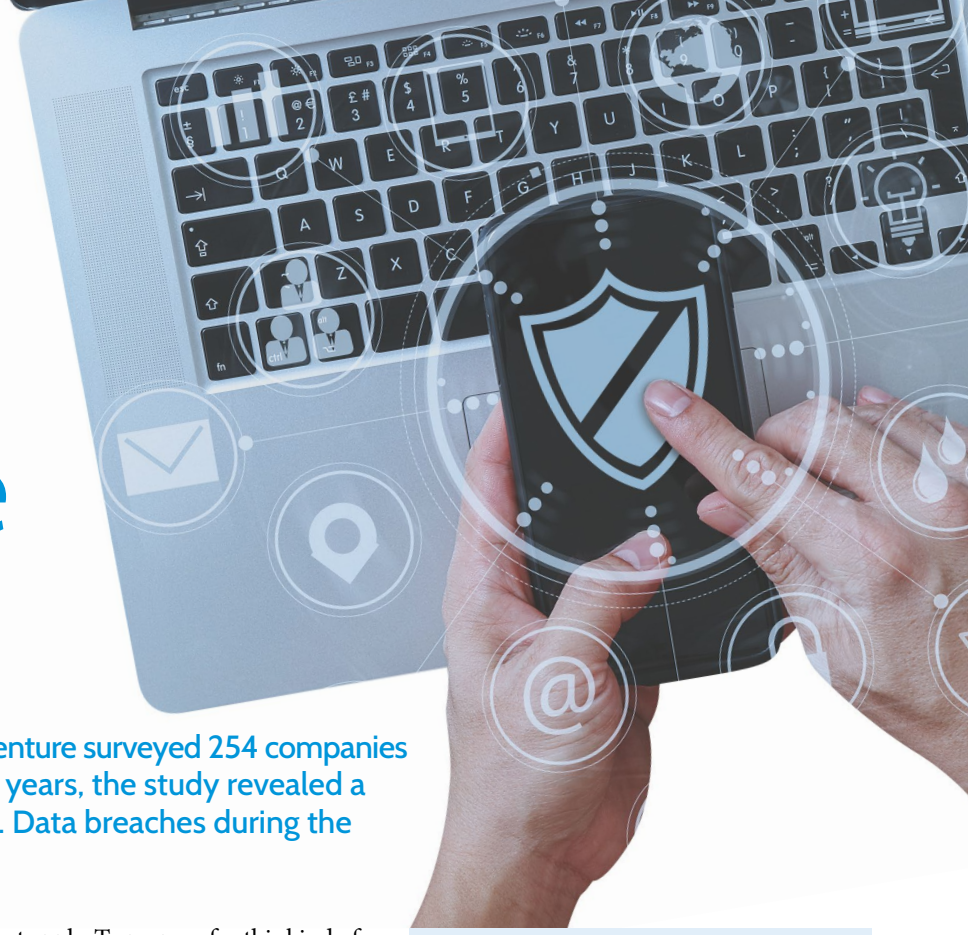
Does your firm need cybercrime insurance?



In a study titled *The Cost of Cybercrime*[1], Accenture surveyed 254 companies in seven countries. Over the course of five years, the study revealed a 62 per cent increase in cybercrime attacks. Data breaches during the same period doubled to 130 per year.

Accenture noted that while not every security breach results in a loss, the two most costly types of breaches (malware and web-based attacks) can take days (up to 23 days in the case of ransomware) to resolve and cost firms over $2 million per incident on average.

LawPRO first suggested that lawyers consider cyber insurance in the December 2013 issue of *LawPRO Magazine*. In the article *Cyber Risk Options: Do You Have the Coverage You Need?* firms were advised that their general liability insurance policies (intended to cover bodily injury and property damage scenarios) may offer only a limited amount of coverage for cyber-related exposures. These policies were not designed to cover loss of data or a breach of a law firm network.

In addition, the cyber coverage under the LawPRO policy is subject to eligibility criteria and a modest sublimit. Says LawPRO's Assistant Vice President, Underwriting, Victoria Crewe-Nelson: "the LawPRO cybercrime coverage relates to professional services. If, for example, a loss (e.g. corrupted accounting data, theft from the general account) does not relate to the provision of professional services, LawPRO coverage would not apply. To prepare for this kind of risk, lawyers should consider exploring broader cyber coverage available in the marketplace."

The rapid growth of cyber insurance

According to Integro Insurance Brokers of Toronto, 10 years ago there was almost no familiarity with or interest in cyber insurance. Now, despite widespread awareness of the risks, many firms still feel their own IT departments can handle cyber dangers.

In light of recent high profile security breaches, demand for cyber insurance has grown 'exponentially.'[2] From 2015 to 2016, the Risk Management Society's worldwide *Cyber Survey*[3] found a 30 per cent increase in companies procuring stand-alone cyber insurance.

The numbers in Canada may not be quite as high. According to a 2017 FICO-sponsored survey of 350 international organizations (including Canadian law firms) 36 per cent of polled Canadian companies have no cybersecurity insurance. Of those that do, less than 20 per cent believe that the insurance will cover all cyber risks.[4]

What are "professional services"?

