State of the Market

Cyber and privacy liability

Mid year 2019

Empower Results®

Market Overview

	Primary	Excess	Items and industries of note
Public companies and private organizations			
1. Capacity	**Ample**	**Ample**	
2. Premium	**Flat on renewal** • Premium increases may result where there has been an increase in revenue or a history of cyber incidents • 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** • Premium increases may result where there has been an increase in revenue or a history of cyber incidents • 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	• 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 for both public and private organizations include: – The number and type of records held by an organization – The scale of the business – Whether a company has an incident response plan, a business continuity plan and uses encryption and network security controls – The scope of cyber insurance coverage being sought and the retention level – Quality of the underwriting information provided • Companies operating in perceived high-risk sectors, such as retailers, educational institutions, financial institutions, health care providers, municipalities and ancillary services, will generally command a higher rate • 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	**Stable**	**Stable**	

Coverage

- **Loss adjustment expenses:** Some cyber insurers are now providing coverage for fees and expenses incurred by an insured to hire a third-party forensic accounting firm to establish and prove the amount of loss incurred where the insured has suffered business interruption stemming from a cyber incident. This coverage typically includes those costs incurred in connection with preparing proof of loss documentation.

- **Voluntary shutdown expenses:** Select domestic insurers are now providing coverage for business interruption loss in connection with a voluntary and intentional shutdown of computer systems after the discovery of a network security failure, whereby the insured has a reasonable belief that such shutdown would limit the loss that would otherwise be incurred as a result of the network security breach.

- **Betterment:** Historically, cyber insurance has not extended to cover the cost for an insured to replace, enhance or upgrade computer systems damaged by a cyber incident. However, some insurers now offer coverage which allows an insured to enhance or upgrade its computer system after a network security breach where certain conditions are met – most commonly, where it is recommended to avoid a similar network security failure in future. Insurers' approach to providing this coverage is not standard, with other markets choosing to pay up to a certain percentage more than it would have cost to replace the insured's original computer system model.

- **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, 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 a limited number of regulatory investigations arising out of certain alleged violations 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.

- **Business Interruption – System Failure – Direct and Contingent:** 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 within the insured organization's control. This "non-malicious" system failure trigger also extends to contingent 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.

- **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. This coverage may also be provided by select property insurers that choose to provide affirmative policy language to this effect. Aon is analyzing the situation closely to ensure that any potential coverage overlaps are addressed appropriately. Although insureds across the board will benefit from this continually broadening 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 previous gaps in existing insurance policies.

- **Property Damage:** Select London cyber 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. Certain property insurers are also choosing to provide affirmative coverage for this type of property damage. Although different coverage options exist, this type of loss is usually most appropriately covered under a property policy, although there are certain exceptions. Aon continues to work with clients and insurers to ensure that any potential coverage overlaps are addressed appropriately. We expect to see the insurance available 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

- OSFI releases new reporting guidelines for technological and cyber security incidents: The Office of the Superintendent of Financial Institutions (OSFI), regulator of federally registered banks and insurers, trust and loan companies, and private pension plans subject to federal oversight, issued an Advisory on Technology and Cyber Security Incident Reporting on 24 January 2019. The new guidelines, which became effective on 31 March 2019, apply to all federally regulated financial institutions (FRFIs) and supersede any prior guidance on cyber security incident reporting released by OSFI. Under the new guidance, technology or cyber security incidents of a "high or critical severity level" should be reported to OSFI "as promptly as possible, but no later than 72 hours". The FRFI has discretion to determine incident materiality, with OSFI noting that "FRFIs should define incident materiality in their incident management framework". However, OSFI does provide a list of criteria that may apply to a "reportable incident". The initial incident notification to OSFI should include details regarding the date/time at which the incident was assessed to be material, as well as information regarding when the incident initially took place, the severity and type (i.e. malware, data breach, extortion) of the incident, the current status of the incident as well as planned mitigation actions, and the date of internal incident escalation to senior management and/or board members. Reporting obligations are ongoing, with OSFI expecting the FRFI to provide regular updates as new information becomes available. Following the incident, FRFIs are obligated to provide OSFI with a post-incident review report, which includes lessons learned.

