Cybersecurity and post-quantum cryptography: burying your head in the sand in a quantum world

October 5, 2026

Authors

Eric Lavallée

Partner, Lawyer Partner, and Trademark Agent

Kiran Younas

Lawyer

The cryptographic mechanisms that currently secure digital transactions, communications and signatures may become vulnerable with the advent of sufficiently powerful quantum computers. For businesses, the issue is no longer merely technological: it also affects governance, contracts, information protection and migration planning.

Understanding post-quantum cryptography

Imagine spending an entire week without transmitting sensitive information over the internet—no banking, no checking health records and no shopping online. Everyday transactions rely in particular on cryptographic mechanisms that:

protect the confidentiality and integrity of information;
authenticate individuals and systems; and
secure digital signatures.

However, the advent of sufficiently powerful quantum computers could compromise some of these mechanisms and consequently undermine a key pillar of our current digital security.

Cryptography brings together the techniques used to protect the confidentiality and integrity of information, authenticate individuals and systems and secure digital signatures. It plays a role in particular when a browser displays a padlock icon, someone electronically signs a document or a company transmits confidential data. Many of these mechanisms rely on public-key cryptography, which uses a pair of mathematically linked keys: a public key and a private key. These keys derive their security from mathematical problems that would take conventional computers an astronomical

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

amount of time to solve. A sufficiently powerful quantum computer, however, could solve some of these problems in virtually no time. As a result, widely used mechanisms, such as RSA and elliptic-curve cryptography, will no longer offer adequate protection.

The immediate nature of the quantum threat

Currently, only prototype quantum computers exist, and it is still difficult to predict exactly when they will become commercially viable or when major corporations and nation-states will use them. The Canadian Centre for Cyber Security nonetheless estimates that a quantum computer capable of posing a threat to current mechanisms could emerge as early as 2030, while acknowledging the uncertainty surrounding this timeline.[1] In August 2024, the U.S. National Institute of Standards and Technology released its first three standards establishing cryptographic algorithms capable of withstanding this threat.[2] For organizations, the issue is therefore not merely knowing when the threat will materialize, but determining what steps to take today to keep their information and systems secure into the future.

Post-quantum cryptography refers to methods designed to resist attacks from both conventional computers and future quantum computers. From a mathematical standpoint, resistant algorithms exist, but many IT systems have yet to adopt them.

The threat of “Harvest Now, Decrypt Later”

The most pressing threat can be summed up by the phrase “Harvest Now, Decrypt Later.” A threat actor can intercept and store encrypted data today, then attempt to decrypt it once sufficient quantum capacity becomes available. Information that retains its value or sensitivity over several years, such as trade secrets, financial data, strategic information and privileged communications, is therefore at the greatest risk.[3]

The level of urgency depends on each organization's specific technological infrastructure. Key considerations include how long information must remain confidential and the time required to replace vulnerable mechanisms. According to Canadian best practices in the field, some systems have product lifetimes of 15 to 30 years, and a cryptographic migration can itself take several years.[4] An organization can therefore fall behind long before a cryptographically relevant quantum computer ever reaches the market.

Why businesses rely on their suppliers for the transition

Most organizations do not develop replacement cryptographic solutions themselves. Instead, they rely on their software, cloud service, hardware, certificate and cybersecurity vendors.

Such reliance does not make planning pointless—on the contrary. It shifts the focus toward governance, procurement and contracts.

When it comes to contracts, organizations must assess these risks right now, particularly the allocation of liability between the contracting parties. Ideally, technology service contracts should specify whether the provider or the client bears the risks associated with using technologies that fall short on quantum security. Achieving balanced risk allocation requires open dialogue: Client organizations must ask the right questions and technology providers must be transparent about the limits of their systems.

The federal government has begun its transition to post-quantum cryptography

The federal government is no longer treating post-quantum cryptography as just a research topic. In June 2025, the Canadian Centre for Cyber Security published a roadmap to migrate the Government of Canada’s unclassified systems. Among other milestones, the document establishes an initial

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

departmental plan and a first progress report starting in April 2026, the migration of high-priority systems by the end of 2031, and the migration of all other relevant systems by the end of 2035.[5] A Security Policy Implementation Notice, which took effect in October 2025, reinforces these requirements and compels relevant federal institutions to demonstrate measurable progress.[6]

While these milestones do not apply directly to private businesses, they can still indirectly affect federal contractors. Since April 1, 2026, in-scope federal contracts with a digital component must incorporate clauses that support post-quantum cryptography and cryptographic agility, among other requirements.[7] Federal directives make clear that orderly migration requires governance, inventories, prioritization, financial planning, procurement policies and coordination with vendors.

