corix partners

Managing the Quantum Threat Horizon

A Management Perspective on a Technological Problem and an Early Roadmap for GRC Professionals

July 2026

A Management Perspective on a Technological Problem and an Early Roadmap for GRC Professionals

Through its processing power, the development of quantum computing could make almost all current encryption algorithms vulnerable

A look at the situation as we can understand it today:

- Where do we stand?
- What challenges, and what roadmap, for GRC professionals?

The Certainties

Technological

- Quantum computing is under development
- AI is accelerating research
- Use cases affecting current cryptographic methods are established
- Post-quantum cryptography standards and products have begun to emerge, making it possible to consider migrating to resistant products
- We are heading towards a ‘Q-Day’, when the first tangible case of compromise of current algorithms will come to light

Regulatory

The situation highlights three long-established families of good practice, reflected in all data-security regulations:

- Protecting sensitive data through encryption
- Keeping encryption methods at the state of the art as technology evolves
- Maintaining some form of monitoring of emerging threats that could affect sensitive data

The topic must find its place on the GRC agenda

The issue is being masked by the monumental background noise around AI

The Uncertainties

- No clearly established horizon for Q-Day, but the consensus is that it is relatively close and getting closer: 2030? 2035?
- No clearly established, structured threat profile, beyond the 'HNDL' type (« Harvest-Now-Decrypt-Later »); how processes using pre-quantum encryption could be affected is not tangibly clear
- The first threats are most likely to be linked to nation states or state-sponsored actors, given the expected technological complexity
- Intelligence appears to indicate that HNDL collection is indeed under way, but at what scale — and whom should we believe in the current geopolitical context?

How will AI have changed our environments and practices by Q-Day?

The Near-Certainties

- Mobilising executive committees and other leaders, who are fixated on AI, around a complex topic with poorly defined timelines and stakes will not be easy

- We are heading not only towards Q-Day but also towards a Y2K-style ‘panic’ movement; but beware of simplistic parallels: the PQC challenges are considerably more complex than those of Y2K

- It remains the role of GRC stakeholders to push — perhaps even champion — the topic

Revisiting the Y2K parallel

Y2K		PQC
A clear timeline horizon	→	No clearly established horizon
A simple, clear, bounded, widespread problem	→	No clarity on how threats would be executed
A problem common to almost all IT components	→	A problem concentrated in encryption modules, which therefore have to be identified
IT environments considerably simpler and less interconnected than today, generally managed in-house	→	Hyperconnected IT environments and complex business processes, generally dependent on many external third parties, and being reshaped by AI
↓		↓
Heavy, costly but simple, linear projects		Projects likely to be long, complex and cross-functional, testing deep knowledge of the IT environment and supplier-relationship maturity

How to act today?

1- Take the issue seriously now, without waiting for absolute certainty

- Raise the topic on the GRC agenda (if it is not already there)
- Treat it as a regulatory topic in its own right (it is)
- Put Governance first: Who will own it? At what level? Who will assess the enterprise's level of exposure?
- Start prioritising now, without waiting for the inevitable panic movement that will hijack all other priorities and resources
- With particular urgency for critical industries / critical infrastructure operators and all organisations that process or host large volumes of sensitive data (personal or otherwise), especially if those data have long lifecycles or may have been compromised (HNDL)
- Prepare the enterprise for a potentially long and complex compliance effort

How to act today?

2- An inventory of the enterprise's cryptographic tools/assets is essential

- To assess the level of exposure, feasibility and cost of achieving post-quantum compliance (and manage the end-of-life or unsupported platforms where this will not be possible)
- This is where to start

BUT

- Such an inventory is unlikely to already exist, so resources will have to be allocated for it to be built
- In a context where the necessary knowledge is likely to be dispersed across development, infrastructure and security teams and their suppliers
- And where the priorities of all those teams are curently entirely focused on AI and its challenges
- Hence the importance of a clear and robust governance, ownership and sponsorship framework established from the outset (see point 1)
- Avoiding an endless debate around prioritisation and the resources required to build the inventory is the clearest pitfall to avoid today; this is a clear leadership matter

How to act today?

3- Two relative ‘quick wins’ that can be validated now by internal governance bodies

- Mandate the use of resistant encryption tools for all new projects and projects currently under way (where possible)
- Include a section on suppliers’ post-quantum approach and maturity in your assessment questionnaires and periodic reassessments

Contact us

Corix Partners Limited

Registered in England and Wales (No. 06774109)
VAT Reg ID: GB970 2205 45

269 Farnborough Road
Farnborough, Hampshire,
GU14 7LY
United Kingdom

contact@corixpartners.com

www.corixpartners.com

@corixpartners