- What's next for PIPEDA: Canada's "Strengthening Privacy for the Digital Age" Discussion Paper: On 21 May 2019, the federal government released its discussion paper, entitled "Strengthening Privacy for the Digital Age" (Paper), outlining various proposals to amend Canada's federal private sector privacy legislation. The impetus for these amendments are multi-faceted and, perhaps, not surprising given the stance taken by the Office of the Privacy Commissioner (OPC) in its report released pursuant to the investigation of Equifax Canada. The government's recent Paper, released in the context of its Digital Charter initiative, focuses on the modernization of the Personal Information Protection and Electronic Documents Act (PIPEDA) through four key areas. The first involves enhancing individuals' control over their PII by utilizing such mechanisms as increased transparency, the right to data mobility and the right to request deletion of PII. Enabling innovation is the second area of focus, whereby the government proposed, among other measures, using data trusts as a mechanism to balance data usage with innovation. The next area revolves around enhancing the OPC's enforcement powers, providing it with the power to make cessation and record preserving orders while also potentially extending the quantum and type of fines it can levy under PIPEDA. Clarifying PIPEDA rounds out the areas of focus, with the government considering extending the scope of the legislation to various non-commercial data collection activities. The government has also indicated that it intends to update and clarify PIPEDA's application, including its treatment of transborder data flows. With the release of the Paper has come the OPC's suspension of its current Consultation on Transborder Data Flows, with the OPC planning to initiate a subsequent round of consultation pursuant to its review of the Paper. The Privacy Commissioner has indicated that, in the interim, organizations are not expected to alter their current transborder data flow practices. Legal experts speculate that these proposed amendments to PIPEDA reflect a growing trend to align Canada's privacy regime with that of the European Union's General Data Protection Regulation (GDPR). This is particularly true as Canada looks to maintain its adequacy ruling with the EU, which could be due for review in 2020.

United States

- **Nevada's amended privacy law to come into force on 1 October 2019:** An amended Nevada privacy law is scheduled to come into force on October 1, 2019, prior to January 1, 2020, when the much-discussed California Consumer Privacy Act (CCPA) is scheduled to come into force (see below for commentary on the CCPA). Whether and when the U.S. will adopt federal privacy legislation that preempts state law remains to be seen and should be monitored. The amended Nevada privacy law will apply to a data collector that also is an operator, meaning a person that: (1) owns or operates an Internet website or online service for commercial purposes, (2) collects and maintains covered information from consumers who reside in Nevada and use or visit the Internet website or online service and (3) purposefully directs its activities toward Nevada, consummates some transaction with Nevada or a Nevada resident, purposefully avails itself of the privilege of conducting activities in Nevada, or otherwise engages in any activity that constitutes sufficient nexus with Nevada to satisfy the requirements of the US Constitution. Note that there are certain exceptions to amended Nevada privacy law that must also

be analyzed. The amended Nevada privacy law provides for privacy notice and verified consumer request requirements that is spurring review and updating of U.S. privacy policies and websites. Although the privacy notice requirements are in effect now and are not changed by the amended Nevada privacy law, the definition of operator is amended by the amended Nevada privacy law. The verified consumer request requirements are added by way of the amended Nevada law. Penalties, such as injunctions and civil monetary penalties, may be imposed for violations of the amended Nevada privacy law. However, the amended Nevada privacy law does not establish a private right of action against an operator, is not exclusive and is in addition to any other remedies provided by law.

