2019 Cyber, Management and Professional Liability Conference
July 10-12, 2019
Boston, MA

**Title: "Cyber Insurance Coverage – Where we are and where we may be going!"**

## I. Current Corporate Cyber Risk Concerns and How Cyber Insurance Mitigates Risk

### Understanding the Role of Cyber Insurance

It is important to understand the purpose of cyber insurance. Unlike other risk mitigation tools, such as firewalls, it is not a technology security solution. Instead, it is a risk transfer option available to insureds after they have already implemented safeguards to protect against exposures. As the last line of defense, it does not seek to prevent a wrongful act; rather, it seeks to minimize the insured's exposure to an incident.

### Understanding how Cyber Insurance is Unique

Unlike most other risks mitigated by insurance coverage, cyber insurance provides benefits beyond mere accidents. Many cyber coverages available protect against attackers who are performing intentional acts against the insured with the intent to cause harm. These attackers may be: (1) nation-state sponsored; (2) hacktivists; (3) organized crime; (4) terrorists; or (5) insiders. Cyber insurance coverage is intended, in part, to help insureds manage their exposure to these attackers and many other types of risks.

## II. Cyber Risks and Insurance Coverages Currently Available In Cyber Insurance Policies

### Not all Cyber Policies are the Same

Cyber insurance is relatively new to the insurance industry. Unlike other insurance coverages, such as Commercial General Liability Policies, cyber insurance has not been afforded an opportunity to fully mature. Consequently, there is no uniform cyber insurance policy in the industry.

When insureds investigate their cyber insurance policy options, they will discover that many cyber insurance policies cover different risks, provide different limits or sub-limits, and contain different endorsements restricting coverage. Further complicating cyber insurance coverage is the lack of case law interpreting the meaning of those insurance clauses. So before

an insured procures cyber insurance coverage, it is imperative that they understand their risk and how the cyber insurance policy being selected best mitigates their exposures.

**Ransomware**

Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. If the malware is more advanced, it will encrypt the insured's files, making them inaccessible, and demand a ransom to be paid, typically in the form of Bitcoins, for a key to be provided to de-crypt the files.

Ransomware is readily available to attackers on the Dark Web, which has resulted in a significant increase in its use.

Some of the consequences of a ransomware attack include: business interruption/dependent business interruption, monetary payments to the attacker and costs incurred as a result of retaining legal counsel and forensic investigators to assist with the ransomware attack. Of particular concern is the business interruption component, which can cause a major disruption to the insured's business, with serious financial and reputational consequences.

For example, Maersk, a victim of the NotPetya attack, commented that the cyber extortion attack against it cost the company more than $300 million. Shockingly, the cyber extortion attack only took Maersk offline for about 10 days. Had Maersk not been so fortunate, its' business interruption loss could have been significantly higher.

In addition, cyber extortion exposures may include the costs of paying for the key to de-crypt the locked files. If the insured is in dire need of the locked information, it may negotiate with the attacker, and pay a ransom. Certain industries, such as medical/hospitals, are more susceptible to a ransomware attack because of their need to have immediate access to their files. Other costs may include legal counsel, forensic investigations and public relations to assist with the ransom attack, preventing further damage and harm to the insured's reputation.

Many cyber insurance policies provide coverage for ransomware attacks and the resulting costs related to those attacks.

**Breach Response**

Most businesses possess data that is considered personally identifiable information. This may be employee or customer social security numbers, credit card numbers, date of birth, passport numbers or other sensitive data. Healthcare providers typically possess information considered to be protected health information, such as Medicaid/Medicare numbers, health diagnosis or other personal health information.

A data breach incident is the potential unauthorized accessing of sensitive data by a third party. Pursuant to state breach notification laws and foreign laws, a business may have an affirmative obligation to disclose the data breach to the individuals who have been a victim of the unauthorized access to their personal information. If an attacker gains unauthorized access to an individual's personal information, the business typically will need to incur costs, including legal counsel to provide guidance as to their legal obligations concerning the data breach, forensic investigators to determine what information may have been improperly accessed, identity protection solutions, such as credit monitoring, public relations, and more, depending on the situation.

Notably, the insured may still be responsible for providing breach response services even if it is not the source of the exfiltration of the personal information. Many businesses have third party partners who assist them with providing services to customers. Consequently, these third-parties may have access to the information, maintain lesser security standards, and be the source of the data breach. Even if the third-parties are the cause of the data breach, it is still the responsibility of the business originally entrusted with the personal information to ensure its protection. For instance, if an insured is storing its' personal data in the cloud, and that cloud provider suffers a data breach exposing the insured's personal information, it is likely the insured's obligation to provide data breach services.

Cyber insurance policies usually cover these types of costs.

