Cyber Challenges

What recent American developments reveal about the potential future of cyber liability in Canada.

BY ANNE JUNTUNEN

While the availability of standalone cyber insurance policies in Canada has increased, the field is still in its infancy. This article reviews recent development in the U.S. while offering a perspective on the uniquely Canadian factors that may affect how cyber insurance claims will develop in this country.

Introduction to Cyber Insurance

Standalone cyber liability policies are principally aimed at covering insureds for losses resulting from unknown third parties hacking into the insured's computer systems and accessing, deleting, or publishing data. Cyber policies often include both third-party coverage (i.e., defence costs and indemnity in the event of a customer's claim for damages arising from the insured's failure to adequately protect the customer's data) and first-party coverage (i.e., reimbursement for loss arising from the insured's costs to respond to breaches, such as IT support and public relations specialists).

This straddling of the third-party/first-party divide is a singular feature of cyber insurance. This has the potential to create challenges as insurers consider whether certain claimed damages fall more appropriately under one or the other – an important question, as many cyber policies provide different limits for each side.

Although data breaches are often the first risk when considering cyber insurance, they are not the only exposures. Depending on the policy, cyber insurance can also cover claims involving defamation, infringement of intellectual property rights and ransom payments associated with cyber extortion threats. Some cyber policies have borrowed coverages usually found in fidelity policies, such as computer fraud and funds transfer fraud coverages.

One challenge of this new line of insurance is the lack of common wording. Unlike older areas of insurance, such as CGL or professional liability, there is no standard "form" cyber policy or wording. The Insurance Services Offices has now published a standalone cyber policy that may eventually serve as an industry standard, but for now, the coverage and wordings available under cyber policies are as varied as the number of insurers that underwrite these policies.

Case Law Interpreting Cyber Policies

To date, there are no Canadian decisions interpreting the scope of standalone cyber liability coverage. In the U.S. there have been only two issued actions involving coverage under cyber insurance policies. The first was *Travelers v. Federal Recovery Services Inc.* (No. 2:14-CV-170-TS D.Utah May 11, 2015), in which the insured, a payment processing company, had been sued by its client for refusing to return certain credit card and bank information belonging to the client's customers. The court held that the insurer had no duty to defend because the client alleged that the insured had intentionally breached a contract, not acted negligently. This decision simply confirmed that cyber liability policies will be treated like traditional liability policies for purposes of assessing whether the insurer has a duty to defend.

In the second action, *Columbia Casualty v. Cottage Health Systems* (No. 2:15-CV-3432 C.D.Cal., filed May 7, 2015), the insurer sought a declaratory judgment that its standalone cyber policy did not provide coverage for an in insured health care provider's data breach. The insurer's position was based on an exclusion for failing to maintain appropriate encryption and other cybersecurity measures. Under the exclusion, coverage was unavailable for any loss arising out of the insured's failure to "*continuously implement the procedures and risk controls*" identified in the insured's coverage application. Unfortunately for the many cyber insurance practitioners anxiously awaiting the court's analysis, the case was dismissed in July 2015 because the insured had not exhausted the policy's alternative dispute resolution requirements.

While it provided no answers, *Columbia Casualty* highlighted a question that is likely to arise again: what are the minimum standards required for insureds under cyber policies that contain such exclusions? And, might the benchmark be different for differing types of companies (i.e., a hospital versus a retail store)?

Although *Travelers* and *Columbia Casualty* may provide some glimpse into the future of cyber insurance litigation, they provide little guidance as to how cyber policies will be interpreted north of the border. In fact, most recent developments have involved the prospect of coverage for data breaches under *non*-cyber policies. For example, in *Eyeblaster*, the court suggested that a CGL policy could potentially cover claims by a third party alleging that the insured had frozen and rendered the third party's computer inoperable (*Eyeblaster, Inc. v. Federal Insurance Co.*, 613 F.3d 797 8th Cir. 2010).

This decision is notable in that U.S. courts have generally held that CGL policies do *not* respond to data breaches. In addition, shareholder litigation in the wake of the widely-publicized Target and Neiman Marcus data breaches has led to speculation about a new wave of litigation against directors and officers who fail to adequately prevent and respond to breaches, with questions about the extent to which D&O coverage may be called upon to respond.

Although cases decided in the CGL and D&O contexts are not directly applicable to cyber coverage, judges are wrestling with similar challenges that cyber insurers will inevitably face. One such challenge involves causation and damages: has the insured's customer suffered a loss simply because her personal information has been compromised, notwithstanding that no stolen-identity loss has yet occurred? And if a customer does eventually suffer an identity-theft loss, how can this be traced to a particular data breach? If cyber policies respond to liability for damages resulting from data breaches, this can significantly affect the magnitude of the risk insured.

The Seventh Circuit Court of Appeals recently touched on causation in a class action brought by customers whose credit card information had been compromised as part of the 2013 Neiman Marcus data breach. In *Remijas v. Neiman Marcus* (WL 4394814 7th

Cir. July 20, 2015), the court held that the class plaintiffs may pursue their action notwithstanding that they had not yet suffered identity theft as a result of the breach. The court held that there was an objectively substantial likelihood of the plaintiffs suffering that result.

Cyber Breaches in the Canadian Context

As the cyber insurance market grows throughout North America, some uniquely Canadian factors are likely to influence the development of cyber coverage here. One is the deeply ingrained value of privacy as an element of the individual's right to autonomy. Academics have posited that, unlike Americans who tend to view privacy as a matter of protecting one's liberty from government intrusion, Canadians view privacy as a matter of protecting one's dignity, which includes shielding one's personal information from misuse by corporations and other individuals. This may be one reason why the scope of a private right of action for privacy-related torts is showing signs of expanding.

The Ontario Court of Appeal first recognized the tort of intrusion upon seclusion in 2012 (*Jones v. Tsige*, 2012 ONCA 32). More recently, in *Hopkins v. Kay* (2015 ONCA 112), the Ontario Court of Appeal held that individual claimants may issue private actions against health care providers who breach their privacy by failing to adequately protect claimants' information. Under *Hopkins*, a health care provider's privacy breach may lead not only to sanctions by the Privacy Commissioner, but also to claims by individual plaintiffs or even class actions by plaintiffs. The broadening of individual rights of action for disclosure of, or failure to protect, private information has the potential to increase the number of claims made under cyber policies.

New regulatory requirements are also likely to change the risk that could be covered under cyber policies. Currently, Alberta is the only province with mandatory privacy breach notification for non-health care-related organizations. However, under the new Digital Privacy Act, PIPEDA has been amended to add mandatory data breach notification. The mandatory notification provisions will require companies to notify the Privacy Commissioner and possibly also the individuals whenever there is a breach that presents a "real risk" of harm such as identity theft or reputational damage. While these provisions are not yet in force, they are widely expected to increase the uptake of cyber insurance policies as companies recognize the risk of penalties for failure to report and the inevitable claims that will come when a breach becomes public.

Conclusion

The uptake of cyber insurance policies in Canada is expected to increase as media coverage of highly-publicized breaches continues to keep the risk visible, particularly as mandatory data breach reporting requirements come into effect. While we wait for the first Canadian cyber claim to wend its way into and through court, claims professionals would be wise to keep one eye turned southward for a preview of what's to come.

Anne Juntunen is an associate at Halfnight McKinlay P.C. in Toronto and a member of Canadian Defence Lawyers. Her practice includes coverage advice and litigation in fidelity and other commercial insurance matters. The author thanks Madeleine Dinnissen, Specialty Claims Examiner at Chubb Insurance Company of Canada, for her input into the issues surrounding cyber policies in Canada.