- **California's privacy law to take effect on 1 January 2020:** The California Consumer Privacy Act (CCPA) is scheduled to come into force in less than a year, on 1 January 2020. The California Attorney General anticipates publishing a Notice of Proposed Regulatory Action regarding the CCPA in the fall of 2019. The CCPA will apply to any organization, regardless of where that organization is domiciled, that: (1) collects personal information of California residents, (2) does business in the State of California, (3) determines the purposes and means of the processing of such personal information, 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 personal information 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' personal information. Note that there are certain exceptions to the CCPA that also must be analyzed regarding the application of the CCPA to an organization. The CCPA provides California residents with consumer data privacy rights (namely, disclosure, access, deletion, and opt-out rights regarding personal information, and anti-discrimination rights regarding the exercise of consumer rights) and contains privacy policy and website requirements that will spur the updating of U.S. privacy policies and websites. The California Attorney General is generally responsible for enforcement of the CCPA, under which an injunction and specified monetary penalties may be imposed. The CCPA also creates a private statutory right of action for the greater of certain amounts per California resident per incident or actual damages against organizations for the unauthorized access and exfiltration, theft, or disclosure of a California resident's nonencrypted or nonredacted personal information resulting from an organization's failure to "implement and maintain reasonable security procedures and practices".
- **State breach notification and data security laws continue to receive amendments:** A number of state breach notification and data security laws continue to receive amendments, including the following:
  - **Massachusetts:** Effective 11 April 2019, the Massachusetts breach notification law was amended to require that a breach notice to the Massachusetts Attorney General, the Massachusetts Director of Consumer Affairs and Business Regulation and any consumer reporting agency include whether an organization maintains a written information security program (WISP), plus other specified content. The WISP must contain certain required content. The amended Massachusetts breach notification law is spurring review and updating of U.S. information security programs.
  - **Oregon:** An amended Oregon breach notification and data security law is scheduled to come into force on 1 January 2020. The amended Oregon breach notification law and data security law expands its application to include vendors, meaning persons with which covered entities contract to maintain, store, manage, process or otherwise access personal information for the purpose of, or in connection with, providing services to or on behalf of covered entities, in addition to covered entities. A vendor must notify the Oregon Attorney General if the vendor was subject to a breach of security involving the personal information of more than 250 consumers or a number of consumers that the vendor could not determine unless the covered entity has so notified the Oregon Attorney General in accordance with the amended Oregon breach notification and data security law. Also, a vendor that discovers a breach of security or has reason to believe that a breach of security has occurred must notify a covered entity with which the vendor has a contract as soon as practicable but not later than 10 days after discovering the breach of security or having a reason to believe that the breach of security occurred. Moreover, if a vendor has a contract with another vendor that, in turn, has a contract with a covered entity, the vendor must notify the other vendor of a breach of security as provided in the immediately preceding sentence. The amended Oregon breach notification and data security law requires both covered entities and vendors to develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information, including safeguards that protect the personal information when covered entities or vendors dispose of such personal information.

Canadian Litigation Update

- **Recent Ontario decision illustrates difficulty in certifying privacy class actions:** The Ontario Superior Court of Justice's May 2019 decision in Kaplan v. Casino Rama denied class action certification for a lawsuit stemming from the November 2016 cyber-attack, and subsequent privacy breach, suffered by Casino Rama. The personal identifiable information (PII) of approximately 11,000 Casino Rama customers, employees and suppliers was stolen and subsequently posted online in the public domain. However, the nature of the stolen PII was diverse – some was simply contact information, while other PII was of a private and confidential nature. One of the criteria that must be met in order for a class action lawsuit to be certified is that the claims of the plaintiffs must raise common issues that are capable of being determined for all class members. The wide variance in compromised PII in this instance ultimately led to certain pleaded causes of action being denied class certification on this basis. Regarding the plaintiff's claim of negligence, the court found that the scope and content of the applicable duty and standard of care depends on the sensitivity of the PII being held. As such, an analysis of whether the defendant's cyber security safeguards were appropriate, and as such whether the standard of care was met, would depend on the type and amount of PII that was compromised. Due to the wide variety of PII at issue in this case, the court held that it was only possible to evaluate negligence on an individual basis, and that the common issue threshold was not met. The tort of intrusion upon seclusion, another of the plaintiffs' allegations, similarly fell on an analogous analysis. This cause of action does not require plaintiffs to show actual economic loss; rather, it is based on the willful or reckless invasion of privacy that a reasonable person would find highly offensive. The evaluation of this claim would, once again, be contingent upon the sensitivity of PII disclosed. As the type of PII varied between individual class members, there was no mechanism to determine whether (1) all class members' privacy had been invaded, and (2) whether such invasion would be highly offensive to each plaintiff. The claim for breach of confidence was dismissed on different grounds – this cause of action requires that the PII was misused by the defendants. As the hacker, and not the defendants, misused the class members' PII, this allegation was also denied certification.