Moreover, the post-quantum transition is by no means confined to the federal government. In September 2026, Canada joined a call to action from the G7 Cyber Security Working Group urging public and private organizations to adopt a phased, risk-based transition. Canadian guidelines likewise recommend that organizations begin preparing before large-scale solutions are rolled out.[8]

Legal implications for Quebec businesses

No Quebec statute expressly requires private businesses to use any specific post-quantum algorithm or complete a migration according to the federal timeline. Instead, Quebec law establishes functional and technologically neutral obligations, which require the adequacy of the selected measures to be assessed in context.

Protection of personal information and reasonable security measures

The *Act respecting the protection of personal information in the private sector* requires businesses to take reasonable security measures, taking into account, in particular, the sensitivity, purpose, quantity and distribution of the information and the medium on which it is stored. It also mandates a privacy impact assessment for projects to acquire, develop or overhaul information systems or electronic service delivery systems that process personal information.[9] For an organization that retains sensitive information with a lifespan of several years, such as banking information or Social Insurance Numbers, the quantum threat may become a material factor when assessing whether existing security measures are reasonable.

Document integrity and confidentiality of transmissions

The *Act to establish a legal framework for information technology* follows the same approach, requiring in particular that the integrity of a document be maintained throughout its life cycle. For instance, where the information contained in a document is declared by law to be confidential, section 34 requires that it be protected by means appropriate to the mode of transmission.[10] Documentation explaining the mode of transmission and the measures taken to protect confidentiality must also be readily available to prove compliance.

Rather than mandating specific technologies, the law sets outcome-based obligations, in particular safeguarding document integrity and information confidentiality.

Civil liability and the state of knowledge

As Quebec legal scholars emphasize, security measures only matter in the eyes of the law if they

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

actually work.[11] Accordingly, official publications and technical standards—while not giving rise to a civil obligation on their own—can help establish the state of knowledge, the foreseeability of the risk and recognized industry practices.[12]

An organization's liability regarding its data protection obligations must be assessed according to the general rules of civil liability.[13]Liability would turn primarily on whether the organization acted with prudence and diligence at the relevant time, taking into account:

the knowledge available at the time;
the sensitivity of the protected information;
the lifespan of its systems; and
the availability of alternative solutions.

Using a cryptographic mechanism that could soon become vulnerable may constitute a civil fault in light of current knowledge.

Connected devices and reasonable security expectations

Similar considerations could apply to manufacturers, distributors and suppliers of connected devices. Under the *Civil Code of Québec*, factors include the safety that a person is normally entitled to expect and the state of knowledge at the time the item was manufactured, distributed or supplied. Given these criteria, a product's reasonably expected capacity to receive security updates could form part of the circumstances weighed when assessing a potential safety defect.[14]

Practical steps for businesses to prepare now

Preparing does not call for an immediate overhaul of all existing mechanisms. Rather, it requires developing cryptographic agility—the ability to identify and replace cryptographic mechanisms without having to rebuild the underlying systems from scratch. The Canadian Centre for Cyber Security recommends a number of practical measures in particular:[15]

Inventory cryptographic assets. The inventory should cover internal and client-facing systems, certificates, authentication mechanisms, digital signatures, network equipment and cloud services. Special attention should be paid to legacy, custom-built or hard-to-update systems.
Establish priorities. Organizations should identify information that must remain confidential over the long term and systems whose modification or replacement will require several years.
Engage vendors. Organizations should obtain their vendors' post-quantum roadmaps to determine whether the transition can be completed through updates or if it will require acquiring new products. Applicable standards, support lifecycles and impacts on interoperability should also be verified.
Align contracts and procurement. New agreements could include, as appropriate, terms governing security updates, end-of-support notifications, the adoption of standardized mechanisms, cooperation during migration and the allocation of associated costs.

Not all organizations face the same level of exposure. However, immediate attention is warranted where a business retains sensitive information over multiple years, operates systems that are difficult to replace or relies on vendors whose migration roadmaps remain unknown. While vendors will likely deliver the technical solutions, each organization must understand its own requirements, ask the right questions and ensure it remains agile enough to adopt these solutions when the time comes.