The 2018 LawPRO policy provides the following definition:

PROFESSIONAL SERVICES means the practice of the law of Canada, its provinces and territories, where conducted by or on behalf of an INSURED in such INSURED'S capacity as a LAWYER or member of the law society of a RECIPROCATING JURISDICTION (not as a member of the Barreau du Québec), subject to Part II Special Provision A; and shall include, without restricting the generality of the foregoing, those services for which the INSURED is responsible as a LAWYER arising out of such INSURED'S activity as a trustee, administrator, executor, arbitrator, mediator, patent or trademark agent.

[1] accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
[2] canadianlawyermag.com/author/michael-mckiernan/demand-for-cyber-insurance-on-the-upswing-3400/
[3] rims.org/aboutRIMS/Newsroom/News/Pages/2017CyberSurvey.aspx
[4] canadianunderwriter.ca/insurance/36-polled-canadian-firms-no-cyber-security-insurance-fico-1004114548/

These statistics reflect the experience of larger companies, but Crewe-Nelson warns that smaller firms should also take heed: "Cybersecurity at smaller firms may be less sophisticated and there are fewer statistics regarding how many are purchasing cyber insurance coverage. But small firms are at the same risk as their larger counterparts."

Where do breaches occur?

Some breaches happen at the technology front end: through email, laptops, mobile devices, and desktops. Many hackers find these to be the a firm's weakest link because they depend on employees' diligence in following proper security procedures.

Other breaches target the back end of a firm's IT network: storage, servers, backup systems, and wireless encryption. In addition, new security problems may soon emerge in the context of the internet of things, increased cloud computing, and the constant expansion of social media. Hackers are continually adapting their methods to new technologies. Visit practicepro.ca/cyber to read more about the cyber dangers targeting law firms.

What does a typical cyber insurance policy cover?

First, there is no such thing as a "typical" policy: different insurers offer different products and a wide range of sublimits. If the insurance is purchased through a group plan, the underwriting might be straightforward, but will typically include only modest limits. A more bespoke insurance product may require detailed underwriting, explains Crewe-Nelson, and may include multiple lines of coverage with corresponding separate sublimits. "Consider, as an example," says Crewe-Nelson "what counts as a business interruption once a cyber-attack occurs: how long does a system have to be down before coverage kicks in, and how soon afterwards will coverage be exhausted?"

Coverage can also include both first-party losses (losses suffered directly by the firm that purchases the policy) and third-party losses (losses suffered by a firm's clients as a result of a breach). It can be made available for scenarios in which the cause of the incident is internal (staff or lawyer at the firm) or external hackers.

Coverage can extend to:

- Specified costs associated with an attack, for example:
  - Lost income and operating expenses related to a loss of business due to a cyber-attack or pre-emptive network shutdown; and/or
  - Hardware, software and data recovery costs
- Payments demanded for cyber extortion/ransomware
- Crisis management expenses, such as IT forensics costs and public relations spending
- Defence expenses related to regulatory fines or penalties
- Measures to help prevent a breach
- Technical assistance to respond to an attack or breach
- Assistance with the aftermath of a breach

Why aren't more companies buying cyber coverage?

Integro states that some of the barriers to wider uptake of cyber insurance policies include confusion around how cyber insurance premiums are set, difficulties in adapting traditional insurance policy language to modern cyber threats, and a lack of data and loss history to make reliable actuarial calculations.

Also, it remains unclear how these policies will respond to claims, and what kinds of breaches will be excluded from coverage. For example, the wording in some policies could be interpreted as excluding breaches caused by human error, mechanical failure or incompatible software. As the market matures and decisions on cyber coverage are made by the courts, there may be more clarity for both law firms and insurers. In the meantime, firms are advised to ask questions of their insurance brokers: it's worth an investment of time and effort at the outset to get as much clarification as possible when comparing policies from different insurers.

Some insurers offer prevention resources

It can be challenging for medium and small firms to develop and implement their own cybersecurity policies and infrastructure. Keeping up with the constantly evolving nature of cyber risk can be beyond the expertise of a typical law firm IT department. In addition to coverage for financial losses, a number of insurers provide access to broader technical support similar to that offered by cybersecurity firms (see "Outsourcing Your Firm's Cybersecurity" available on practicepro.ca). Such services may include:

- Around-the-clock access to cybersecurity specialists
- Training for firm staff to help prevent a breach
- Assistance with notifying clients of the breach

Crewe-Nelson notes that access to a breach coach can be a significant asset in cases of cyber extortion and ransomware: "The coach can help determine whether the ransom should be paid, and can coach staff about how to do it. There are examples of companies phoning up and asking if they can pay for the return of just certain key documents, and being told no. Once the full ransom is paid, the company realizes that the criminals have withheld the sensitive information that the firm helped identify – and that they are now demanding a premium for those."

If your Ontario firm has not yet explored cybersecurity coverage options, we urge you to do so. The cost of a cyber-breach goes beyond the financial losses of stolen funds, damage to equipment and lost income. There is also the damage to a firm's reputation and the loss of confidence of its clients. With many insurers now offering cyber risk policies, firms have many options to tailor a policy to their specific needs. ■

Tim Lemieux is Claims Prevention & Stakeholder Relations Coordinator at LawPRO.