CANADIAN Lawyer

Demand for cyber-insurance on the upswing

Awareness about cyberbreaches has reached the mainstream, but the law is still nascent

By Michael McKiernan

When Patrick Bourk started touting cyber-liability insurance to clients a decade ago, he got little more than blank stares in return.

"The insurance market was near barren in terms of interest," says Bourk, a trained lawyer who is also the senior vice president of Integro Insurance Brokers in Toronto.

Five years ago, a higher proportion of his audience knew what he was talking about, but they were almost as unlikely to take him up on the offer.

"They would often profess to have the best IT department in the world to handle their cyber-liability exposures," rendering insurance "unnecessary," Bourk says.

Since then, a series of high-profile and costly breaches at some of the largest companies in the world has gradually chipped away at that confidence: In the U.S., retailers Target and The Home Depot each suffered breaches that compromised the debit and credit card data of millions of customers, while closer to home, hackers exposed the personal details of users of the Canadian dating web site Ashley Madison, which specializes in facilitating extramarital affairs. Earlier this year, the University of Calgary also admitted paying off cybercriminals to unfreeze almost 10,000 faculty and staff e-mail accounts after its systems were infected with a ransomware virus.

TARA HARDY

Demand for cyber-insurance products has in turn "grown exponentially," as businesses come to terms with the possibility they could be the next victim of a headline-making cyberattack, according to Bourk. A recent study by PricewaterhouseCoopers attempted to put numbers to the trend, predicting annual premiums worldwide, which stand currently at around US$2.5 billion, will double to about US$5 billion by 2018 and treble to US$7.5 billion as soon as 2020.

"It's growing at a rapid clip," says John Davis, whose Toronto firm Gilbertson Davis LLP has recently formed a cyber-liability sub-specialty within its insurance and commercial litigation practice group.

And while litigation around policies

in Canada is currently scarce, some firms have channelled Wayne Gretzky, developing expertise in the area in anticipation of the eventual arrival of that particular puck.

"We feel that for any insurance defence firm, you have to start being part of the cyber-insurance world, because it's going to become more and more of an issue," says Kadey Schultz, co-founder of Toronto boutique Schultz Frost LLP.

As the sector matures, "it will become a core area of practice for a number of lawyers going forward," predicts David Mackenzie, a partner at Blaney McMurtry LLP with a focus on insurance litigation.

Greg Markell, president of Ridge Canada Cyber Solutions, says coverage under policies is typically divided into first party, relating to expenses incurred in the immediate aftermath of a security breach, and third party, which applies to losses or damages caused to customers as a result of the incident.

Lawyers are already establishing themselves as "breach coaches" appointed under first-party claims, to quarterback the response effort following a cyberattack. They co-ordinate a team that can include systems engineers, IT companies and public relations specialists working to recover lost data, notify regulators and affected customers and get the company back up and running as quickly as possible.

"Breach coaches should always be lawyers. I'm of the opinion that your first call after a breach should be to a lawyer, so that they can help protect privilege. After that, they're helping to triage the process," Markell says.

Jill Shore, a lawyer with Vancouver insurance boutique Dolden Wallace Follick LLP who has acted as a breach coach for companies, says someone at the firm is always on call for insured businesses facing a cyber-emergency.

"They get a 1-800 number in their policy, where we provide them with some limited free advice if it's needed on an urgent basis. If they choose to retain us to proceed further, then they have the benefit of knowing that we have been pre-approved by the insurance company in the event there is coverage," she says.

Shore also carries out more traditional work for insurance companies in the cyber realm, drafting policies and advising them on the implications of amendments or enhancements made to them.

According to Davis, parties to cyber-insurance policies face "enormous challenges on the drafting front" thanks to the disconnect between ancient traditional policy terms and language and the modern cyber-risks to which they are being applied.

In addition, no two cyber-insurance policies are alike, according to Bourk. At this early stage in their evolution, they tend to be bespoke products, changing depending on the specific needs and attributes of individual clients.

