Aon Risk Solutions
Financial Services Group

State of the Market

Cyber and privacy liability

January 2018

Empower Results®

Market Update

The cyber and privacy liability market continued to have ample capacity through the second half of 2017. Both STARR Companies and Berkshire Hathaway Specialty Insurance released new cyber insurance forms in Canada inspired by their related U.S. products. Alongside domestic carriers, London markets have also provided good solutions for clients seeking coverage for more complex or individually tailored risks.

Premiums and retentions have generally remained flat on renewal for both public and private companies where other factors have stayed equal. Insureds that do not operate within an industry seen as high-risk have seen some decrease in pricing on renewal when the account is marketed. The U.S. market has hardened for big box retailers, due in part to an increased frequency and severity of data breaches affecting organizations in that sector. Other high risk sectors such as universities, financial institutions, health care providers, municipalities, and ancillary services will also generally command a higher rate.

When determining premiums, revenue is a main factor, with drastic increases resulting in higher premiums. Predictably, a history of cyber incidents will also raise rates. Insurers also continue to look to the number and type of records held by an organization, the scale of the business, and 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 are also key factors that will impact cyber insurance pricing. Clients should be aware that insurance forms available in the marketplace vary significantly in the breadth and scope of coverage, which can result in substantial rate differences among carriers.

Organizations that process electronic payment card transactions are viewed as high risk and insurers are more often requiring these insureds to be compliant with Payment Card Industry Data Security Standards (PCI-DSS). In fact, an insured may be refused coverage by some carriers where it is not compliant with PCI-DSS or may be subject to an exclusion for PCI-DSS fines and penalties (usually otherwise covered where an insured is PCI-DSS compliant). At times, insurance can be difficult to procure for clients that are perceived to have a large payment card risk exposure.

Coverage

Following the widespread outbreak of WannaCry ransomware that infected organizations around the globe, cyber extortion has become one of the most talked about cyber risks of 2017. 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. Typically coverage is only triggered by a demand for money in the traditional sense. However, as bitcoin and cryptocurrencies are now more widely available, Aon has negotiated the triggers of cyber extortion coverage to ensure it will respond in these circumstances. Aon is also working to expand the coverage trigger to ransomless extortions, in which the demand made is such that it requires the victim to take, or not take, a particular action. The Ashley Madison incident provides a well-known example of a damaging extortion where no ransom payment was demanded.

Many domestic carriers have expanded the scope of their contingent business interruption coverage. 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. Currently American International Group, Allianz Global Risk U.S. Insurance Company and Beazley Group (Beazley) are providing this coverage.

A few London carriers have started offering unique coverage options on cyber liability forms. Expanded system failure coverage is now being provided on a blanket basis, and applies to any system failure -the trigger is not limited to a third party hacking incident. Depending on the particular policy wording, this type of coverage could trigger in a multitude of situations, for example, where a system is shut down by an electrical failure specific to the insured.

Social engineering fraud coverage is also now being provided by some London insurers under 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.

The internet of things (IoT) continues to be a significant cyber risk for businesses that have automated systems. Buildings, transportation and equipment run electronically can have access points that may be exploited by third parties causing personal injury or property damage. Until recently, insurance coverage for these risks was piecemeal under property, casualty and cyber insurance products. However, in late 2016, Aon launched a new insurance product, the Aon Cyber Enterprise Solution, to address property and casualty losses arising out of a cyber-breach specifically. The policy is designed to protect large organizations against catastrophic cyber risk with a high limit/high retention approach. It is one of the first insurance products to clearly provide coverage for exposures such as cyber terrorism and property damage, products liability and other major losses resulting from an IoT related network security breach. Some Lloyds syndicates are also providing coverage to address IoT risks for companies requiring more modest retentions and limits. Now more widely available, forms such as these provide a solution for small to mid-sized businesses that are concerned with a potential cyber breach causing injury to individuals or damage to property.

In 2016, Aon collaborated with Beazley to develop an insurance program designed specifically for small to mid-sized organizations that can be applied for and purchased through an online platform. This new approach to purchasing insurance streamlines the underwriting for this category of cyber risk and facilitates an easier and less-expensive cyber insurance procurement process while providing robust coverage. The online tool can bind risks for companies with revenue of up to $200 million. Only seven non-IT related questions are required to obtain firm terms and the product provides full retroactive coverage. This easy-to-use, brokerless tool has found success across many industry sectors and regions in Canada, with numerous organizations providing positive feedback about the placement process and end pricing result.

Canadian Regulatory Update

PIPEDA's mandatory breach notification is around the corner – analysts predict Q2 2018 implementation

The much anticipated mandatory breach notification provisions of the Digital Privacy Act (Bill S-4) will soon be in force and effect. Included as part of a series of amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA) in 2015, these provisions require mandatory notification to the Office of the Privacy Commissioner and affected individuals in certain instances where a breach compromised personal identifiable information. Companies will also be required to keep a record of every breach of security safeguards for 2 years after the breach is discovered. Most legal analysts and industry experts are predicting that the regulations will be in force by the end of Q2 2018. 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 Commissioner may also disclose breach reports and records obtained from the organization to law enforcement or the Public Prosecution Service of Canada for investigation and prosecution.