**Cyber Crime**

Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network. Cybercrime is typically defined as "offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet and mobile phones.[1]"

In the context of risks covered under a cyber insurance policy, cybercrime usually refers to fraudulent instructions provided by a third-party attacker that results in financial harm to the insured. For example, a third-party attacker may gain access to the insured's network through a phishing campaign, or alternative means. The attacker then conducts basic due diligence of the insured, identifies key management, educates him/herself about ongoing transactions, and then changes the insured's email rules. Instead of having emails sent to the insured's employee, the

[1] Halder, D., & Jaishankar, K. (2011) Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

attacker re-routes the email so that he/she is the sole recipient. The attacker, aware of ongoing business transactions, may then provide one of the insured's employees or customers with new instructions – instead of transferring funds to a prior bank account, the attacker instructions the payor to transfer funds should to a different bank account. As the email received by the employee or client is either from the proper individual's email account or has the appearance of being from the proper individual's email account, the funds are transferred. Only later does the insured realize that the transfer was fraudulent. Efforts to claw back the funds are usually unsuccessful.

Certain cyber insurance policies provide coverage for this type of risk by reimbursing for the fraudulent payment. However, those cyber insurance policies may provide sub-limits on exposure, meaning that the insured may have less coverage for the loss because the limits of insurance on the cybercrime crime risk is lower than the policy limits for other claims.

**Regulatory Investigations/Fine & Penalties**

In an effort to protect consumer personal information, states and countries have enacted legislation to establish standards for the collection, use and dissemination of data. These privacy laws and regulations require insureds to apply certain information governance criteria to their management of data and, if the insured fails to comply, may result in an investigation as well as fines and penalties. Government regulation of businesses continues as new laws and regulations continue to be passed. More recently, the European Union passed the General Data Protection Regulation (GDPR) which may result in the levying of significant fines, including up to €20 million or 4% of the company's global annual turnover of the previous financial year, whichever is higher.

While there is an ongoing debate regarding the insurability of such fines and penalties, certain insurance policies provide coverage for such claims. Notably, there is a significant case making its way through the United Kingdom courts involving Morrisons, the major United Kingdom supermarket chain. In the Court's Judgment it commented on the levels of compensation payable for breaches under GDPR and how companies may deal with them.

The Court of Appeal wrote that the solution to the potentially ruinous levels of liability created by their judgment is to insure against it.

> There have been many instances reported in the media in recent years of data breaches on a massive scale caused by either corporate system failures or negligence by individuals acting in the course of their employment. These might, depending on the facts, lead to a large number of claims against the relevant company for potentially ruinous amounts. The solution is to insure against such catastrophes; and employers can likewise insure against losses caused by dishonest or malicious employees. We have not been told what the insurance position is in the present case, and of course it cannot affect the result. The fact of a defendant being insured is not a reason for imposing liability, but the availability of insurance is a valid answer to the

Doomsday or Armageddon arguments put forward by Ms. Proops on behalf of Morrisons.

**Third Party Claims**

In addition, cyber insurance policies generally provide coverage for third party claims against insureds relating to technology, media and privacy exposures. These matters may range from multi-million claims arising from significant data breach notification incidents, such as Target and Home Depot, to claims for the disclosure of a single patient's healthcare information.

Other types of third party cyber claims that may be covered under a cyber insurance policy include technology or media based incidents. These claims could be based on allegations of defamation, libel, misappropriation or other types of wrongful acts. Although these matters do not receive the same attention as privacy notification litigation, they can result in significant exposures.

## III. Future Corporate Risks and Growth of Coverage

**Bodily Injury/Property Damage**

Traditionally, cyber insurance policies have not encroached upon coverage for bodily injury and property damage. However, with the proliferation of the Internet of Things, cyber coverage may expand. The insurance industry will have a dilemma – do autonomous cars that cause bodily injury or property damage due to a security breach receive coverage under automobile policies, cyber policies or both. Similarly, if attackers breach firewalls of inter-connected monitors that cause a property damage, will a products policy respond for inadequate security or will a cyber insurance policy respond.

**Concerns about Expansion of Consumer based Protections**

GDPR may be just the tip of the iceberg with respect to expanding consumer rights. Although GDPR's extra-territorial reach into the United States results in its' application to many U.S. businesses, California's enactment of the California Consumer Privacy Act (CCPA), which becomes effective January 1, 2020, is likely to have a more significant impact on U.S. businesses. In particular, unique to the CCPA is the statutory damages provision providing damages of $100 to $750 per consumer per incident on certain data breaches. As a result, courts that previously dismissed class actions lawsuits for lack of standing because the claimants could not demonstrate injury in fact, may now have sufficient standing to survive a motion to dismiss and engage in discovery. Therefore, the stage may be set for an exponential growth of class action litigation in the privacy space.

Most cyber insurance policies, as currently drafted, would likely cover a third party action commenced under the CCPA. However, if litigation costs and damages are predicted to be significant, insurers could add an endorsement excluding such coverage from cyber policies, much like Telephone Consumer Protection Act (TCPA) claims were excluded from coverage.