Key takeaways:

The quantum threat is already here, even if quantum computers capable of breaking certain cryptographic mechanisms are not yet widely available.
The primary threat is "**Harvest Now, Decrypt Later**."Data encrypted today can be intercepted, stored and decrypted in the future.
The most exposed organizations are those that **retain sensitive information over many years**, operate systems

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

that are difficult to replace or rely on vendors whose migration strategies are uncertain.
In Quebec, there is no general obligation mandating any specific post-quantum algorithm, but businesses are bound to adopt **reasonable security measures**, assessed in context and in light of the state of knowledge.
Preparation starts with **cryptographic agility**: inventorying assets and uses, prioritizing critical systems, engaging vendors and adapting contracts.

---

1. CANADIAN CENTRE FOR CYBER SECURITY, “Preparing your organization for the quantum threat to cryptography (ITSAP.00.017),” February 2025, online: https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017
2. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, “NIST Releases First 3 Finalized Post-Quantum Encryption Standards,” August 13, 2024, online: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
3. CANADIAN CENTRE FOR CYBER SECURITY, *supra*, note 1.
4. CANADIAN FORUM FOR DIGITAL INFRASTRUCTURE RESILIENCE and CANADIAN NATIONAL QUANTUM READINESS WORKING GROUP, *Canadian National Quantum-Readiness Best Practices and Guidelines,* Version 04, July 10, 2024, pp. 3–7, online: https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/documents/Quantum-Readiness%20Best%20Practices%20-%20v04%20-%2010%20July%202024.pdf.
5. CANADIAN CENTRE FOR CYBER SECURITY, *Roadmap for the migration to post-quantum cryptography for the Government of Canada* (ITSM.40.001), June 23, 2025, p. 13, online: https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001.
6. TREASURY BOARD OF CANADA SECRETARIAT, *Migrating the Government of Canada to Post-Quantum Cryptography: Security Policy Implementation Notice*, effective since October 9, 2025, online: https://www.canada.ca/en/government/system/digital-government/policies-standards/spin/migrating-government-canada-post-quantum-cryptography.html.
7. TREASURY BOARD OF CANADA SECRETARIAT, *supra*, note 6, s. 6.3.1.
8. CANADIAN CENTRE FOR CYBER SECURITY, “G7 Cybersecurity Working Group call to action on preparing for the post-quantum era,” September 3, 2026, online: https://www.cyber.gc.ca/en/news-events/g7-cybersecurity-working-group-call-action-preparing-post-quantum-era?; CANADIAN FORUM FOR DIGITAL INFRASTRUCTURE RESILIENCE and CANADIAN NATIONAL QUANTUM READINESS WORKING GROUP, *supra*, note 4, ss. 3–5.
9. *Act respecting the protection of personal information in the private sector*, CQLR c. P-39.1, ss. 3.3 and 10.
10. *Act to establish a legal framework for information technology*, CQLR, c. C-1.1, ss. 6 and 34.
11. Éric LABBÉ, “L’efficacité technique comme critère juridique ou la manière dont les lois se technicisent,” (2004) 9-2 *Lex Electronica*.
12. Éric LABBÉ, “La multiplicité des normes encadrant le contrat électronique : l’influence de la technologie sur la production des normes,” (2004) 9-2 *Lex Electronica*; Charles-Étienne DANIEL, “Coder son propre droit : quand la machine pousse l’humain à énoncer de nouvelles normes de gouvernance,” dans *Quand la société fait son droit : la gouvernance de proximité en action*, 2026, EYB2026QSD19, pp. 397–432.
13. *Civil Code of Québec*, CQLR, c. CCQ-1991, s. 1457; *Act respecting the protection of personal information in the private sector*, supra, note 9, s. 10.
14. *Civil Code of Québec,* supra, note 13, arts. 1468, 1469 and 1473.
15. CANADIAN CENTRE FOR CYBER SECURITY, supra, note 1; CANADIAN CENTRE FOR CYBER SECURITY, *Guidance on becoming cryptographically agile* (ITSAP.40.018), May 2022, online: https://www.cyber.gc.ca/en/guidance/guidance-becoming-cryptographically-agile-itsap40018.

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.