The GDPR is coming to Canada: New privacy compliance challenges for Canadian companies

The General Data Protection Regulation (GDPR) is the European Union's new data privacy legislative regime, intended to harmonize privacy laws across Europe. After over four years of consultation and debate, the GDPR will come into force on May 25, 2018, superseding the Data Protection Directive 95/46/EC (Directive 95/46/EC).

The GDPR has extra-jurisdictional effect, and will apply to Canadian companies that obtain personal information of EU residents in connection with "the offering of goods or services" (irrespective of whether payment is required), or "monitoring" an individual's behavior within the EU. In the absence of judicial guidance it is prudent to construe these parameters broadly, with the result that most Canadian companies doing business with EU companies or targeting EU residents will be subject to the GDPR.

Fines for non-compliance with the GDPR 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".

As many Canadian companies will find themselves subject to the far reaching extra-territorial provisions of the GDPR, and it's uncertain whether the adequacy ruling conferred on PIPEDA under Directive 95/46/EC will continue, it is important that organizations take proactive measures to comply with the standards set out in the GDPR to ensure a smooth transition.

Canada's privacy commissioner announces stronger enforcement of privacy laws imminent

In September 2017, Canada's privacy commissioner (the Commissioner) submitted the 2016-2017 annual report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act. The report was accompanied by a written message from the Commissioner describing some of the challenges that the swift evolution of technology is creating for individuals, organizations and Canada's privacy laws.

As part of this message, the Commissioner indicated a need to modernize Canada's privacy regime, which would require changes to existing legislation and the country's national security framework, as well as a shift in the Commissioner's role from a complaints-driven ombudsman to a proactive enforcement body. To implement this change, the Commissioner has suggested that amendments to PIPEDA would be sought, permitting the issuance of orders and imposition of administrative monetary penalties for non-compliance.

While it may take some time to amend Canada's existing privacy legislation to provide the Commissioner with the additional enforcement tools requested, organizations will still have the potential to be subject to monetary penalties with respect to the mandatory breach notification and record-keeping requirements under PIPEDA, as discussed above.

CSA publishes results of cyber security and social media practices survey

Published by the Canadian Securities Administrators (CSA), Staff Notice 33-321 cyber security and social media summarizes survey results pertaining to registered firms' cyber security and social media practices. The survey was sent to over 1,000 registered firms and obtained a 63% response rate. Although 51% of respondent firms experienced a cyber security incident in 2016, a whopping 59% reported that they do not carry specific cyber security insurance. Victimized firms identified the most common type of cyber incident that they experienced as phishing (43%), followed by malware incidents (18%) and social engineering fraud (15%). Although most firms have policies and procedures to address cyber security, there are noticeable holes. For example, while a significant number of firms surveyed (66%) had a cyber security incident response plan that was tested annually, one quarter of respondents had not tested their plan at all. And, should an incident occur, preventing operational downtime is critical to minimizing loss. However, just 57% of respondent firms reported having specific policies and procedures to address continued operation during a cyber security incident. The CSA explicitly reiterated their expectation that firms are vigilant in using appropriate measures to safeguard themselves and their clients against cyber threats, and also provided various cyber security recommendations to that effect.

Canadian Litigation Update

Walmart Canada class action settled

In May 2017, Walmart Canada (Walmart) settled a class action lawsuit pertaining to a data breach that took place at a Walmart Canada Photo Centre (Walmart Photo) in 2015. Walmart Photo, operated by PNI Digital Media (PNI), was the victim of a cyber-attack when malware was installed on PNI's data center servers. Credit card data and other personal identifiable information of customers were compromised. Parallel class action lawsuits were launched against Walmart in Ontario and Saskatchewan. After the parties agreed to settle both lawsuits, an Ontario court certified the class action for settlement purposes in December 2016. The final settlement was approved by the courts in May 2017, and included costs related to legal fees, administration, customer reimbursement expenses and credit monitoring. Maximum amounts were specified under each category of costs, with Walmart and PNI potentially facing a combined aggregate payout of over CAD $1.5 million.

Equifax now potentially facing Canadian class action lawsuit

In addition to the litany of class actions facing Equifax in the U.S. (discussed further below), the troubled credit reporting company is now facing a potential class action lawsuit in Canada. In early September 2017, a statement of claim was filed in the Ontario Superior Court of Justice seeking certification of a class action lawsuit. The claim is filed on behalf of Canadian customers who had their data compromised in the well-known U.S. data breach, and is seeking aggregate damages of CAD $550 million. The action includes Equifax customers who are residents of Canada and whose personal identifiable information was accessed without authorization between May and July 2017. At the time of writing the lawsuit hadn't yet received class action certification. Aon will continue to monitor the action closely.

