, defense and settlements. Cyber policies may also provide cover for lost devices, cyber terrorism, regulatory defense and penalties and contingent business interruption coverage.

Common Limitations / Exclusions

Although most cyber policies are robust, there are certain exclusions which are often covered under other standard business policies. Those exclusions include malicious acts by employees, failure to update or patch network devices, employment- related claims, ERISA Act exposures, patent, trade secret and copyright infringement, mechanical or electrical failure and losses from portable and mobile devices. Coverage for these exclusions can usually be obtained through an endorsement.

Underwriting Trends

The wide variety of policies in the marketplace breeds creativity and enhances the product for policy holders. However, this creativity leads to differing levels of terminology to describe similar coverages. This may frustrate a potential customer when comparing different policies from different insurers. Underwriters acknowledge this frustration and the market may be trending to a more uniform nomenclature.

The cyber insurance market is now in its teenage years. A sufficient amount of data has been amassed where analytics and predictive modeling can be useful for quickly generating quotes in some markets. However, these tools are not yet perfected for some larger companies and those in high risk industries. For those entities, it is still necessary

for underwriters to work with Risk Managers and other service providers to properly price and understand the risk level.

As data breaches reach the Board Room, companies are increasing their cyber security and insurance budget. This is leading to a demand for increased capacity and higher retentions. In these circumstances, it is imperative that underwriters get accurate information and really drill down into the potential exposure. With more data breaches in the news on a daily basis, underwriters need to work with brokers and customers to properly address these new marketplace demands.

II. 2015 Cyber Claim Trends

In their 2015 Cyber Claims study, NetDiligence analyzed information about 160 data breach insurance claims from various business sectors. As was the case in 2014, the Healthcare industry reported the most claims with 34, followed by Financial Services with 27, retail with 21, technology with 15, and professional services with 13. The information below and discussed by the panel will be the 160 claims analyzed by NetDiligence.

Claims / Cause of Loss

There are many avenues that could lead a company to file a claim under their cyber policy. More than likely, the cause of loss is due to a hacker (31%), malware (14%), staff mistakes (11%), or rogue employees (11%). Hackers are most likely to enter a network and cause loss by exploiting a weak password, an improperly configured network device or common network vulnerabilities exposed by unpatched operating systems and firmware. Once a hacker enters a network, the goal is to escalate user privileges in such a way as to not to alert any IT resources that may be monitoring logs. Once the appropriate privilege level is achieved, the hacker will begin to exfiltrate Personally Identifiable Information (PII), Personal Health Information (PHI), Payment Card Information (PCI) or other financial data from the database

Malware is a general term which refers to viruses, trojans, ransomware, spyware, or any other software whose intention is to extort money. Malware is no longer created and developed by teenagers exploring the extent of their technical skills. These malicious programs are now being developed by criminal enterprises and state actors to extort money and data or to surveil governmental or business entities.

Ransomware is a particularly popular form of malware that is on the rise over the past few years. In 2015, the FBI received 2,500 reports of ransomware attacks resulting in $24 million in ransoms being paid. In the first quarter of 2016, the FBI reports that Americans have paid $209 million in ransoms.[1] A ransomware attack usually unleashed when an unsuspecting user clicks on PDF attachment (which is disguised as an

[1] http://www.cnbc.com/2016/04/26/ransomware-hackers-blackmail-us-police-departments.html

executable file) or link in an email. This practice is called phishing. The email could be socially engineered and targeted for a particular victim or part of a mass email campaign. According to the 2016 Verizon Data Brach Investigations Report, 13% of the people who were sent emails as part of an internal training exercise clicked on the phishing attachment.

After the victim clicks on the malicious attachment or link, a program is unleashed which encrypts as many local and shared files as possible. The main target of the program are files which impact a user's functionality such as Microsoft Office documents, PDFs, pictures and media files. Unless the company has a proper backup that was not subject to the attack, there is little choice but to pay the ransom. The business model of the hackers is to keep ransoms low and maintain the trust of the computing community in order to encourage payment. The ransom must usually be paid in BitCoin and before the allotted time runs out. If the ransom is not paid in time, the hacker will destroy the files.

The losses stemming from staff mistakes or rouge employees involve transferring money to a hacker posing as a legitimate entity, lost or stolen devices (computers, phones, removable drives, etc.), poor password security protocols, lax encryption practices or employees selling login credentials on the Dark Web. Whether innocent or malicious, PII, PHI, PCI or financial information in the wrong hands can lead to a claim being made under a cyber policy.

