Interesting times (and cybercrimes)

call for active risk reduction efforts, not just insurance coverage

Legal systems and their participants have a reputation – perhaps no longer just – for being slow to embrace technological change. But while good lawyers know that technology tools are not (at least not yet!) a full replacement for the exercise of professional judgment and the application of legal knowledge, they also know that a head-in-the-sand approach to the hurtling evolution of computer technology is a recipe for being trampled.

The stampede, in this analogy, involves two different herds: the first is comprised of honest competitors who, using technology to their own and their clients' advantage, will claim an ever-increasing share of the legal services market. The second herd is more sinister: tech-savvy criminals increasingly use the Internet to exploit both human and technological vulnerabilities in their quest to steal money and valuable information.

In the previous issue of *LawPRO Magazine* we explored the future of legal services, and in doing so, touched on some of the technologies driving that evolution. In this issue, we turn our attention to the "black hats" of the high tech world: the perpetrators of cybercrime.

Cyber criminals have lawyers and law firms in their sights. For one thing, lawyers' computer systems often harbour valuable information – not just clients' personal information, but also information about pending commercial deals, trade secrets, and intellectual property: information that is worth money. Lawyers' computers also, in many cases, provide access to actual funds, in the form of trust account monies accessible via electronic banking.

Not only do law office computers contain valuable information, but they can also be fairly vulnerable from a security perspective. Smaller firms may not have staff with the knowledge needed to build state-of-the-art security systems, and generally do not have in-house computing professionals available to monitor and respond to immediate threats. While good-quality security products are available at a cost that is affordable for most small firms, the extent to which firms have

actually invested in and implemented these protections varies widely. Cyber criminals prey on the most vulnerable firms. When a firm's security system is weak, the firm can easily become a target.

We know that law firms are targeted by cybercriminals, because these attacks are often in the news, and even directly reported to us via the practicePRO program's AvoidAClaim blog or in the form of claims. We reviewed the issue of cyber risk in 2013, and have introduced a $250,000 sublimit of coverage for eligible cybercrime claims in our 2014 policy. See "The LawPRO $250,000 cybercrime coverage: What it covers and why" at page 25 for more information on this coverage.

While "coverage" can be a comforting word, lawyers would be making a big mistake in feeling comfortably complacent about cybercrime. The potential for losses from cybercrime for any firm is equal to *or greater than* the balance in the firm's trust accounts plus the value of the confidential information contained in its computer systems. Why greater? Because cybercrime can lead to reputational, equipment, and business interruption losses, too. These losses are not covered by your LawPRO policy.

In the article "Other cyber risk insurance options: Do you have the coverage you need?" on page 26, we discuss types of cybercrime insurance coverage, other than professional indemnity coverage, that you may want to consider. But this information – and those types of coverage – come with a very important caveat: *no* form of insurance coverage should be seen as a complete answer to cybercrime.

In fact, to the extent that overly rich insurance coverage for cyber losses creates a disincentive to law firms to invest in appropriate security protections, such coverage actually encourages cyber attacks. In introducing modest sublimit coverage, we hope to provide a small safety net, without inspiring dangerous complacency on the part of lawyers and exploitative behaviour on the part of criminals.

An insurance "band-aid" is not enough. Preventing cybercrime requires an active, vigilant, and multi-faceted approach. It is the responsibility of each of us to reduce our vulnerability to cybercrime, both in our professional and in our personal lives. Cyber security is a complex discipline that requires not only technical protections (such as antivirus and anti-malware programs), but also the learning, adoption, and consistent application of protective behaviours like using strong passwords and changing them regularly.

The first step in improving your firm's cyber security is to educate yourself about the nature of the risks and the approaches available for dealing with them. In this issue, we introduce some of the most important cyber risks in "Cybercrime and law firms: The risks and dangers are real" at page 6. In "Protecting yourself from cybercrime dangers: The steps you need to take" at page 10, we review some of the best strategies that firms can use to reduce their exposure to those threats.

But lawyers must not stop there. Each of us must come to embrace cyber security as an important aspect of life-long learning. While I don't count myself an expert quite yet, I've had my share of learning experiences. For example, when I needed to have a new wireless network established for my home computer, I watched with interest as the technician stepped outside to see if he could gain unauthorized access to my system. He couldn't, but I was shocked to discover the number of unprotected networks in my own neighbourhood. More recently, I learned about the differences between an antivirus program and an anti-malware program – the biggest take-away being, it's not a question of choosing one or the other – you need both! But while there are doubtless many other aspects of cyber security that I will need to investigate further, my awareness is growing, and my behaviours are evolving. These days, when I encounter a site that does not allow (or require) me to choose a "strong" password (don't know what that means? See the "Tech Tip: Keeping your passwords strong and secure" on page 30!), I find myself wondering about other aspects of the site's security, and about what risks I might be incurring by doing business there. I know that I'm gradually developing the cyber safety instincts that will reduce my risk of becoming a victim of cybercrime. I hope that the articles in this issue will help other lawyers do the same. Relying on insurance coverage to prevent or "solve" cybercrime is tantamount to shutting the stable door after the horse has bolted. Only active risk reduction will give us a fighting chance against those who would threaten our funds, our privacy, and our professional reputations.

Kathleen A. Waters
President & CEO