Outsourcing your law firm's cybersecurity

According to a survey[1] of UK law firms, a quarter of them have been the victims of cyberattacks, as have almost a third of US firms according to the ABA *Legal Technology Survey Report*. While there has not been a similar survey done of Canadian firms, the numbers are probably similar. And the high-publicity hacks keep coming: recent examples of firms suffering cyber breaches include Cravath, Swain & Moore in New York, Johnson & Bell in Chicago, and of course the Panama Papers hack of Mossack Fonseca.

In the examples above the hackers were after client data stored on firm servers, but they can also target client trust account money through spear-phishing attacks or malware attached to emails. Recently, firms' networks have been the victim of ransomware attacks in which firm data was locked until a ransom was paid to the hackers.

The financial and reputational damage of a cyber-breach to both clients and law firms can be severe. Clients are increasingly demanding to know what cybersecurity safeguards firms have in place and making it a condition of doing business.

It can be challenging for medium and small firms to develop and implement their own cybersecurity policies and infrastructure. Hardware and software can be costly, and hiring (and keeping) knowledgeable IT people can be difficult when they are in such high demand. Keeping up with the constantly evolving nature of cyber risk can be beyond the expertise of a typical firm. While large firms may be able to afford to spend what it takes to shore up their cyber defences, what should smaller firms do?

To meet this need, a number of data protection services have emerged that allow companies (including law firms) to outsource their cybersecurity. Companies offering these services include Ekota (ekota.ca), Cyberscout (cyberscout.com), and FireEye® (fireeye.com).

The benefits are similar to outsourcing of other IT functions: it can be cost effective for firms to essentially share the costs of infrastructure and expertise, while ensuring that software and threat detection is always up-to-date. Using these companies can also have the advantage of flexibility as the services can be purchased depending on the particular needs and size of a firm. And as firms grow or data security needs change, the services offered can be scaled accordingly.

In addition to standard IT functions like storage and communications that some firms have already begun to outsource, the security services offered by these companies that would be of interest to law firms may include:

- Consultants to assess your firm's data security needs and identify vulnerabilities
- Data security software and training staff on its use
- 24-hour technical support in the event of a breach
- Incident response planning
- Outreach to clients affected by the breach
- Advice on dealing with cybersecurity insurers in the event of a breach

While LawPRO is not in a position to make recommendations as to any one company and the services they offer, it may be worthwhile for firms to consider this option if they are struggling with how to offer the best cybersecurity to their clients within their own particular staffing and budget constraints.

For further reading on the threat of cyber risks, and why law firms are considered to be lucrative targets, see *Locked Down: Practical Information Security for Lawyers* and the *ABA Cybersecurity Handbook*, both available in the practicePRO lending library (practicePRO.ca/library) as well as December 2013 Cybersecurity issue of *LawPRO Magazine* (lawpro.ca/magazine). ■

[1] The survey results are published in the *NatWest annual legal benchmarking report.*