QUANTUM SECURITY INTELLIGENCE REPORT™

MOONA EDERVEEN-SCHNEIDER

Quantum Security Connection | Edition 1 | March 2026

www.quantumsecurityconnection.com

Published under Chatham House Rule. Quotes reproduced with permission

CONTENTS

ABOUT THIS REPORT

On 30 March 2026, we held the inaugural *Quantum Security Connection* in Central London, hosted by Helaba Bank. This quantum-transition table top exercise session brought together senior professionals from finance, law, defence, healthcare, government, critical national infrastructure, and FMCG: a hand-selected group, deliberately covering various sectors. Participants are united by a shared challenge: preparing their organisations for the post-quantum transition.

This report captures participant findings. It is not a technical primer on post-quantum cryptography. For that, we recommend the Practical Post-Quantum Transition Framework™, developed by Moona Ederveen-Schneider and referenced throughout the exercise. It is available free of charge to organisations as a practical roadmap. Designed for leaders and practitioners at all levels, it requires no deep cryptographic expertise, and is structured to be embedded in existing risk management and governance processes rather than treated as a separate technical programme.

This report offers insights into where senior leaders and practitioners currently stand: their awareness, blockers, and the actions they are preparing to take. It is published openly, in the belief that the insights will serve the wider community and those who generated them.

The exercise was designed and facilitated by Moona Ederveen-Schneider, Founder of Resilia Connect, and supported by Alice Bromage, Principal at of Quantum North, with additional table group moderation by cyber security leaders, Vikas Patel and Raminder Ruprai.

Several participants shared their reflections publicly following the session. We are grateful for their permission to include them here.

KEY FINDINGS

1. Quantum threat awareness exists, but it is thin and siloed. Post-quantum cryptography (PQC) is known to security teams in most organisations represented but has not meaningfully reached leadership, procurement, legal, or operations.
2. The dominant barrier is not technical but prioritisation. Five-year planning cycles, unquantified costs, and the absence of regulatory consequence make quantum readiness seemingly easy to defer.
3. Quantum is not yet being treated as an organisational problem. It is discussed in isolation, rarely overlaid on existing projects, refresh cycles, or risk frameworks.
4. Perhaps unsurprisingly, data estates are poorly mapped. Most organisations cannot fully articulate what sensitive data they hold, where it lives, how long it must be protected, or who is responsible for it.

5. The business case should be straightforward but must be framed in financial and regulatory terms to reach boards and chief executives.
6. Immediate, high-value actions are available to every organisation in the room and beyond, regardless of sector or budget. The blocker is initiation, not capability.

"This belongs on every board agenda. Now."

Participant — QSC Edition 1, Chrissy Hill, Chief Legal Officer

NEXT STEPS

FUTURE QSC EDITIONS AND BOARD BRIEFINGS

We are exploring how the Quantum Security Connection will continue with further editions of the tabletop exercise and the opportunity to expand into regular workshops or to cover specific topics and breach scenarios. The sessions can be held within organisations, sector-specific, or cross-sector to build the awareness and momentum that the post-quantum transition requires. Tailored Board briefings and advisory for how the Framework applies to your organisation are also available.

HOSTING AND SPONSORSHIP OPPORTUNITIES

We appreciate if you can help spread the word and if you would like to attend a future QSC edition, explore hosting or sponsorship, please get in touch with Moona Ederveen-Schneider via www.quantumsecurityconnection.com.

PEER SUPPORT

Vetted QSC participants also have the option to stay connected using the private LinkedIn group: Quantum Security Connection.

IN DEVELOPMENT

Moona Ederveen-Schneider is working on a companion paper to the transition framework, called Practical Quantum Mechanics, for those who wish to better understand the mechanics behind the threats we are facing, such as HNDL and TNFL (Harvest Now, Decrypt Later; Trust Now, Forge Later). The *Quantum Security Directory™* is also in development, to help practitioners navigate this space.

"It's not a dark art — but having deep specialists guide you through certainly helps."

Alice Bromage, Principal, Quantum North

EXERCISE OUTCOMES

The show-of-hands scores at the start and end of the session were instructive: the majority of the room rated PQC as low priority initially and almost everyone rated it as feeling highly unmanageable. By the close, priority and manageability scores had shifted noticeably, suggesting that structured discussion and a clear framework move the needle even in a single session.

FURTHER INFORMATION

- DHS Quantum Information
- Quantum Glossary
- ISMG Quantum Video Interview with Moona Ederveen-Schneider
  - https://www.databreachtoday.co.uk/practical-post-quantum-transition-start-now-heres-how-a-31393
- Security Insights Quantum Podcast Interview with Moona Ederveen-Schneider
  - https://podcasts.apple.com/gb/podcast/security-insights/id1514154540?i=1000761756149
- InfoSecurity Magazine Article: *Why Your Organization Should Start Quantum Preparedness Today (Even If Quantum Computers Are Years Away)* – by Moona Ederveen-Schneider
  - https://www.infosecurity-magazine.com/opinions/why-your-organization-should-start
- Sample *Enterprise Cyrptography Policy*, by Louise Davey
- Exercise Participant Feedback by Sector
  - Defence, Legal, Military

THE POWER OF COMMUNITY

Participants were drawn from finance, legal, military and defence, healthcare, critical national infrastructure, government, FMCG, and investment. The cross-sector composition was deliberate: quantum risk does not respect sector boundaries, and practitioners recognised a shared challenge from different angles. Facing a challenge of this scale, peer learning across sectors shortens the learning curve and organisations can avoid duplicating early mistakes, draw on frameworks already tested by others, and build the kind of cross-sector relationships that make coordinated response possible.

"Post-quantum readiness isn't a future problem. Or just a crypto problem."

