2019 CLM New York Conference
December 5, 2019
New York, NY

What Coverage Concerns Keep Cyber Insurers Awake at Night?

I. Cyber Exposure Today

There is certainty in knowing that cyber exposure is ever changing. What was a concern ten years ago is ancient in terms of cyber insurance. Ten years from now, the current cyber issues will likely be obsolete as well. It is plain that the number of cyber claims has steadily increased in the past couple of years. These claims, both big and small, have impacted entities in various sizes and industries. The exposures are not only for technical response needed to the cyber event itself, but also the legal and regulatory defense costs, settlements, and fines. Not to mention the business interruption costs and the hit to public credibility. In the NetDiligence 2018 Cyber Claims Study, the average records exposed in a breach was 1.2 million, with a per-record cost of $308.00. The top four causes of such losses were hackers, ransomware, malware/virus, and lost/stolen laptop/devise. These exposures have been across all sectors, making cyber exposure a concern not only limited to large corporations, but also small organizations as well.

II. Evolution of Cyber Insurance

The cyber insurance product has evolved as the risk has become more prevalent since organizations began using the Internet more frequently starting in the 1990s. Initially, it was sold as an add-on to certain professional liability and errors and omissions policies. Now, it is usually a stand-alone product. As the market for cyber insurance has expanded, insurers have been shying away from providing cyber coverage under other policy types. Insurers have been recently addressing "silent cyber," or cyber-related coverage on policies that were not specifically designed to cover cyber risk. As such on a number of general liability policies, there is now exclusionary language that bars cyber liability coverage altogether. To this point, the Lloyd's marketplace on July 4, 2019 mandated that by January 1, 2020, Lloyd's underwriters are required to clarify whether first-party property policies affirm or exclude cyber coverage. Given the increase of exposure to cyber risk and the evolving risk itself, insurers will need to continue to modify the applicable language in their policies.

III. Key Areas of Potential Cyber Exposure

Breach Notification Laws

The importance of notifying individuals of a security breach involving personally identifiable information has been codified by each state. In general, the breach notification laws have provisions as to (1) what is personal information, (2) who must comply with the law, (3) what constitutes a breach, and (4) the requirements for the notice. The timing and method of notice is very concerning for entities in terms of compliance with the state law. While most states require entities to provide notice of the breach in the most expedient time possible, some notification deadlines are explicit in providing notice by a date certain. Other unique features of certain state notification laws include (a) regulator notification requirements, (b) sector-specific notification requirements, and (c) credit monitoring requirements. Thus, it is important for insurers and the professionals they retain in response to a breach to understand what is needed to prepare for and respond to data breaches.

Cyber Regulations

Government regulation of cyber risks continues to grow in prevalence and cyber policies have slowly been changing to keep up with the risk. The one regulation that has received a lot of attention of late is the European Union's General Data Protection Regulation ("GDPR"). The GDPR, which went into effect on May 25, 2018, is designed to protect the personal identifiable information of the estimated 508 million people in the European Union. The GDPR also provides EU citizens the "right to be forgotten" in terms of their Internet history. It does not matter where the insured is located for the GDPR to be applicable, but whether they have information from EU residents. The GDPR does not mandate any specific security measures for companies maintaining information, but rather to take "reasonable steps." Going forward, there are other regulations that may impact an insured similar to the GDPR such as the California Consumer Privacy Act ("CCPA"), Japan's Act on the Protection of Personal Information, Brazil's Data Protection Law, and Canada's Personal Information Protection and Electronic Documents Act. As these regulations are enacted around the world, it remains to be seen whether there is any teeth to the regulations. As an example, the government agencies under the GDPR can levy heavy fines, such as the greater of €20 million or 4% of the global revenue per infraction. However, to date the fines actually imposed have been relatively minimal. On January 21, 2019, France's regulatory agency, National Data Protection Commission ("CNIL") imposed a €50 Million penalty against Google under the GDPR. The fine was based upon Google not providing enough information to users about its data consent policies. There have been other fines assessed under the GDPR against a Portuguese hospital, German social media and chat service, and local Austrian business, but such were nominal.

