ISSUE 4

THIS WEEK IN QUANTUM SECURITY

June 5, 2026

By
Joel Van Dyk
Quantum Security Advisor and Strategist

This week, the conversation around quantum security continued to shift from theory to implementation. For years, organizations have asked whether quantum computers will eventually threaten today's cryptography. Increasingly, the question is becoming much more practical: what should we be doing now?

The strongest signals continue to come from the financial sector. Last week, the Reserve Bank of India announced a new committee focused on quantum technology in financial services, while regulators, industry groups, and infrastructure providers continued emphasizing preparation, inventory, and migration planning.

One word appeared repeatedly throughout the week: **adaptability.**

The challenge facing organizations is no longer simply choosing a post-quantum algorithm. The challenge is building systems capable of evolving as cryptography changes over time. That is why cryptographic agility, an area of increasing focus for the FS-ISAC Post Quantum Cryptography Working Group, continues to emerge as one of the most important concepts in cybersecurity.

The organizations making the most progress are not necessarily the ones predicting exactly when quantum computers will become a threat. They are the ones identifying where cryptography exists today and building plans to adapt when change becomes necessary.

This week also provided an opportunity to visit EdenBase here in London, where founder Eric Van der Kleij continues building one of the UK's most interesting communities focused on cybersecurity, AI, emerging technologies, and digital resilience. What stood out was not simply the technology being discussed, but the emphasis on bringing founders, investors, security professionals, and innovators into the same room.

As quantum security moves from theory to implementation, those conversations matter. The transition to quantum-safe infrastructure will not be solved by cryptographers alone. It will require collaboration across technology, finance, government, and industry — exactly the kind of ecosystem that organizations like EdenBase are helping to create.

THREE TRENDS WORTH WATCHING

1. **Financial Services Are Moving First**
   Banks, regulators, and financial infrastructure providers increasingly view post-quantum cryptography as a business resilience issue rather than a research project. The financial sector appears determined to avoid being caught unprepared.

2. **Cryptographic Agility Is Becoming Essential**
   The ability to change cryptographic systems without disrupting operations is becoming a strategic priority. Organizations are recognizing that migration will be an ongoing process, not a one-time event.

3. **Visibility Remains the Biggest Challenge**
   Many organizations still do not know where all of their cryptographic assets reside. Before migration can begin, discovery and inventory work must take place. In many cases, that remains the largest obstacle.

WHAT I'M READING

- **G7 Cyber Expert Group: Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector**
  https://www.gov.uk/government/publications/advancing-a-coordinated-roadmap-for-the-transition-to-post-quantum-cryptography-in-the-financial-sector
- **Circle's Post-Quantum Security Roadmap**
  http://docs.arc.network/arc/concepts/post-quantum-security
- **UK National Cyber Security Centre: Next Steps in Preparing for Post-Quantum Cryptography**
  https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography
- **European Commission: Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography**
  https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
- **EY: Is the Financial Sector Ready for the Transition Towards Post-Quantum Cryptography?**
  https://www.ey.com/en_nl/insights/financial-services/is-the-financial-sector-ready-for-the-transition-towards-post-quantum-cryptography
- **World Economic Forum: Quantum-Safe Migration**
  https://www.weforum.org

ONE NUMBER TO WATCH

2030

Across Europe and other major jurisdictions, 2030 is increasingly being discussed as a significant milestone in post-quantum readiness planning. The exact requirements vary by sector and regulator, but the direction is clear. Organizations that begin inventory and planning efforts today will have more options tomorrow.

CLOSING THOUGHT

The biggest story in quantum security right now is not quantum computing. It is preparation.
The algorithms are emerging. The standards are maturing. The guidance is becoming clearer.
The organizations that succeed will not be those that perfectly predict the future. They will be the ones that understand their environments, build flexibility into their infrastructure, and prepare before urgency arrives.