# State of the Market

Cyber and privacy liability

*February 2019*

Empower Results®

# Market Overview

## Public companies and private organizations

| | Primary | Excess | Items and industries of note |
|---|---|---|---|
| **1. Market capacity** | Ample | Ample | |
| **2. Premium** | Flat on renewal<br>• Premium increases may result where there has been an increase in revenue or a history of cyber incidents<br>• Clients operating outside of perceived high-risk sectors may see some decrease in premium on renewal if the account is marketed and all other factors remain the same | Flat on renewal<br>• Premium increases may result where there has been an increase in revenue or a history of cyber incidents<br>• Clients operating outside of perceived high-risk sectors may see some decrease in premium on renewal if the account is marketed and all other factors remain the same | Factors that may impact pricing include:<br>• 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<br>• Factors that may contribute to cyber insurance pricing for both public and private organizations include:<br>– The number and type of records held by an organization<br>– The scale of the business<br>– Whether a company has an incident response plan, a business continuity plan and uses encryption<br>– The scope of cyber insurance coverage being sought and the retention level<br>– Quality of the underwriting information provided<br>• 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<br>• Complex technology risks purchasing a combined cyber and technology errors and omissions policy may be subject to more stringent underwriting and higher premiums |
| **3. Retention** | Flat on renewal | Flat on renewal | |

# Coverage

- **GDPR fines and penalties:** The advent of the European Union's General Data Protection Regulation (GDPR) has many organizations concerned about exorbitant fines and penalties and the possible increased exposure to regulatory investigations and proceedings. While the insurability of GDPR fines and penalties remains uncertain in Canada, some cyber policies now contain language that could allow them to be covered in jurisdictions where they are insurable. In addition, traditional policy triggers, that covered regulatory investigations and proceedings only where they arose out of a cyber breach, have been amended to cover regulatory investigations arising out of an alleged violation of the GDPR – even if the regulatory investigation or proceeding is not preceded by a cyber incident.

- **Reputational harm:** Some domestic and London insurers are now offering business interruption coverage to protect against reputational harm by providing indemnity for revenue losses associated with lost customers due to a cyber incident. The scope and trigger for this coverage differs by insurer and it remains to be seen what evidence must be presented by an insured to substantiate a claim.

- **Cyber extortion:** It is standard for cyber insurance policies to contain a cyber extortion insuring agreement, providing coverage for the extortion payment itself as well as associated mitigation costs, such as the cost to engage computer experts and forensic teams. In the past year we have seen insurers expand the trigger for this coverage to include extortions where the demand requires the victim to take (or refrain from) a particular action, rather than a demand for financial compensation.

- **Coverage for damaged hardware**: Historically, cyber insurance has not extended to cover the cost for an insured to replace, enhance or upgrade computer system hardware damaged by a cyber incident. However, some insurers will now endorse the cyber insurance policy to allow an insured to enhance or upgrade its computer system where certain conditions are met (i.e. where it is necessary to avoid a future security failure or the hardware can only reasonably be replaced with an upgraded component).

- **Business interruption – contingent:** It is now standard for domestic carriers to provide full limit contingent business interruption coverage where the key service provider is an IT vendor. This coverage triggers when an insured company's vendor or key service provider experiences a cyber incident that has the indirect effect of interrupting the insured's own business operations. Contingent business interruption coverage for non-IT vendors is also available by endorsement but this coverage is typically still subject to a sub-limit.

- **Business interruption – system failure:** Some domestic and London carriers have started offering expanded business interruption coverage where the loss results from a system failure that occurs as a result of "non-malicious" actions. While policy wording varies, this coverage could trigger in a multitude of business interruption situations, such as a system failure arising out of an operational or administrative error. This "non-malicious" system failure trigger also extends to dependent business interruption insurance, which responds to cover the insured's lost profits and additional expenses if business is interrupted at an insured's service provider. Insureds interested in purchasing this coverage will be required to complete a questionnaire and pay additional premium.

- **Social engineering fraud:** Social engineering fraud coverage is now being provided by certain domestic and London insurers under cyber insurance policies. While a cyber policy would not typically respond to cover direct financial loss arising out of a cyber breach, the social engineering fraud endorsement makes an exception where the financial loss results from an executive, vendor or client impersonation scam. The coverage is typically sub-limited and may not be as broad as the social engineering coverage provided under commercial crime insurance policies. On some cyber policies, the social engineering coverage is drafted such that it will not respond where there is duplicative coverage available on an insured's commercial crime insurance policy.

- **Business interruption – property damage:** Aon is working with the markets to create coverage under cyber policies for business interruption stemming from property damage caused by a cyber incident. Although insureds across the board will benefit from this broadened coverage, it is anticipated that companies in the manufacturing, oil and gas, transportation, mining and utilities industries will especially look to this coverage to address significant gaps in existing insurance policies. In addition, 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, under a cyber policy. We expect to see the available insurance for the "internet of things" risk exposure continue to evolve in the next few years.

- **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 these resources.

