CLM Claims & Litigation Management Alliance™
ADVANCING ETHICS, COOPERATION AND EDUCATION

CLM 2015 Cyber Liability Summit
October 21, 2015 in New York City

The Future of Cyber Liability Risks and Exposures

I. Basis for Cyber Attacks

Cyber-attacks come in many different forms and for many different reasons. The motivation for attacks may be financially driven, in pursuit of trade secrets, terrorist in nature or even based in war. Due to the lack of information surrounding a cyber-attack it is difficult, if not impossible, to determine the true motivations of the attacker. However, as technology continues to evolve, and attackers become more brazen, the ability to determine the basis for the attack may become clearer. As a result, insureds may find that claims once covered are now excluded.

Financially Driven

One of the most common motivations behind a cyber-attack is the theft of consumer personal identification information. Armed with PII, a hacker can open lines of credit in individuals' names or sell the information to third-parties. Businesses are vulnerable to similar attacks. There is a robust market for stolen PII and the threat of these types of cyber-attacks is an everyday reality.

Notable financially driven data breaches that have resulted in large-scale damage to both individuals whose information were compromised and the reputation of the businesses that were hacked include Target and Home Depot. Target's 2013 data breach resulted in up to 40 million customers' credit card data stolen and up to 70 million customers' PII stolen. Target's exposure was significant. Home Depot's 2014 data breach resulted in over 56 million customers' debit and credit card data being exposed. Although corresponding lawsuits have not yet settled, the liability Home Depot faces is also significant as experts' estimate $3 billion in fraudulent charges as a result of the data breach.

Businesses who are the victim of a cyber-attack may mitigate their risk through cyber insurance policies. But these cyber policies have limitations, namely that the business which was attacked had followed and kept up with industry best practices regarding data protection. These best practices are not clearly outlined, and they are constantly changing. As a result, it is the imperative that businesses regularly update their privacy policies and incident response plans.

5639240v.1

Trade Secrets and Gaining Access to Corporate Information

In some instances, cyber-attacks are motivated by the hackers desire to steal trade secrets or expose corporate information. Consequently, businesses must take steps to safeguard their intellectual property from theft.

A well publicized data breach involving corporate information involved the publication of Sony's corporate emails to the public. The believed culprit behind this attack is North Korea. The believed rationale behind the attack is that North Korea's leader was upset that Sony was releasing the 2014 film, *The Interview*, in which North Korea's leader and its' way of life were the subjects of ridicule. To retaliate for the production of the film, North Korea hacked into Sony's network, obtained and then released private corporate emails to embarrass Sony's executives. The damage to Sony's reputation is difficult to estimate, but the consequences of the hack were very real, as Sony did not release the film as originally intended.

It is believed that China is notorious for hacking businesses with the intention of stealing their trade secrets. *The New York Times* published an article titled Hackers in China Attacked The Times for Last 4 Months to steal passwords of reporters and other employees. These believed Chinese attacks coincided with a Times investigation that found the relatives of China's prime minister had accumulated a fortune worth several billion dollars through business dealings.

Terrorism

Another increasingly common motivation driving cyber-attacks is terrorism. Terrorism is difficult to define when it comes to cyber-attacks because language in cyber insurance policies is vague regarding what constitutes a cyber terror attack. Sometimes, the policies are interpreted in such a way that to provide coverage, the carrier requires that the attacker be a recognized group which has been classified as a terrorist organization by the government.

Recently, the United States' Central Command of the Armed Forces was the victim of a cyber terrorist attack perpetrated by the Cyber Caliphate – the group proclaims itself as being part of ISIS. In this attack, the Cyber Caliphate gained took over control of the Twitter account and changed its' profile picture to a symbol of the terrorist organization.

War

Cyber-attacks which occur during a time of war or are acts of war themselves are, like cyber terror attacks, difficult to define and label. Examples of cyber warfare are not uncommon: up until 2010, Israel utilized the Stuxnet virus to infiltrate Iran's nuclear program; and on multiple occasions, China has been accused to gaining access to either spy on or disrupt the United States' space shuttle design and nuclear programs. In the absence of a clear declaration of war, it is difficult to determine when a cyber attack constitutes an act of war.

The ability of an insurer to preclude coverage during and after these occurrences is based upon the war exclusion found in many cyber policies. The war exclusion comprises

5639240v.1

language that effectively states, an act-of-war or warlike activity is grounds for denying coverage. In the past, general liability policies contained war exclusions that required that the act-of-war be done by state powers engaging in military acts. But today, cyber insurance policies' war exclusions aim to exclude acts that may have come from either state powers or state-affiliated groups whose intention is to attack a society by harming businesses in that society. Accordingly, there are still many unanswered questions regarding what the threshold is in connection with the type of and origin of cyber attacks which may be excluded under the war exclusion.

II. Language in Insurance Policies Regarding the War Exclusion

Cyber Policies' *War Exclusion* Provision Includes "Act-of-War" and "Warlike Activity"

The public policy behind expanding the war exclusion in cyber insurance policies to exclude incidents arising out of situations which may not have been deemed warlike activity in historic general liability (or other) policies is fairly straightforward. In our ever-increasing technologically centered global marketplace, there are more and greater threats that are directed at businesses from foreign, and maybe even domestic, enemies. Carriers cannot possibly be liable for the wide spread severity associated with state sponsored cyber attacks.

