AXIS / Technology

Risk Atlas

Axis Technology Risk Atlas

May 2026 Edition

Recommended Risk Improvements, Industry Trends, and Emerging Technology Insights.

This month, we examine how quantum readiness, AI buyer confidence, and advanced tech infrastructure are becoming operating, contractual, and insurance realities. May's edition focuses on where technology trust must be evidenced before growth can scale.

Client Highlight: Quantum Secure Encryption Corp. helps organizations prepare for quantum-era cybersecurity through readiness, entropy delivery, and quantum-proof storage.

Subscribe for Monthly Tech Risk Highlights

Monthly Summary

May's risk theme is trust under pressure. Encryption, AI performance, and advanced technology supply chains are no longer abstract risk categories; they are becoming part of how buyers diligence vendors, boards allocate budgets, and insurers assess whether coverage can respond.

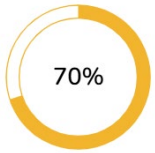
If you are selling AI into enterprise environments, relying on long-life sensitive data, custodying digital assets, or scaling infrastructure into customer deployments, this is the month to test whether your controls, contracts, and insurance strategy can prove the risk is being managed.

Contents

Industry Trends

What's shaping the technology risk landscape.

PQC is Now a Board and Procurement Issue

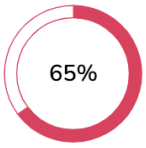


With NIST standards usable and Canada's Cyber Centre roadmap setting plans, reporting, and phased deadlines through 2035, quantum readiness now affects board oversight, budgets, procurement, and vendor evidence.

Quantum Capital Goes Commercial

McKinsey reports quantum start-up investment hit $12.6B in 2025, with 90% going to quantum computing. Commercialization raises IP, confidentiality, indemnity, reliance, and coverage questions.

"Harvest Now" Extends Breach Risk



Google's 2029 PQC migration timeline highlights today's risk: encrypted data stolen now may be decrypted later, extending liability well beyond the incident response window.

Quantum Supply Chains Go Strategic

With $2.013B in planned U.S. quantum incentives across nine companies, quantum is joining AI, cyber, semiconductors, and critical minerals as strategic infrastructure.

Featured Resource

Practical tools you can implement immediately.

AI Warranty Readiness

Turning AI Performance Claims into Buyer Confidence

Enterprise AI buyers are looking for more than demos and broad performance claims. They want measurable KPIs, independent assessment, clear use cases, defined remedies, and insurance support behind the promise.

This Practical Guidance piece explains how warranty-backed AI can help vendors reduce procurement friction, strengthen customer confidence, and support contract negotiations before deployment.

Use it to pressure-test whether an AI product has the right metrics, contract language, monitoring process, and insurance alignment to support a credible warranty solution.

Click here for the full guide.

Monthly Spotlight: QSE

Client success and risk maturity in action.

Quantum Secure Encryption Corp. (CSE: QSE) is helping organizations prepare for one of the most significant emerging cybersecurity challenges: the transition to a post-quantum world. Through its Quantum Preparedness Assessment platform, entropy-based security infrastructure, and quantum-resilient storage solutions, QSE works with enterprises and public-sector organizations to identify cryptographic vulnerabilities, assess exposure, and strengthen long-term data protection strategies.

As adoption of QPA V2 continues, QSE is moving quantum readiness from a theoretical risk conversation into practical implementation, giving security, compliance, and technology teams a clearer view of where legacy encryption may create exposure, which systems and data require prioritization, and how to build more resilient protection around sensitive information and critical infrastructure.

The cybersecurity market is entering one of the most significant technology transitions in decades. As quantum computing advances, governments, regulators and large enterprises are no longer treating post-quantum security as a future consideration. QSE is addressing this accelerating market need with a fully built, commercially available platform designed to help organizations move from awareness to action.

QSE's solutions enable customers to assess quantum-related exposure, prioritize remediation and deploy quantum-resilient protection without requiring a disruptive replacement of existing infrastructure.

Following a period of product development, platform integration, certification milestones and strategic partner expansion, QSE has entered a commercial scaling phase. The Company is generating revenue, currently serves 262 customer accounts, and is experiencing growing pipeline activity across enterprise, government and regulated-industry channels.

We are proud to support QSE as they continue building in one of the most important areas of emerging technology risk. Companies operating in post-quantum cybersecurity face a complex landscape across cyber liability, technology E&O, intellectual property exposure, regulatory developments, customer contracts, and evolving security expectations. Our role is to help innovative companies like QSE align their insurance and risk strategy with their growth, so they can continue protecting critical infrastructure and sensitive data in a rapidly changing security environment.

Industry Insights

Deep dives into high-impact risk topics.

Click Any Insight to Download the Full Article

When AI Becomes Systemic Cyber Risk

AI at Systemic Scale

AI-enabled cyber capability can turn one vulnerability into simultaneous, repeatable attacks across shared software, cloud, and vendor dependencies. Test cyber events, Technology E&O;, contractual liability, and aggregation risk together.

The Hidden Risk Layer Beneath the AI Boom

The Infrastructure Risk Layer

AI infrastructure risk is moving into specialized suppliers: cooling, packaging, materials, testing, power, and automation. Contract alignment, precision failure, cyber-physical loss, and single-point-of-failure exposure need review.

Quantum Risk: Cyber and D&O Exposures

Quantum as Board-Level Risk

Quantum risk can create delayed privacy, contractual, regulatory, and litigation consequences. Start with cryptographic inventory, vendor roadmaps, board reporting, and cyber/D&O; wording.

When Quantum Breaks the Chain

Post-Quantum Crypto Exposure

Crypto-exposed businesses should begin post-quantum planning now. Wallets, custody platforms, exchanges, smart contracts, and digital asset policies need a roadmap before quantum-related risk becomes commercially disruptive or difficult to insure.

NGen N3 Summit 2026

From Innovation to Industrial Execution

NGen framed advanced manufacturing around execution: industrial AI, AI agents, robotics, digital twins, advanced materials, defence, and industrialized homebuilding. Technology must be trusted, integrated, secured, maintained, insured, and scaled.

From Prototype to Production

Commercialization Has a Balance Sheet

Government funding can accelerate advanced manufacturing, but it does not transfer private commercialization risk. Review IP ownership, indemnities, product liability, Technology E&O, cyber/OT, vendor governance, and insurer questions before scale.

Closing Thoughts

May's themes point to a clear message: the next technology risk conversation is about evidence. Boards need evidence that post-quantum risk is owned and budgeted. Buyers need evidence that AI performance promises can be measured and remedied. Underwriters need evidence that contracts, vendors, cryptographic dependencies, and coverage have been reviewed before failure occurs.

Before your next renewal, financing round, customer contract, or vendor negotiation, pressure-test four areas first: where encryption or identity systems create long-tail exposure; where AI performance claims need independent support; where customers or funders are asking for stronger risk evidence; and where your insurance program may treat one connected loss as several separate coverage questions.

The companies that build this evidence early will be easier to diligence, easier to insure, and better positioned to scale when trust becomes a buying requirement.

If you'd like to continue receiving our monthly newsletters, please subscribe below.

Subscribe

Unsubscribe

> **"There's no free lunch: every unit of crypto-procrastination translates either into a unit of catastrophic risk or a unit of rushed migration risk."**
>
> – Michele Mosca, CEO, evolutionQ

Contact Us

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

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

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

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

AXIS / Technology