Costs

The costs associated with properly handing a cyber incident or data breach are not limited to sending notice to the affected parties and paying for credit monitoring. Of the 160 claims which were part of the 2015 NetDiligence Claims Study ("Claims Study"), 105 involved paying for crisis services. The average costs for crisis services was just under $500,000. This number has decreased substantially since its peak in 2012 of $982,620, which indicates that smaller cyber incidents are being reported.

According to the same Claims Study, there were five main costs associated with a cyber incident/data breach. [2] Those costs are computer forensics, notification, credit monitoring, as well as legal and public relations. Cyber policies may also cover business interruption losses, which could easily exceed the costs associated with the above listed expenses. Insurers paid of the most for notification costs, with an average of $567,777. However, of the 48 claims that paid notification costs, losses ranged from $14 to $15,000,000. As for the other costs, here are the average losses:

Forensics	$261,579
Credit/ID Monitoring	$80,706
Legal Guidance/Breach Coach®	$58,685

[2] It is important to note the difference between a cyber incident and data breach. All data breaches are cyber incidents, but not all cyber incidents are data breaches. A cyber incident becomes a data breach when a data breach notification law of a particular state are triggered. For purposes of data breach notifications, the residence of the party whose data has been compromised controls.

Public Relations	$46,308

The Claims Study identified a smaller number of claims that included costs for legal damages (10%) and regulatory actions (3%). The average cost for legal defense was $434,354 and the average legal settlement was $488,839. As for regulatory actions, the average cost for regulatory defense was $186,125, while the cost for the sole regulatory settlement was $750,000.

Records Exposed

The Claims Study reviewed 104 claims where the number of records exposed was reported. There were 55 claims where PII was exposed with the average number of records being 1,739,373. The range of exposed PII records was between 4 and 80 million. Next, there were 28 claims where PCI was exposed with the average number of records being 8,338,028. The range of exposed PCI records was between 1 and 110 million. In comparison, the average number PHI and financial records exposed were only 10,941 and 260 respectively.

III. Mitigation of Risk & Loss

Preparation for a Cyber Incident

Making sure your policy holders are prepared to respond to a data breach is one of the key factors in mitigating risk and minimizing losses. Some of the tools cyber insurers like to see utilized are network assessments, penetration testing, incident response plans, incident logging protocols, and employee training. Although not necessary when pricing a policy, an underwriter or broker may want to encourage a policy holder to engage in some, if not all, of the exercises outlined above.

Responding to a Cyber Incident

Ensuring that a policy holder responds quickly and properly to a cyber incident is essential to mitigate risk and control loss. Once a policy holder reports a potential incident or claim, the first step is to retain experienced counsel to help the policyholders obtain the necessary advice and vendors to handle the incident. This is important for many reasons, especially to maintain the attorney-client privilege if litigation results from the incident. After consulting with an attorney, a decision will be made as to what steps should be taken and whether an outside computer forensics team should be retained to examine the situation.

If it is determined that it is necessary to retain a computer forensic team, they will analyze the network to determine the extent of the hack, the attack vector, what information, if any, was exfiltrated and how to remedy the breach. It is also a good idea to retain a Public Relations firm in case the cyber incident turns out to be a major data breach. If it is determined that data within the network has been compromised, the attorney will work with the forensic and internal IT team to determine if a particular

state's data breach notification laws were triggered. Even if a state notification law was not triggered, the company may consider notifying the affected parties and offer credit monitoring to prevent a potential public relations nightmare.

If the data breach notification laws for a particular state is triggered, it will be necessary to coordinate notification of the affected parties and the applicable regulatory authority as defined by statute. This will involve retaining a data breach response firm who can coordinate mailing notifications and establishing a call center to answer questions. Although not mandated by statute, the company and the insurer must make a decision as to whether credit monitoring services would be a prudent expense to incur.

It is also important to establish a litigation hold on any documents, whether electronic or physical, in the event that litigation ensues from the incident. Depending on the industry or the state data breach laws, a company may be subject to class and individual actions, as well as fines from state and federal regulators. With this in mind, it is important to ensure that the response to a cyber incident is handled properly.

IV. Recent Developments in Cyber Litigation

Coverage Opinions

After several courts found that cyber losses were covered under Commercial General Liability ("CGL") policies, insurers began to place cyber exclusions into those policies and offered stand-alone cyber policies or coverage through a cyber endorsement. This industry transition was essentially complete in 2014. Since there has been a change in product and coverages, judicial opinions addressing state-alone cyber coverage disputes are just starting to surface.