Participant, QSC Edition 1

PARTICIPANT INSIGHTS

QUANTUM SECURITY POSTURE

Awareness of post-quantum risk exists across the sectors represented, but it is thin, unevenly distributed, and rarely backed by action. Security teams are broadly familiar with the threat. Leadership, procurement, legal, and operations functions are largely not. Where awareness has surfaced, it tends to be deprioritised quickly the moment it competes with operational demands.

The picture is compounded by a data problem that predates quantum entirely. Most organisations cannot fully map their data estate with confidence: what sensitive information they hold, where it resides, how long it must be protected, and who is responsible for it. Retention policies are inconsistent and frequently exceed what is defensible. This is not a quantum-specific failure, but it is the foundation on which quantum readiness must be built. The Practical Post-Quantum Transition Framework™ addresses this directly, beginning with data lifecycle management as the first structured step.

Cryptographic discovery presents a similar challenge. Tooling to identify and map cryptographic usage across an organisation is limited. Different teams manage different areas; cloud key management is often handled separately from on-premise systems. Data in transit, data at rest, authentication, and third-party dependencies are frequently bundled under a single label that obscures the reality: these are materially different systems with different risk profiles and different migration timelines.

> "Quantum-enabled threats are no longer theoretical. They are a present and accelerating risk that require coordinated, intelligent and forward-leaning responses."
>
> Bobbi Trehan-Young, Microsoft Architect & Engineer, BAE Systems for Military Aviation

QUANTUM SECURITY BLOCKERS

The dominant barrier is not technical. It is prioritisation, and the structure of how organisations plan. For most organisations represented, quantum readiness competes poorly against near-term operational demands. Five-year planning horizons place the 2035 NCSC deadline outside the window entirely. The unpredictability of Q-Day compounds this: unlike a regulatory deadline, it carries no fixed date, making it structurally similar to other ignored inflection points such as Y2K or the rapid rise of AI, theoretically understood and practically deferred.

A sharper observation emerged across multiple tables: quantum is still being treated as an isolated problem rather than something to be overlaid on existing

programmes of work. This framing is significant, because it is precisely wrong. Organisations are not being asked to run a separate quantum project. They are being asked to develop the awareness to recognise where quantum risk intersects with work already underway. That reframe had not yet landed widely in the room.

When it comes to migration, the blockers are concrete: identity services, operational technology, and embedded systems that cannot be updated easily; cloud providers operating on their own timelines; legacy systems with hard-coded cryptography; and the straightforward reality of financial outlay competing against a threat that remains, for many boards, theoretical. The board-level calculation described by one table was direct: is the risk of not doing it less than the fine? Until regulatory consequence becomes concrete, this will continue to favour deferral.

IMMEDIATE ACTIONS

The business case is available to every organisation in the room, and it does not require a quantum computer to materialise to deliver value. Regulatory consequence, insurance exposure, and financial liability are the levers that move boards. Abstract risk arguments do not. As one table put it plainly: the CEO listens when you say there will be a financial impact.

On immediate action, the room was practical. Education within technical teams, ensuring cryptographic considerations are raised earlier in development and infrastructure pipelines, was consistently identified as a step available now at low cost. Several tables made a strong case for applying quantum-secure standards to all new builds from this point forward rather than attempting to retrofit legacy systems later. This is not a quantum project. It is sound engineering practice that also builds quantum resilience.

On migration, the first steps are not technical either. The priority is data discovery: understanding what sensitive data the organisation holds, where it resides, and how long it must remain protected. Cryptographic discovery follows, mapping where encryption exists across systems, third parties, and infrastructure. Together, these activities form the foundation from which a credible, risk-based migration plan can be built. This is precisely the sequence set out in the Practical Post-Quantum Transition Framework™, available free of charge at moona.net. Quick wins lie in systems already due for refresh, greenfield projects, and newer platforms. Low-value data should be removed as its worth decreases. The estate that requires protection should be shrinking, not growing.

The legal dimension deserves particular attention. Privileged legal information with retention periods of ten years or more is already in scope for harvest-now-decrypt-later attacks. That is not a future risk. It is a current one.

REGULATORY ROUND-UP

Participants expressed a strong preference for regulation and guidance as a tool to demonstrate urgency. Therefore, below are a number of key regulations and government initiatives, that we reviewed in the session. This is not aiming to be a complete overview. A more detailed overview can be found in the Practical Post-Quantum Transition Framework™ and other sources online, given that the paper was written in 2025 and it is a fast-moving space.

Region	Body	Key Detail
United Kingdom	National Cyber Security Centre (NCSC)	Strategic planning complete by **2028**. Critical assets protected by **2031**. Full migration by **2035**.
United States	NIST / Department of Homeland Security (DHS)	RSA encryption deemed insecure by **2030**. Federal agencies: inventory and migrate by **2035**.
Germany	Federal Office for Information Security (BSI) — TR-02102	Annually updated cryptographic recommendations. Transition of most sensitive applications to quantum-resistant methods by **2030**.
India	National Cybersecurity Reference Framework	CII (Defence, Power, Telecom): full migration by 2029. Enterprise (Govt & Private Sector): full migration by 2031.
Australia	Australian Signals Directorate (ASD) — Information Security Manual (ISM)	Cease use of vulnerable asymmetric cryptography by 2030. Full transition to post-quantum algorithms by 2030.
Canada	Canadian Centre for Cyber Security (Cyber Centre) — ITSM.40.001	High-priority systems by 2031. Full migration of all federal IT systems by 2035.
South Korea	PQC Master Plan	Pilots 2025–28. Nationwide by 2035.
Singapore	Monetary Authority of Singapore (MAS)	Financial institutions: act now (Advisory TCRS/2024/01).