Recently, the Federal Trade Commission ("FTC") is getting more involved in the regulation of companies in the United States as it relates to cyber and consumer protection. While Section 5a of the Federal Trade Commission Act does not specifically address data breach or a consumer's right to privacy, it instead generally prohibits "unfair or deceptive acts or practices." On July 22, 2019, it ordered Equifax to pay up to $700 million in compensation and penalties because 147 million Americans credit data was compromised. Then on July 24th, the FTC hit Facebook with a $5 billion fine in a settlement over the company's privacy policies. This investigation began

following the March 2018 reports that Cambridge Analytica had improperly accessed the data of 87 million Facebook users. The FTC's $5 billion fine was based upon Facebook's failure to protect consumer privacy based on the FTC Act. The SEC at the same time, announced a settlement with Facebook of $100 million in connection with misleading disclosures about the risk of misapplication of user data. As such, the increased government regulations of corporation and their control of data can lead to greater potential for fines and penalties to be levied.

Thus whether it is GDPR, CCPA, or any other regulation, compliance with these regulations can impact the coverage available under the cyber policies.

Data Breaches

The cyber cases that make the big headlines are those involving a data breach. Such examples include a data breach of 3 billion accounts for Yahoo, the personal information of 147 million people exposed at Equifax, and recently over 100 million customer accounts at Capital One. However, not all data breaches are the same. Not only can the size of the breach vary, but also the potential scope of liability based on the Insured's actions.

Most data breaches are not making the headlines because the majority of breaches are not large in scale. In the last 5 years according to NetDiligence, the median amount of records exposed in a data breach was 1,000. However, even if a breach does make the news, that may not be the full picture. In connection with the breach at Target in 2013 involving 70 million customer credit card information, Target settled the main class action complaint for $18.5 million in May 2017. However, the settlement was only a small fraction of the overall impact. It was reported that Target spent more than $200 million in connection with multiple litigations, including one against the directors and officers, notification and credit monitoring costs, and the implementation of a comprehensive security program.

As underwriters consider issuing cyber policies providing the retention of defense counsel to respond to a third-party complaint against a company stemming from a data breach, it is important to understand not only the steps taken to prevent a data breach, but the steps taken in response to the breach.

In the case against the directors and officers ("D&Os") of Target, a special litigation committee spent nearly two years investigating whether the D&Os: (1) failed to properly provide for and oversee an information security program and (2) failed to give customers prompt and accurate information in disclosing the breach. The investigation found and the case was then not pursued because that the directors and officers took a lot of steps in attempting to prevent the security breach. The special litigation committee concluded that it was not in the best interest of the shareholders to pursue the case because, in part, Target had a long trail of consistent efforts to address cyber concerns, through unsuccessful, but greater than most companies were doing at the time. This is seemingly contrasted with the FTC's actions against Wyndham hotels in connection with a theft of 500,000 customers' personal information in 2013 where the FTC alleged that Wyndham failed to provide "reasonable and appropriate security" measures. The court did not find that Wyndham's practices constituted unfair security measures, but rather remanded the case to the district court for a trial on the merits. This case was later settled.

As the value of big data and critical information assets are increasing daily, the instances of data breaches will remain in the headlines.

VI. Practical Takeaways in Assessing Cyber Exposure

As such, it is important to understand what are the cyber exposures for an insured and what maybe sought in terms of coverage if they are the subject of a cyber event. This not only involves consideration of the industry of the insured, but what type of data they are maintaining. The statistics reveal that most data breaches involve the healthcare industry, followed by education, government, and retail. Most of the data breaches involved personally identifiable information, such as name, phone number, address, and social security numbers. Thus, it is important to know if the insured collects and/or stores personally identifiable information, as well as if the insured is subject to certain state or Federal laws on safeguarding such information.

When you are looking at the risk of your insured, one should also consider where the information is being maintained. This includes not only an understanding of the security for an insured's computer system, mobile devices, and servers, but also if third-party vendors are maintaining data. The Insured may have great internal protocols, but a third-party may lead to the breach of the data. It is significant to know what security measures are being taken by the insured and its third-party vendors. This includes anti-virus programs, intrusion detection, and penetration testing. There also should be a review of the insured's backup and archiving process for its own information.

Further, people are often the weakest link and many data breaches are caused by an insured's personnel opening a link or an attachment for an untrustworthy source leading to unauthorized access. All the security systems in the world cannot replace having good training of an insured's staff so that they understand how their actions can lead to a data breach. An insured's use of encryption and multi-factor identification can help safeguard data. Insurers and their brokers should also be aware if an insured has an incident response plan because without one, the effects of a cyber exposure can be exacerbated.

As more of today's commerce involves some aspect of the Internet, the insurance industry needs to be aware of the prevalence of cyber exposures. While cyber insurance can help address some of the cyber exposures present today, preparation and education for those risks will always be vital.