Torkin Manes
Barristers & Solicitors

Article

Emerging Technology
Technology, Privacy & Data Management

July 2019

Tech competence should be required

By Lisa R. Lifshitz

With data breaches making news almost daily, I was not surprised by a recent survey by Robert Half Legal that found that 87 per cent of 150 full-time lawyers surveyed in Canada said their law firm plans to either slightly or significantly increase their resources allocated to cybersecurity-related tools in the next 12 months.

While it's laudable that some lawyers are finally taking the need for better cybersecurity more seriously, this is no guarantee that the legal profession has grasped the importance of effective cybersecurity protection. And that's because the word must come from the top – namely, our law societies.

It is utterly shocking to me that, in 2019, lawyers and law firms where I practise in Ontario (and to my knowledge, everywhere in Canada) are not explicitly required by their regulatory body to have a basic minimum understanding of the technology, privacy and cybersecurity necessary to protect their clients. Simply put, there is currently no mandatory legal duty of technological competence required of lawyers. Period.

In Ontario, s. 3.1.1. of the Rules of Professional Conduct set out the various positive duties of competence that lawyers are supposed to possess. For example, a "competent lawyer" means a lawyer who has and applies relevant knowledge, skills and attributes in a manner appropriate to each matter undertaken on behalf of a client, applying appropriate legal skills, pursuing appropriate professional development to maintain and enhance legal knowledge and skills and otherwise adapting to changing professional requirements, standards, techniques and practices.

Conspicuously missing, however, is an explicit obligation for lawyers to have a minimum understanding of technology, including for the protection of clients.

What does technological competence look like for lawyers?

Arguably, all lawyers should understand basic information security practices and ensure they have reasonable policies and measures in place to protect client data against intrusion. Technology containing

client data should be hardened against third-party hackers and malware, using firewalls, encryption tools, appropriate anti-virus technology/URL threat protection and other security software. Lawyers should stop using legacy software and always use supported versions of software that receive regular security patches and updates from their vendors. They should also deploy adequate backup and recovery software. Individual lawyers should periodically undergo cybersecurity training or self-educate so they don't make the basic mistakes that compromise their clients' data (i.e., no more coffee shop Wi-Fi).

Additionally, technological competence should include lawyers doing a thorough job vetting and selecting cybersecurity vendors. Lawyers should perform due diligence and not just choose the least expensive option. Lawyers and their firms should devote sufficient resources to help manage this process. While it is tempting to entirely outsource to the cloud, lawyers must still choose their vendors wisely as not all cloud providers employ the same level of security or contractually meet required legal/regulatory or other security standards.

Critics may argue that it is unreasonable to expect all lawyers to understand technology and cybersecurity. To that I say: balderdash. Clearly the duty of technological competence will have to be tailored to individual practices as lawyers use technology differently. It will ultimately be up to law societies to determine the base level of technological competency (and the scope of the exact regulatory duty), but that is no reason why they shouldn't be able to regulate this requirement in the same manner that they regulate other areas.

To its credit, the Law Society of Ontario appears to be moving in this direction. It recently established a technology task force and has posted a technology guideline on its website. However, the LSO undercuts the importance of its own advice by stating that "a decision not to follow the Guideline will not, in and of itself, indicate that a member has failed to provide quality service. Conversely, use of the Guideline may not ensure that a lawyer has delivered quality service. Whether a lawyer has provided quality service will depend upon the circumstances of each case." It's not exactly a ringing endorsement!

Sole practitioners and smaller firms may decry the costs of technological competency, but this argument ignores the risks (and the prohibitive costs) associated with data breaches, not to mention mandatory federal data breach reporting requirements, as well as reputational and financial losses (including loss of clients). Being small is no excuse for ignorance or inadequate cybersecurity practices. Resources do exist. Moreover, lawyers who do not feel that they do possess the necessary technical acumen can also hire reputable technology consultants.

Given the regulatory gap, many large clients have taken matters into their own hands by requiring law firms to attest to their technological competence and overall cyber-readiness in their RFP documents and engagement letters. However, don't all clients deserve adequate technological competence and cyber-preparedness rather than just the larger ones?

The time for lawyers to have a positive and meaningful duty of technological competence has arrived. Our clients deserve nothing less.

This article originally appeared as Lisa's IT Girl column in Canadian Lawyer Magazine.

Author

Lisa R. Lifshitz is a partner in Torkin Manes' Business Law Group, specializing in technology and privacy law, and is the leader of the firm's Technology, Privacy and Data Management Group. She has been nationally and internationally recognized for her technology law expertise and enjoys writing and speaking on technology law issues. She is the immediate past president of the Canadian IT Law Association.

Lisa R. Lifshitz
Partner

Tel: 416 775 8821
llifshitz@torkinmanes.com