An example of a Court addressing cyber coverage under a CGL policy can be found in *Travelers Indemn. Co. of America v. Portal Healthcare Solutions, L.L.C.*, 2016 WL 1399517 (4th Cir., April 11, 2016). In *Travelers*, the 4th Circuit affirmed the District Court's decision to grant Portal's Motion for Summary Judgment and directed Travelers to defend its insured under a 2012 or 2103 CGL policy. Travelers sought a declaratory judgment that it did not have a duty to defendant Portal against a class action complaint that did not allege a covered publication of personal information by Portal. *Id.* at *1. The Court found that a "Google" search which returned the medical records of the named plaintiffs and putative class members constituted a publication and was covered under the policy. *Id*. at *2.

With regard to cyber policies, only a few Courts discussed coverage disputes. One example is *Travelers Property Cas. Co. of America v. Federal Recovery Services, Inc.*, 103 F.Supp.3d 1297 (D. Utah 2015). Plaintiffs in *Travelers* sought a declaratory judgment that the insurer had no duty to defend under defendant's CyberFirst technology errors and omissions policy. *Id.* at 1298. Defendant processed membership and payment information for a gym. *Id*. at 1299. The gym entered into a sales agreement with LA

Fitness and requested that defendant provide the membership information stored on their servers. *Id* at 1300. Defendant held the membership data for ransom and the resulting delay caused the gym's deal with LA Fitness to collapse. *Id.* The Court found that the suit between the gym and Defendant did not allege "errors, omissions or negligence," but instead "knowledge, willfulness, and malice." *Id*. at 1302. As a result, Travelers had no duty to defend. *Id.*

In *P.F. Chang's China Bistro, Inc. v. Federal Insurance Company*, 2016 WL 3055111 (D. Arizona, May 31, 2016), the Court found that a Fraud Recovery Assessment charged to Chang's by MasterCard to compensate it for the fraudulent charges that were related to a security compromise were not covered. Pursuant to the Master Services Agreement, the card processor "may pass through to [Chang's] any fees assessed …by the Card Organizations, including but not limited to, new fees, fines, penalties and assessment[s]." Id. at *7. In coming to its conclusion, the Court found the exclusions which provided that the insurer shall not be liable for any liability assumed by the insured under any contract or agreement barred coverage. *Id*. Although Federal did reimburse Chang's $1.7 million for valid claims, they did not have to reimburse them for the assessment by the card issuers.

Data Breach Litigation

The main issue in data breach litigation is whether the Court determines if the plaintiffs have standing to bring their case. For the most part, Courts have found that Plaintiffs have not alleged sufficient harm to merit standing. There are a few exceptions, including the *Target* case which found that the "unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees" were sufficient damages to survive a Motion to Dismiss. *In re Target Corp. Data Sec. Breach Litigation*, 66 F.Supp.3d 1154, 1159 (D. Minn. 2014).

In a departure from a majority of Courts, the 7th Circuit has recently found that "certainly impending" future injuries satisfied the Article III's injury in fact, causation, and redressability requirements. *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015). In *Neiman Marcus*, the Court found that the "Neiman Marcus customers should not have to wait until hackers commit identity theft or creditcard fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur. *Id.* at 693. (citing *Clapper v. Amnesty Intern. USA*, 133 S.Ct. 1138, 1147 (2013)).

More recently, in a similar data breach case, the 7th Circuit reaffirmed its holding in *Neiman Marcus*, finding that plaintiff's alleged injuries, such as increased risk of fraudulent charges and identity theft, was sufficient to satisfy the standing requirements for Article III standing. *See Lewert v. P.F. Chang's Bistro, Inc.*, 819 F.3d 963, 966 (7th Cir. 2016). This holding has since been followed by *In re Anthem, Inc. Data Breach Litigation*, 2016 WL 3029783, *26 (N.D. Cal. May 27, 2016) which held that "[p]laintiff attempts to respond to this imminent threat – whether by paying out of pocket for credit monitoring or by using their own time for credit monitoring – resulted in damages that

may be recoverable. *See also In re Premea Blue Cross Customer Data Security Breach Litigation*, 2016 WL 4107717 (D. Or. August 1, 2016). However, there are some courts that have rejected the 7th Circuit's reasoning in *Neiman Marcus*, which may be resolved by the Supreme Court. *See Duqum v. Scottrade, Inc*., 2016 WL 3683001 (E.D. Mo, July 12, 2016); *see also Attitas, et al., v. CareFirst, Inc., et al.*, 2016 WL 46250232 (D.D.C., August 10, 2016).