# Canadian and International 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.

## United States

- **California's new privacy law and U.S. federal privacy legislation:** The California Consumer Privacy Act (CCPA) is scheduled to come into force on 1 January 2020. The California Attorney General is to adopt regulations on or before 1 July 2020, and is not to bring an enforcement action until 6 months after the publication of the regulations or 1 July 2020. Whether and when the U.S. will adopt federal privacy legislation that preempts state law such as the CCPA remains to be seen and should be monitored. The CCPA will apply to any organization, regardless of where that organization is domiciled, that: (1) collects personal information (PI) of California residents, (2) does business in the State of California, (3) determines the purposes and means of the processing of such PI, and (4) either (a) has annual gross revenues in excess of US$25 million, (b) alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the PI of 50,000 or more California residents, households, or devices, or (c) derives 50 percent or more of its annual revenues from selling California residents' PI. Note that there are certain exceptions to the CCPA that must also be analyzed. The CCPA provides California residents with consumer data privacy rights and contains privacy policy and website requirements that will spur the updating of U.S. privacy policies and websites. Penalties, such as injunctions and specified monetary penalties, may be imposed for violations of the CCPA. The legislation also creates a private statutory right of action for the greater of (1) certain amounts per California resident per incident, or (2) actual damages against organizations for the unauthorized access and exfiltration, theft, or disclosure of the resident's nonencrypted or nonredacted PI resulting from an organization's failure to "implement and maintain reasonable security procedures and practices".

- **California's new Internet of Things law:** Coming into force on 1 January 2020, the new legislation requires any manufacturer of a device that is capable of connecting "directly or indirectly" to the internet and that is assigned an Internet Protocol address or Bluetooth address to equip it with "reasonable" security features designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure. Affected manufacturers will include the person that manufactures, or contracts with another person to manufacture on their behalf, such connected devices that are sold or offered for sale in California. The California Attorney General, a city attorney, a county counsel, or a district attorney will have the exclusive authority to enforce this legislation. Note that there are certain exceptions that also must be analyzed as to whether this legislation is applicable.

- **U.S. SEC enforces data breach disclosure and imposes penalty:** In April 2018, the U.S. Securities and Exchange Commission (SEC) announced the settlement of charges against Altaba, formerly known as Yahoo!, which accused the company of misleading investors in connection with the two-year delay in disclosing to the investing public one of the world's largest data breaches, in which hackers stole personal information relating to hundreds of millions of user accounts. Altaba paid a USD $35 million penalty, and neither admitted nor denied the findings in the SEC's order.

## 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" that had occurred from mid-May 2017 through July 2017. The breach compromised various forms of 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 allowed the lawsuit to advance to the certification stage on the basis of the common law tort of intrusion upon seclusion. This is significant because the tort allows individuals whose personal privacy has been invaded to bring a lawsuit, even where they cannot show economic harm or loss. As the judge noted in the ruling, "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.
- **Transmission of malware leads to CASL fine for two companies:** In July 2018, the Canadian Radio-television and Telecommunications Commission (CRTC) levied administrative monetary penalties (AMPs) under Canada's Anti-Spam Legislation (CASL) against two companies for aiding in the installation of malware via online advertising. Sunlight Media Network Inc. (Sunlight) and Datablocks, Inc. (Datablocks) provide networks to online third-party advertisers, allowing them to distribute their advertisements on various legitimate websites. The CRTC alleged that Sunlight accepted anonymous and unverified clients who used its services to distribute malware, and Datablocks provided the necessary software for Sunlight's clients to carry this out. After investigation, the CRTC found that both companies could have prevented the distribution of malware but omitted to implement the necessary safeguards to that effect, thus violating CASL. Datablocks faced a fine of $100,000, while a $150,000 fine was levied against Sunlife.

# U.S. Litigation Update

- **Marriott data breach affects 500 million and triggers multiple lawsuits:** On 8 September 2018, Marriott learned that its Starwood guest reservation database had been compromised since 2014 and that an unauthorized party had copied and encrypted the information of up to 500 million guests who had made a reservation at a Starwood property. For the majority of those affected, the guest information that was accessed includes some combination of name, mailing address, phone number, email address, passport number, Starwood account information, date of birth, gender and travel information. For some guests, the affected information also includes payment card numbers and expiration dates. Marriot announced the breach in a press release on 30 November 2018. That same day, consumer class action lawsuits were filed in Oregon and Maryland, with the plaintiffs in Oregon seeking $12.5 billion in damages. These were quickly followed by the filing of a securities class action lawsuit in the Eastern District of New York on December 1st. It is anticipated that additional lawsuits will be filed in the coming months.

- **Yahoo settles yet another data breach-related class action lawsuit in the U.S.:** Earlier this year, Yahoo agreed to pay $80M to settle securities class action litigation arising out of breaches of the company's data in 2016-2017. In October 2018, Yahoo reached a separate settlement with a class action group comprised of roughly 200 million individuals in the U.S. and Israel who were affected by the breach. As part of the settlement agreement, Yahoo has agreed to establish a USD $50 million compensation fund, pay USD $35 million in lawyers' fees and provide affected users in the U.S. with credit monitoring services for two years. The deal is subject to final approval by the Northern District of California court.

## About Aon in 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®