Aon Risk Solutions
Financial Services Group

State of the Market

Cyber and privacy liability

July 2018

Empower Results®

Market Overview

Public companies & private organizations

	Primary	Excess	Factors that may impact pricing
1. Market capacity	Ample	Ample	
2. Insurance rate	Flat on renewal • Rate increases may result where there has been a drastic increase in revenue or a history of cyber incidents • Clients operating outside of perceived high-risk sectors may see some decrease on renewal when the account is marketed and all other factors remain equal	Flat on renewal • Rate increases may result where there has been a drastic increase in revenue or a history of cyber incidents • Clients operating outside of perceived high-risk sectors may see some decrease on renewal when the account is marketed and all other factors remain equal	• Public companies generally command higher premiums vs. private companies due to: (1) the large reputational cost of a cyber incident; and (2) increased litigation risk • Factors that may contribute to cyber insurance pricing: – The number and type of records held by an organization – The scale of the business – The extent to which records are outsourced to third party service providers – Whether a company has an incident response plan, a business continuity plan and uses encryption • Companies operating in perceived high-risk sectors, such as retailers, universities, financial institutions, health care providers, municipalities and ancillary services, will generally command a higher rate • Organizations that process electronic payment card transactions are viewed as high-risk, and those with a large payment card exposure may experience difficulty procuring cyber insurance – Insurers are more often requiring these insureds to be compliant with Payment Card Industry Data Security Standards (PCI-DSS)
3. Retention	Flat on renewal	Flat on renewal	

Coverage

Cyber extortion

The vast majority of cyber insurance policies contain a cyber extortion insuring agreement, providing coverage for the extortion amount itself and associated mitigation costs, such as payments for computer experts and forensic teams. While in the past coverage was only triggered by a demand for money in the traditional sense, most markets now include bitcoin and other cryptocurrencies within the triggers of cyber extortion coverage. Aon is also working to expand the coverage trigger to ransomless extortions, where a demand requires the victim to take, or not take, a particular action.

Business interruption – contingent

Many domestic carriers have expanded the scope of their contingent business interruption coverage. Often available as an endorsement, this coverage triggers when an insured company's vendor or service provider experiences a cyber incident that suspends the insured's business operation. Formerly limited to IT vendors, this endorsement has now been extended to any type of vendor or service provider. This "any vendor/service provider" coverage is often sub-limited.

Business interruption – reputational harm

Some domestic and London insurers are now offering business interruption coverage to protect against reputational harm, providing indemnity for revenue losses associated with lost customers due to a cyber incident.

Business interruption – system failure

A few domestic and London carriers have started offering expanded system failure coverage on a blanket basis, applying to any business interruption that occurs pursuant to a system failure that occurs for "non-malicious" reasons -the trigger is no longer limited to a third-party hacking incident. Subject to the particular policy wording, this expanded coverage could trigger in a multitude of situations, such as a system failure resulting from an operational or administrative error. This "non-malicious" system failure trigger also extends to contingent business interruption insurance.

Social engineering fraud

Social engineering fraud coverage is now being provided by some domestic and London insurers on cyber insurance policies. This cyber form coverage is typically subject to a call-back requirement, and may not be as broad as the social engineering coverage provided by commercial crime insurance. When purchasing this coverage on a cyber liability policy, companies should ensure that any commercial crime insurance providing similar coverage is coordinated such that the two policies work together.

Business interruption – property damage

Aon is working with the markets to create coverage under cyber policies for business interruption stemming from property damage and associated loss of use arising directly from a cyber breach. For example, if a manufacturing company's systems were hacked by a malicious third party, causing one of their assembly line belts to become damaged and/or cease operations, coverage for the resulting business interruption might previously have been precluded by the Bodily Injury/Property Damage (BIPD) exclusion. However, with insurers now willing to soften the BIPD exclusion on a case by case basis, the policy may, in some instances, respond to cover business interruption where it results from a cyber breach causing property damage and associated loss of use to machinery, equipment or other systems. Although insureds across the board will gain from this broadened coverage, it is anticipated that companies in the manufacturing, oil and gas, transportation, mining and utilities industries will benefit to the greatest extent. In this vein, select London carriers are starting to provide coverage not only for business interruption resulting from property damage caused by a cyber incident, but also for the property damage itself.

Pre-breach consulting services

In conjunction with cyber liability insurance, more carriers are providing an extended array of complimentary pre-breach consulting services, such as forensic, legal and public relations risk consultation services, employee training, domain protection and infrastructure vulnerability scans. As markets continue to emphasize these services, an increased number of clients are taking note and availing themselves of this coverage.

Canadian and EU Regulatory Update

Canada – Federal

- **Canada's mandatory data breach notification regime in force 1 November 2018:** Included as part of a series of amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA) in 2015, the Digital Privacy Act (Bill S-4) provisions require mandatory notification to the Office of the Privacy Commissioner and affected individuals in certain instances where a breach compromises personal identifiable information (PII). The mandatory breach reporting regime requires private companies subject to PIPEDA to report privacy breaches that the organization believes "create a real risk of significant harm to an individual." The breach must be reported "as soon as feasible" to both the Privacy Commissioner and the individual(s) whose PII was compromised. Knowingly failing to report privacy breaches in compliance with PIPEDA could result in an offence punishable by fines of up to CAD $100,000.
- **The Standing Committee on Access to Information, Privacy and Ethics releases its review of PIPEDA:** The Standing Committee recently released its report, which reviewed PIPEDA and made 19 recommendations to the Government of Canada. These recommendations included granting individuals the "right to be forgotten," improving transparency regarding artificial intelligence programs behind websites, and bestowing the Office of the Privacy Commissioner with the power to make orders, impose fines and elect which complaints to investigate. The extent to which the recommendations will be adopted is unknown at this point, but will be monitored closely.