U.S. Litigation Update

- **Mondelez cyber terrorism coverage dispute:** Mondelez was a victim of the global NotPetya malware attack in June 2017. The virus disabled and allegedly caused permanent damage to 1,700 of the company's servers and 24,000 laptops. The company also claimed theft of user credentials, unfulfilled customer orders, and other losses – altogether, damage estimates topped $100 million. Mondelez claimed the loss under its property insurance policy, which provided coverage for (1) "physical loss or damage to electronic data, programs or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction," and (2) "interruption directly resulting from the failure of electronic data processing equipment or media resulting from malicious cyber damage." In June 2018, Zurich, the insurer, denied coverage on the basis of an exclusion contained in the policy, which precluded coverage for loss from "hostile or warlike action in time of peace or war…by any government or sovereign power, military, naval or air force, or agent or authority of any party specified above." The two parties have since been locked in an ongoing coverage dispute. Notably, in February 2018, the UK government publicly attributed the NotPetya attack to Russia. Similar official statements from other nations followed, including the U.S. As the burden of proof laid with Zurich to show that the exclusion applied to preclude coverage, the insurer has pointed to these statements in support of their position that the 'terrorism' exclusion applies. However, it is important to note that Mondelez is seeking cyber coverage under its property insurance policy, which provides more limited cyber coverage compared to a dedicated cyber liability insurance policy. While most cyber insurance policies contain a 'war' or 'terrorism' exclusion, such as the one contained in Mondelez's property policy, it is market standard for this exclusion to be carved-back to allow coverage for cyber-terrorism related risk exposures, including state-sponsored cyber-attacks. In this vein, a cyber liability insurance policy can provide protection in the event an insured is the victim of a hack or malware virus potentially initiated by a state-sponsored actor.

- **U.S. derivative lawsuit stemming from data breach settles for $29M:** In September 2016, Yahoo! Inc. (Yahoo) publicly revealed a data breach that had taken place two years prior, affecting the personal identifiable information (PII) of up to 500 million users. Later that year, in December 2016, the company announced a second breach that had occurred three years prior in 2013, compromising PII of potentially all of Yahoo's 3 billion users. Shareholders in the U.S. filed a derivative lawsuit, alleging breach of fiduciary duty, unjust enrichment, insider trading, and waste against various defendants including Yahoo, Yahoo's board of directors and certain officers and senior managers. The plaintiffs claimed that Yahoo executives and board members were aware of the privacy breaches prior to public disclosure and, moreover, that the individual defendants sought to cover up the breaches. Verizon, which ultimately acquired the assets of Yahoo, was also named in the litigation for allegations of aiding and abetting. Verizon had initially announced plans to acquire Yahoo in July 2016. Following Yahoo's disclosure of the data breaches, Verizon negotiated a $350 million reduction in the acquisition price. In January 2019, the Superior Court of the State of California approved a settlement of $29 million pertaining to the lawsuit. It has been stated that the amount will be funded by insurers of both the individual defendants and Verizon, as agreed to and allocated between the two parties. This case represents the first significant recovery in a data-breach related derivative lawsuit. Notably, Yahoo also previously agreed to pay $80 million to settle securities class action litigation arising out of the same cyber security breaches.

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®