Federation of Law Societies of Canada | Fédération des ordres professionnels de juristes du Canada

Media Monitor | Relevé des nouvelles

How hackers broke into four of Canada's top law firms, stole client files and caused chaos

The Globe and Mail/ online/ posted October 30, 2026

One week ago, lawyers at Canada's top firms received urgent calls from their IT departments about a critical software update or an expired password. The agents were happy to stay on the phone and help.

Even to a skeptic, the calls could seem legitimate. They were often placed through Microsoft Teams, appearing to come from internal IT employees, or they were phone calls from the IT department's number.

The reality: Hackers were on the other end, spamming Canadian lawyers en masse.

The tactic the hackers used is called vishing, short for voice phishing – and it worked. At least four companies were broken into, all among the country's most prestigious law firms: McCarthy Tétrault LLP, Davies Ward Phillips & Vineberg LLP, Bennett Jones LLP and Borden Ladner Gervais LLP.

The extent of the damage is still being assessed, but the fallout is already immense. Law firms market themselves as trusted advisers, and the nature of their work means they store sensitive files on their servers. These include non-public corporate information, communication between client and counsel, and their clients' tax, financial or health records.

Because so much sensitive information is potentially exposed – at McCarthy Tétrault, 31,000 files were stolen, according to a source directly involved – some clients are extremely concerned, but so far remain in the dark. Lawyers at the hacked firms have been told which clients were affected, but specific details are often still coming, according to four sources and communication reviewed by The Globe and Mail.

Still unknown in some cases, according to one of the sources: the hackers' identities, how they're using the stolen information, and whether the firms are monitoring the web for leaked data or have found any yet.

The Globe is not identifying the sources because they are not authorized to speak publicly about the data breaches.

There's also a fear of more breaches to come. Hackers are increasingly targeting law firms, and the Canadian hack proves even the largest firms with the most sophisticated technology can't always ward them off. What the top firms spend on hacking defences would likely exceed the annual revenues of scores of smaller boutiques across Canada that specialize in practice areas such as employment and family law.

Across the four firms that were breached, at least seven employees granted the hackers access to internal files, according to The Globe's reporting and confirmed by the respective firms. McCarthy Tétrault had four employee accounts compromised; Bennett Jones had two; Davies had one. It is unclear how many users were compromised at BLG.

The depth of the breaches varied. At Bennett Jones, the firm's document management system, used to protect client legal files and work product, was not affected, the firm said Friday. Its accounting system was also unaffected.

"The compromised information included reports on revenue from clients; for certain clients, general descriptions of our mandates for them were also involved and as we identify those clients, we will contact them directly," Bennett Jones said in a statement.

At BLG, an internal investigation confirmed that "certain files, including files related to clients, were accessed by an unauthorised third party," the firm said Friday in a statement.

On Thursday, McCarthy Tétrault said a third party "gained access to certain files, including information relating to clients," while Davies said Thursday it identified "the compromise of information from one account." McCarthy Tétrault was hacked on Oct. 22 and Davies was hacked on Oct. 23.

Vishing attacks are a form of social engineering in which cybercriminals use telephone calls or voice messages to trick victims into giving them access to accounts or sharing sensitive information.

Targeting law firms by impersonating IT employees takes advantage of the fact that people at large companies are unlikely to know all of their co-workers, said Brent Arnold, a cybersecurity lawyer and the founder and principal of Capstan Legal. On top of that, turnover in an IT department can be high.

“The anonymity of working in a really big organization makes it easier to pull this off, because it comes in on your Teams, it looks legitimate, it sounds boring enough that it’s probably real,” Mr. Arnold said.

“That’s part of why it’s working – you’re exploiting the weakness of a large organization where not everybody knows each other,” he added.

Mr. Arnold said these types of attacks often fool higher-level employees. They’re more likely to skip cybersecurity training, and are “always in a hurry,” giving them less time to question whether what they’re seeing is legitimate. “Busy people are easier to exploit.”

With technological advances, hackers are getting more sophisticated and learning to find their ways into organizations that have defences in place, such as multifactor authentication (MFA).

In the law firm breaches, employees who followed the hackers’ instructions were directed to fraudulent sign-in pages capable of bypassing MFA. In a recent security warning, researchers at Google wrote that the rise of these vishing campaigns “underscores the critical importance of organizations moving toward phishing-resistant MFA” to protect their systems.

In Canada, law firms and IT departments are working together to understand how the hackers got access to confidential data, what to do to help clients and how to ensure it doesn’t happen again.

“All the major law firms, and in particular all the CIOs [chief information officers], are sharing intel and best practices,” Peter Castiel, Montreal-based chair of Stikeman Elliott LLP, said in an interview. (Stikeman was recently targeted by hackers, but was not breached.)

Mr. Castiel said lawyers are being urged to explain the full extent of the problem to clients, as well as steps being taken to fix the issues. Regarding client relationships, he said: “The first and most important step is being completely transparent.”

McCarthy’s has brought in cybersecurity firm CrowdStrike of Austin, Tex., to investigate, while BLG has engaged Mandiant, a cybersecurity consulting firm and Google subsidiary.

Return to the newsletter