AXIS / Technology

Practical Guidance

Quantum Risk: Cyber and D&O Exposure

Why every organization must reassess encryption, governance, and insurance before quantum disruption arrives.

Written by Tristan Smith

Quantum computing is not simply another cyber trend. It represents a potential disruption to the cryptographic foundation that allows companies to secure data, authenticate users, sign software, process transactions, and trust third-party systems.

The risk is not that every company will face a quantum-enabled attack tomorrow. The risk is that encrypted data can be stolen today and decrypted later, while migration to quantum-resistant cryptography will take years. PLUS frames quantum risk as more than a technology issue; it is also a balance sheet, governance, and liability issue for cyber insurers, D&O underwriters, boards, and risk managers.

This matters now because the standards are no longer theoretical. NIST has finalized its first principal post-quantum cryptography standards, including FIPS 203 for key establishment, FIPS 204 for digital signatures, and FIPS 205 as an additional digital signature standard.

From Encryption Risk to Enterprise Risk

Quantum risk refers to the possibility that future quantum computers will be able to break widely used public-key encryption algorithms that protect data, network communications, software updates, identity systems, and digital signatures.

1. **Harvest Now, Decrypt Later:** Threat actors steal encrypted data today with the expectation that they will decrypt it once quantum capabilities mature. This is especially concerning for information with long-term value, including health records, biometrics, trade secrets, government communications, financial information, and intellectual property.
2. **Future Cryptographic Failure:** Once quantum computing reaches sufficient capability, commonly used encryption and signature systems could become unreliable. That could affect VPNs, TLS/SSL, digital signatures, identity systems, authentication tools, blockchain-based assets, and other trust-based infrastructure.

Why This Matters: A Structural Shift in Loss

Traditional cyber risk analysis often treats encrypted data as lower severity if the encryption keys were not compromised. Quantum risk weakens that assumption.

A breach involving encrypted data today may not appear catastrophic at the time of discovery. Years later, if that data can be decrypted, the same incident could create privacy claims, regulatory scrutiny, contractual disputes, reputational harm, and litigation. This creates a long-tail cyber exposure: the theft happens now, but the harm may emerge later.

The Cyber Coverage Gap: Breach Today, Claim Tomorrow

Most cyber policies were not written with quantum-enabled decryption in mind. A quantum-related loss could raise difficult coverage questions:

- Which policy period responds: the year data was stolen, the year it was decrypted, or the year a claim was made?
- Is quantum decryption a security failure, a cryptographic failure, a systemic vulnerability, or something else?
- Does encrypted data theft trigger notice obligations if the data cannot yet be read?
- Could systemic risk, infrastructure, war, or state-backed actor exclusions become relevant?
- Does dependent business interruption apply if the failure occurs inside a critical vendor environment?

Broker's Recommendation: Review cyber wording now, particularly definitions of security failure, privacy event, dependent business interruption, system failure, data restoration, regulatory coverage, exclusions, and notice triggers.

D&O Exposure: When Inaction Becomes the Claim

Boards do not need to become cryptographers. They do need to oversee material cyber and technology risks and show that management has a credible process for identifying, prioritizing, budgeting for, and managing the transition.

Potential D&O allegations could include:

- Failure to oversee cybersecurity readiness;
- Inadequate investment in post-quantum migration;
- Misrepresentation of the company's data security posture;
- Failure to identify risks in major vendors or acquisition targets; and
- Inadequate disclosure of cyber risk management and governance.

For public companies, this also intersects with cyber disclosure controls. Material incident reporting, annual cybersecurity risk management disclosure, and board governance narratives all increase the importance of documenting how emerging cyber risks are escalated and addressed.