People's Trust class action lawsuit to proceed

Stemming from a September 2013 hacking incident in which the personal information of approximately 11,000- 13,000 customers was compromised, People's Trust, a federally regulated B.C. based bank, is now facing a class action lawsuit. Recently certified by the Supreme Court of British Columbia, the class action suit is seeking CAD $13 million in compensatory damages for numerous injuries, including damage to credit reputation and future damage due to potential identity theft. Interestingly, the court allowed both claims under PIPEDA and claims based on breach of contract, negligence and breach of the common law tort of intrusion upon seclusion to proceed. In doing so, the B.C. court stated that it was "not plain and obvious" that PIPEDA forecloses common law claims, even those claims that might provide remedies that overlap with the enforcement regime provided by the legislation. This case will be monitored as it unfolds.

U.S. Regulatory Update

This past year in the U.S. the number of state data breach notification laws continued to increase and to receive amendments. At the time of writing, forty-eight states, plus the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, had breach notification laws. Alabama and South Dakota currently do not have laws in this area.

All state breach notification laws require notification to affected individuals. Delaware's law was amended to require that, in addition to notifying affected individuals, a company must also notify state attorney generals about a breach. A new New Mexico breach notification law has similar requirements. These states join twenty-seven other states – plus Puerto Rico - whose laws require notification of the breach to a state attorney general or regulator in addition to the affected individuals.

The Delaware breach notification law was also amended to require that where there is breach (or it is reasonably believed there has been a breach) involving a social security number, credit monitoring services must be offered at no cost to each affected Delaware resident for one year. All information necessary for such resident to enroll in these services must be provided, including information on how the resident can place a credit freeze on their credit file. Such services are not required if, after an appropriate investigation, it is reasonably determined that the breach is unlikely to result in harm to the affected individuals.

This Delaware breach notification law amendment follows an amendment to the Connecticut breach notification law in 2015, which requires an owner or licensor of personal information to offer appropriate identity theft prevention services and, if applicable, identity theft mitigation services to each Connecticut resident whose first name or first initial and last name, in combination with their social security number, was or was reasonably believed to have been compromised as a result of a breach. These services must be provided at no cost for at least 12 months. All information necessary for enrollment in these services must be provided, and information on how the Connecticut resident can place a credit freeze on his or her credit file must be included. The California, Florida, and Rhoda Island breach notification laws also address identity theft prevention and mitigation services.

In 2017 the number of state laws requiring organizations to develop, implement and maintain reasonable security practices and procedures to safeguard personal information continued to increase. With the above noted new Delaware and New Mexico laws, fifteen states now have laws addressing personal information security procedures. States including New York and Ohio have recently proposed new legislation aimed at increasing the protections surrounding personal information. Similar to the Canadian landscape, this area continues to evolve in the U.S. with legal experts predicting further developments going forward.

U.S. Litigation Update

Over 70 class action lawsuits filed against Equifax since September

On 7 September 2017, Equifax announced that it had experienced a significant privacy breach affecting millions of customers. The company made the announcement after it discovered that hackers accessed social security numbers, birth dates, addresses, driver's license numbers, credit card numbers and other information between May and July of that year. It is estimated that the breach affected 143 million people in the United States in addition to some individuals in Canada and the UK. Since Equifax disclosed the breach, reports have stated that over 70 class action lawsuits have been filed against the company. Included in these is a securities class action filed in the District Court for the Northern District of Georgia-Atlanta Division on behalf of all purchasers of common stock between 25 February 2016 and 7 September 2017. The securities suit alleges that Equifax failed to maintain: adequate measures to protect its data systems, adequate monitoring systems to detect security breaches and proper security systems, controls and monitoring systems. Aon will monitor this lawsuit as it unfolds.

Class action lawsuit against Yahoo will proceed

In 2016, Yahoo announced that two separate data breaches took place – the first attack, which took place in 2013, impacted more than a billion users; a subsequent attack in late 2014 affected approximately 500 million user accounts. The account information accessed was believed to include names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5), and in some cases, encrypted or unencrypted security questions and answers.

After previously consolidating five putative class action suits against Yahoo, an August 2017 U.S. District Court ruling out of the Northern District of California found that the class action can proceed as “All plaintiffs have alleged a risk of future identity theft, in addition to loss of value of their personal identification information.” While many of the claims were dismissed, thus reducing the scope of the litigation, the judge offered the plaintiffs an opportunity to amend their allegations. Many class action lawsuits in the U.S. resulting from data breaches are dismissed due to the inability of the plaintiffs to establish that the victims suffered an actual or threatened injury. Now that the plaintiffs have surpassed this hurdle, in part, it remains to be seen what liability Yahoo will face.

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.

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.

Empower Results®