International

- **European Union's General Data Protection Regulation (GDPR) in force 25 May 2018:** Intended to harmonize privacy laws across Europe, the regulation will apply to Canadian companies that process PII of EU residents. Fines and penalties for non-compliance can reach exorbitant amounts – up to the greater of €10 million or 2% of an organization's global annual turnover for contraventions related to technical measures, such as breach notifications or impact assessments; or €20 million or 4% of an organization's global annual turnover for non-compliance with key provisions of the GDPR, such as transfers of personal data outside the EU to countries or organizations that do not ensure an "adequate level of protection".

Canadian Litigation Update

- **Invasion of privacy tort argued in Equifax class action:** Initially coming to light on 7 September 2017, Equifax U.S. announced that an unauthorized intrusion into their computer systems due to a "cybersecurity incident" had occurred from mid-May 2017 through July 2017. The breach compromised various forms of personal identifiable information (PII); close to 20,000 Canadians were affected. As a result, Equifax is facing a Canadian class action lawsuit seeking CAD $550 million in damages, including $50 million in punitive damages. In January 2018 the Ontario Superior Court released its written decision on the carriage motion. In its ruling, the court allowed the lawsuit that based its claim upon the common law tort of intrusion upon seclusion to advance to the certification stage. The significance of this ruling is that this tort allows individuals whose personal privacy has been invaded to bring a lawsuit- even where no economic harm or loss was suffered. As the judge in the ruling noted, "Such a claim provides a significantly broader basis for the claim of the class members, as it is not necessary to prove harm." However, this class action will still need to meet the test for certification to move forward. Aon will continue to monitor this case moving forward.

U.S. Regulatory Update

- **State data breach notification laws:** The number of state data breach notification laws has continued to increase and receive amendments. As of the time of writing, all fifty states, plus the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, have data breach notification laws. All state breach notification laws require notification to affected individuals. Of the fifty state data breach notification laws, the laws of thirty-one states – plus Puerto Rico - require notification of the breach to a state attorney general or regulator in addition to the affected individuals.
- **State data security laws:** The number of state laws requiring organizations to develop, implement and maintain reasonable security practices and procedures to safeguard personal information also continued to increase. Eighteen states have laws addressing personal information security procedures.
- **Cybersecurity disclosure under federal securities laws:** In a related development, in February 2018 the U.S. Securities and Exchange Commission (SEC) issued an interpretive release regarding cybersecurity disclosure requirements under federal securities laws for public companies. This interpretive release expands upon the SEC's 2011 guidance on cybersecurity disclosure requirements in terms of addressing:
  (1) the importance of comprehensive company policies and procedures related to cybersecurity risks and incidents;
  (2) applicable insider trading prohibitions under the general antifraud provisions of the federal securities laws; and
  (3) the obligation to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents.

Organizations that are subject to these varying state laws are interested in distilling them into one standard covering all the states. One reason for this is to be able to compare such a U.S. standard with the laws of other countries, such as the GDPR in Europe and PIPEDA in Canada. The current structure of U.S. privacy legislation makes it difficult for organizations that are interested in incorporating the U.S., EU and Canadian data privacy requirements into their incident response plans.

U.S. Litigation Update

- **Yahoo settles data breach-related securities class action lawsuit in the U.S. for $80 million:** The litigation stemmed from two data breaches Yahoo experienced in 2016, which ultimately compromised PII (personal identifidable information) associated with over 1 billion user accounts. Following the two data breaches, Yahoo's share price declined 3.06% and 6.11% respectively.
- **The first data breach disclosure enforcement penalty in the U.S.:** The U.S. Securities and Exchange Commission has levied a $35 million penalty against Altaba, Inc. (successor in interest to Yahoo! Inc.) for Yahoo's two-year delay in reporting the massive cybersecurity breach that initially occurred in December 2014. The penalty settles charges that Yahoo misled investors by failing to disclose the breach, in which hackers stole PII pertaining to millions of user accounts.

About Aon Risk Solutions Canada

Aon Reed Stenhouse

For more than 160 years, in one form or another, Aon Reed Stenhouse has been a major force in the Canadian insurance industry.

Aon Reed Stenhouse, operating under the brand name Aon Risk Solutions, is Canada's leading insurance brokerage and risk management services firm. We serve an extensive client base, handling more than $2 billion in annual premiums on behalf of our clients.

- Insurance brokerage
- Risk management
- Employee health and benefits

Our 1,600 professionals serve clients from 23 offices located across Canada. We provide our clients with a wide range of innovative solutions. Each day, Aon professionals work to deliver the best solutions to our clients.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Empower Results®