OSLER

Cybersecurity and privacy: key takeaways from our second annual conference

This is the first in a series of articles recapping the second annual Privacy Conference in Montréal.

Access all five Updates in this series

NOVEMBER 21, 2025 6 MIN READ

Related Expertise

- Artificial Intelligence
- Corporate Governance
- Disputes
- Privacy and Data Management
- Risk Management and Crisis Response
- Technology

Authors: Éloïse Gratton, Ad. E., François Joli-Coeur

Key Takeaways

- Osler's second Annual Privacy Conference focused on key issues like Law 25 amendments, cybersecurity, and AI governance.
- Guillaume Clément, a cybersecurity expert at KPMG, emphasized that cybersecurity is a shared responsibility across organizations, not just a tech issue.
- Organizations must adopt comprehensive strategies to counter AI-driven fraud and enhance their human and technical defenses.

In October, Osler's Montréal office hosted the firm's second annual Privacy Conference, organized by the Privacy and Data Management team. The half-day program, followed by a networking lunch, brought together industry experts and in-house counsel to discuss a range of hot topics, including the implementation of amendments introduced by Law 25, emerging litigation trends, artificial intelligence governance, new technologies, and cybersecurity.

One highlight of the event was a conversation between Eloïse Gratton, partner and Co-Chair of Osler's national Privacy and Data Management practice, and Guillaume Clément, partner, Advisory, Cybersecurity at KPMG, and President of KPMG Egyde Conseils. Below are the key insights from their discussion, with practical guidance for Canadian organizations.

Guillaume Clément: an expert perspective on modern cybersecurity threats

Drawing on his many years of hands-on experience across a range of industries, Guillaume regularly advises organizations that have been the target of sophisticated cyberattacks. His message was clear: threats are evolving rapidly, and meeting them requires more than technology — it demands strong culture, sound processes and committed leadership.

"Cybersecurity is no longer solely the domain of the CISO or CIO — it's a shared responsibility

across the entire organization," says Guillaume.

Biometric data: the risk isn't always where you think

Biometric data (e.g., fingerprints, facial recognition, voice recordings, iris scans) is often viewed as the most sensitive form of personal information. However, not all biometric data carries the same level of risk. According to Guillaume, the danger increases mainly when this information is centralized and linked to other personal identifiers, such as names or device IDs.

"Standalone biometric data is difficult to exploit. The risk comes from combining it with other databases," says Guillaume.

When stored separately and in the form of a biometric template, this information becomes much harder to reuse. Even when biometric databases are stolen — which is rare — putting the data to practical use is still a technical challenge. Nevertheless, under the *Act respecting the protection of personal information in the private sector* (ARPPIPS) and the *Act to establish a legal framework for information technology*, both recently amended by Law 25, organizations must comply with a stringent set of obligations when collecting biometric information. They must ensure the collection is strictly necessary, obtain express consent, and file the required declaration with the Commission d'accès à l'information du Québec.

Cyber insurance: strategic partner or emerging risk?

Insurance companies now play an essential — and increasingly influential — role in managing cybersecurity incidents. Many have built specialized teams that support insured organizations during forensic investigations and even in communications with cybercriminals.

Guillaume sees this as a natural evolution of the market and a sign of the sector's increasing professionalization. At the same time, he notes that coordination among stakeholders — including insurers, organizations and technical experts — can pose challenges related to governance, confidentiality and strategic alignment that must be navigated carefully.

Another trend is the adoption of stricter coverage conditions. Insurers are increasingly denying claims when organizations have not implemented the minimum security measures required under their policies. To mitigate this risk, organizations should

- carefully review the technical clauses in their insurance policies
- document their compliance practices and existing security measures
- most importantly, maintain control over their incident response plan

Quantum computing: future threat, present risk

While quantum computing is not yet an immediate threat, it could ultimately undermine the foundations of modern cryptography and render obsolete many of the standards currently used to protect sensitive data.

According to Guillaume , the key issue today is the "harvest now decrypt later" (HNDL) strategy. "Some actors — particularly state-sponsored ones — are already storing massive volumes of encrypted data in anticipation of eventually decrypting them using quantum computing," he says.

To prepare without veering into alarmism, organizations should start by identifying where their encryption mechanisms are deployed, mapping sensitive data and communications,

and integrating quantum risk into their technology and security roadmaps. A gradual, crypto-agile approach — combined with monitoring standard-setting efforts (such as those led by NIST) — enables organizations to reduce HNDL risk without overinvesting or disrupting operations.

AI-driven fraud: the era of deepfakes and targeted disinformation

Digital fraud has evolved significantly with the rise of generative AI. Visual and audio deepfakes and multichannel phishing campaigns are becoming more convincing, easier to produce, and harder to detect.

“In the hands of malicious actors, AI is a powerful tool of persuasion. It exploits trust and urgency — two universal human pressure points,” says Guillaume.

He points to a striking example: one senior executive received a coordinated series of emails, text messages and voice calls that perfectly mimicked a superior. Although entirely AI-generated, the attack appeared authentic down to the smallest detail.

To counter these threats

- some organizations are testing three-factor authentication that combines technical, behavioural and personal verification
- segmented access controls and dual-control procedures are becoming essential standards
- employee training should also cover identifying synthetic content

Despite the tools available, human error remains the leading cause of incidents. Training is the first line of defence, but it must be supported by automated detection and verification mechanisms.

Organizational security: rethinking human defences

Privacy laws require organizations to implement appropriate physical, technical and organizational measures to safeguard personal information.

While this requirement is technologically neutral, regulators are increasingly clarifying what it means in practice. Recent decisions from oversight authorities provide a more precise understanding of what constitutes “appropriate security.”

Yet on the ground, Guillaume notes that

- most incidents originate from unpatched software vulnerabilities, poorly secured remote access, phishing, malicious attachments, and configuration or human errors
- security tools are frequently misconfigured or underused
- the number of detected incidents is rising — not necessarily because attacks are increasing, but because organizations now have greater visibility and stronger detection capabilities

“Cyberattacks exploit both technical and human weaknesses, which is why multilayered security is essential: updates, strong authentication, training, vigilance and sound governance,” says Guillaume.

Recommended best practices include continuous employee training using real-world scenarios, measuring human resilience through simulation testing, and integrating

cybersecurity considerations into management decisions from the earliest stages of project design.

Governance and leadership: cybersecurity as a business imperative

According to Guillaume, cybersecurity is a strategic governance issue that extends far beyond the technical realm. “CEOs and boards of directors must understand digital risks in order to ask the right questions and make the right decisions,” he says.

Yet despite ranking among the top organizational risks, cybersecurity remains underfunded and underprioritized. CISOs and CIOs are often overextended and struggle to obtain the resources they need.

The gap between recognizing the risk and taking concrete action persists. The solution? Committed leadership, backed by a cybersecurity culture embedded at every level of the organization.

Conclusion: building digital trust

Guillaume ‘s insights highlight how legal, technological and strategic considerations are inseparable. In a Canada where regulations, technologies and threats are rapidly evolving, an effective response requires three things: preparation, coordination and governance.

Leaders must anticipate what’s ahead and turn cybersecurity into a driver of trust and performance.

Key insight

“Cybersecurity is not a cost — it is a vital investment to preserve and strengthen the trust of all stakeholders.”
Guillaume Clément

About the event

Osler’s second Annual Privacy Conference took place in Montréal on October 21. Organized by the Privacy and Data Management team, the half-day event brought together law, technology and governance professionals to discuss the strategic issues shaping personal information protection in Canada.

If you have questions about personal information protection, cybersecurity incident management or data governance, our team is here to help.