Naturally, there is a significant amount of uncertainty regarding what does and what does not constitute an attack excluded under the war exclusion. And it is unlikely that a bright line rule will be drawn anytime soon. This is especially true considering the ever-evolving nature of these attacks, let alone the difficulty in determining the origins of attacks. However, it is important to know that the war exclusion is regularly included in a cyber policy and may exclude coverage for claims believed to be covered.

Coverage for Terrorism is Another Polemic

Providing coverage when a potential cyber terror attack occurs has similar uncertainties as the war exclusion. First and foremost, even if the origin of the attack is known, one must examine whether the attacker is a terrorist. Sometimes, cyber policies require that the attacker be formally recognized and deemed a terrorist organization by the government. The nature and effect of the attack may define whether a cyber terror attack occurred, rather than simply the classification of the attacker itself.

The threshold for whether a cyber attack may be deemed a terrorist attack is unclear. It is in the interest of the business community, and especially the risk management community, to have some consistency with respect to this issue so that parties can appreciate their risk ahead before an attack. Numerous questions in connection with these types of attacks have not been answered, and new questions are constantly popping up as technology raises new issues. These issues may ultimately be flushed out, but in the interim, a case-by-case analysis will be necessary in evaluating coverage for these claims.

5639240v.1

III. The increased reliance on the computer network to run everything ("the more complex a system the more likely it is to fail")

a. The Decoupling of Computer Power: the growth of software as a service (SAAS)

The vast majority of essential business tools, computers, smart phones, processing, tracking, sales, servicing require connectivity to another machine or set of machines in order to be operational. Connection to internal company servers, cloud based storage/servers are essential for most modern business operations. The lack of availability of these systems has the potential to lead to significant business income loss. This creates the potentially fraught liability dynamic between service providers and companies when there is a service providers issue resulting in an interruption of operations at the company. This dynamic becomes even more complex if the issue at the service provider results in a data loss or the companies. Currently there is no clear cut way to address these issues but, contractual requirements and risk transfer via insurance are becoming increasingly popular. A patch work for privacy regulations in the US leads to further confusion.

This issue will only increase as forecast stagnant growth in the developed world leads to pressure to increase productivity and to cut costs. Companies will increasingly outsource operations and data storage to parties that can better scale the services and deliver at a lower price point. Increasingly sophisticated hackers, combined with more stringent privacy regulations will lead to the outsourcing of data security as keeping those operations internal become increasingly cost prohibitive. Companies will also look to risk transfer via insurance as network security becomes increasingly recognized as a risk that cannot be avoided.

b. The Networked Computer in Anything and Everything

The potential exists for a new wave of liability suits to come forward as parties are increasingly damaged by the failure of network security inside everyday devises. Chrysler/Jeep is currently undergoing a costly recall when it was demonstrated that critical systems inside of one of their vehicles could be hacked and controlled remotely by an attacker. The potential exists for catastrophic liability to arise from seemingly insignificant devices/systems inside cars, homes, offices. The potential exists for financial, property damages and even bodily injury loss. The rise of autonomous and semi-autonomous machines has implications, for all industries but more specifically the automotive and logistics industries.

c. Liability

We will bring it all together and summarize the overall risks that we see increasing as they continue to evolve. It is not clear where liability will begin and end given the increased reliance on outside vendors for a company's computer network to function.

We anticipate that the liability will become so nebulous in this space that companies will increasingly rely on risk transfer to compensate for potential losses and to avoid as much as possible costly litigation between companies and service providers.

5639240v.1

d. Availability

Network computers will increasingly become required to complete even simple business tasks. Companies will have to handle this potential exposure from an IT, legal, and risk management perspective.

Risk financing issues will become increasingly important as it is recognized as not an if, but when type of scenario. This is a system of the inevitability of an increasingly complex system interacting with one another.

The profitability of underwriting these risks may come into question. There is skepticism as to whether the insurance community will be able to profitable create risk transfer vehicles for these risks if they become as ubiquitous as anticipated. Insurance carriers will begin to "look under the hood" of companies IT in greater depth. As with property insurance, the requirements of insurers in order to maintain coverage may drive how companies operate and manage their IT systems. If the risk does become ubiquitous, the large influx of premium and the law of large numbers may sufficiently offset the risk.

e. Security failures: Attacking us at our most vulnerable

"So in war, the way is to avoid what is strong, and strike at what is weak."
— Sun Tzu, *The Art of War*

"The supreme art of war is to subdue the enemy without fighting."
— Sun Tzu, *The Art of War*

Network attacks will continue to increase in number as our economic reliance on networked computers increases. Throughout history enemies have sought to harm each other at the heart of their economy. As our global economy increases reliance on networked computers to operate the basic functions of our society, these types of attacks will increase. In the nuclear world, being able to harm your enemy without firing a shot is a tempting proposition for enemies looking to harm each other without starting a highly destructive kinetic war.

As we continue to speed our way through the technological revolution, the issues that businesses are facing are evolving in an effort to maximize profit and reduce costs. The path to optimal profitability is riddled with hazards that will attempt to exploit vulnerabilities. Nefarious entities are looking to take advantage of weaknesses to undermine business reputation, decrease your revenue and create ways to increase their profitability. Integrated systems that seek to advance profits present security risks that must be properly maintained. But it is virtually impossible to build a wall that will keep all invaders out. When security failures occur, the mitigation of damages is essential.

5639240v.1