Insurers Are Paying Attention

Cyber and D&O underwriters may not expect a completed migration today, but they will increasingly expect a clear process. Companies should be ready to answer practical questions:

- Have you inventoried where cryptography is used?
- Which data would remain sensitive if decrypted five, ten, or twenty years from now?
- Have critical vendors provided post-quantum cryptography roadmaps?
- Is quantum risk included in the cyber risk register?
- Has the board or risk committee been briefed?
- Is migration planning aligned with IT refresh cycles and budget forecasts?

Absent these controls, organizations may face tougher underwriting questions, narrower coverage, reduced limits, or less favorable terms. Conversely, a documented readiness process can help distinguish the organization as a better-managed risk.

Practical Readiness Measures

A quantum readiness plan does not need to begin with a full technology overhaul. It should begin with visibility, ownership, and documentation.

1. **Cryptographic Inventory:** Identify where the organization relies on public-key encryption, TLS/SSL, VPNs, certificates, digital signatures, identity systems, APIs, code signing, cloud services, hardware security modules, and embedded systems.

2. **Data Lifespan Review:** Prioritize data that would still cause harm if exposed years from now, including health information, biometrics, trade secrets, source code, financial records, M&A materials, and sensitive customer data.

3. **Vendor Roadmap Diligence:** Ask critical vendors whether they support post-quantum cryptography, whether they have a migration timeline, and whether their products are crypto-agile.

4. **Contract and Procurement Updates:** Build post-quantum readiness, crypto-agility, security update obligations, incident notice, and vendor roadmap requirements into new technology contracts.

5. **Board-Level Reporting:** Add quantum risk to the cyber risk register and provide periodic updates to the board or risk committee.

6. **Insurance Alignment:** Review cyber and D&O policies to understand how coverage may respond to encrypted-data theft, delayed harm, vendor failure, disclosure claims, regulatory investigations, and securities-related allegations.

Broker's Recommendation: Start with the assets and relationships that matter most: long-life sensitive data, externally exposed systems, identity infrastructure, cloud providers, and vendors that control encryption, authentication, or digital signatures.

From Future Risk to Current Governance Obligation

The companies best positioned for quantum risk will not necessarily be those that migrate first. They will be the companies that can demonstrate a thoughtful process.

That means knowing where cryptography lives, identifying which data has long-term sensitivity, engaging vendors, documenting board oversight, and aligning insurance coverage with the way the risk may actually unfold.

Takeaway

Quantum risk is not science fiction. It is a developing cyber, contractual, and governance issue that is already relevant to underwriting, board oversight, vendor management, and disclosure controls.

The question is no longer whether quantum exposure exists. The question is whether your organization can show that it has identified the risk, assigned responsibility, and started building a credible migration and insurance strategy.

Contact us for assistance reviewing your cyber and D&O program against emerging quantum risk.

Contact Us

Chris Jones
Account Executive,
Mining & Technology
+1 (778) 788-2853
Chris.Jones@axisinsurance.ca

Clive Bird
Senior Vice President,
Mining & Technology
+1 (604) 817-8072
Clive.Bird@axisinsurance.ca

Stacey Copeland
Vice President,
Mining & Technology
+1 (604) 619-7775
Stacey.Copeland@axisinsurance.ca

Tristan Smith
Business Development Specialist,
Mining & Technology
+1 (416) 885-0671
Tristan.Smith@axisinsurance.ca

About

Axis Insurance - Safeguarding the Exceptional. Axis Insurance is your strategic advantage; we cut through the complexity of risk management enabling you to confidently embrace the opportunities of tomorrow. Our role is to provide you with the best insurance value that combines coverage, service and price. We also provide personalized, quality service that includes professional insurance advice, ongoing policy maintenance and claims support. When any issue arises regarding your insurance coverage, we are your advocate, using our professional experience to best represent your individual interest. Follow Axis on LinkedIn, X, Facebook and Instagram. Stay up to date by signing up for our newsletter here.

axisinsurance.ca
#2000 – 1055 Dunsmuir Street, Box 49264, Vancouver, B.C. V7X 1L2
1-800-690-7475