"The exposures of a retailer are often different to those of a municipality, a hospital, a manufacturer, a hi-tech company or a professional firm such as a law firm," he says. "Coverage and premium negotiations, depending on the client, can be nuanced."

Underwriters, too, are facing struggles thanks to the lack of data and loss history needed to make reliable actuarial calculations about exposure. Meanwhile, the level of competition in the market has prevented them from taking too conservative an approach to premiums levels. With as many as 60 insurers offering cyber-insurance products of one sort or another, competitors can easily price themselves out of the market.

"It's an interesting time to be an underwriter. To a great extent, they're operating in the dark. Nobody knows if they're taking in enough premiums to cover the risk," Mackenzie says. "That's why policies are drafted the way they are: There are some fairly broad exclusions and some very carefully crafted agreements."

When the current wave of new customers advances to the next phase in the life cycle of an insurance policy and the claims start rolling in, light will be shed on some of the unknowns troubling underwriters. According to Davis, the current emphasis on exclusions could also mean a spike in coverage disputes.

"There are a plethora of exclusions, which may take away more coverage than the insured anticipates in some of these types of polices," Davis says.

For example, he says some cyber-insurance policies could be interpreted as excluding claims for breaches that occurred due to human error, an arguable factor in the vast majority of cyber-breaches.

"You may find exclusions for mechanical failures, errors in design or incompatibility of software, and we don't really know how they are going to be treated," Davis says.

According to Schultz, some case law on point will prove extremely valuable to the cyber-insurance policy drafters of the future, since virtually none exists yet in Canada. Although there are some decisions that give guidance on privacy rights and potential damages when those rights are violated, she says there are still a lot of gaps in the jurisprudence.

"I have said in the past that it feels almost like the Wild West in Canada, because the way our system works is that we need to establish this body of case law to give some specific guidance and standards," Schultz says.

Shore says the situation reminds her of the work she did in environmental and aboriginal law in the mid-1990s near the start of her career.

"Every time a new case came out, it changed the legal landscape," she says. "It's like any developing area of the law. Until you get some decisions, it's wide open."

In the meantime, Shore says lawyers can learn a lot from cases south of the border, where cyber-insurance has a much longer history and the jurisprudence has developed further.

"We pay very close attention to what is going on in the U.S. The regime in many places is quite statute driven, so the case law will not always be analogous, but when they are taking old established legal principles and applying them to new facts, that can be very helpful," she says.

Belinda Bain, a partner at Gowling WLG in Toronto, says at the very least U.S. cases provide clues as to which issues might get litigated in this country.

"It can also set the framework for the analysis that a Canadian court has to make, even if the law is not identical," says Bain, the co-head of the international firm's Toronto insurance group.

For example, she says a number of

U.S. courts have pronounced on the applicability of traditional commercial general liability policies to cyber-related losses. Back in 2014, Sony claimed for coverage after a massive hack exposed the personal details of PlayStation users. However, a New York state judge sided with the company's insurer, Zurich, which argued it had no duty to defend because the data release by the hackers did not amount to "publication" under the general liability policy.

The matter is still the subject of some controversy, since a more recent decision by the U.S. Fourth Circuit appeal court recently ordered an insurer to defend a health-care client whose patient records ended up in an unencrypted form online on the basis that the leak could potentially amount to a "publication" under a similar provision of the company's general liability policy.

Either way, Bain says there's a good chance insureds in this country will make similar claims in the event of a big cyber-loss.

Bourk says another recent U.S. case involving Asian food chain P.F. Chang's holds important lessons for Canadian players in the cyber-insurance market. The company's insurer reimbursed $1.7 million paid out to customers whose credit card details were posted online by hackers in 2013. However, a court decided the insurer was justified in refusing to reimburse a further $2 million P.F. Chang's spent on payment card industry fees due to the breach because they were not covered by the policy.

"That protection is available, but they did not purchase it. It's important to know exactly what you are buying from your broker," Bourk says.

"I would say that Canada is about 10 to 15 years behind the U.S. right now when it comes to cyber-insurance. We're at the early stages, but we're catching up quickly," he adds. **CL**