The Quantum Threat is already a Cyber Security Issue

Quantum computing is no longer a topic that cybersecurity leaders can afford to treat as a distant technological concern. The prospect of future quantum capabilities poses significant challenges to current cryptographic systems, making it essential for organizations to understand their exposure and begin preparing today.

This presentation examines the practical cybersecurity implications of the quantum threat, with a focus on cryptographic dependencies, cryptographic inventory, and crypto-agility. It explores why organizations need visibility into where and how cryptography is used across their infrastructure, applications, communications, and data, and how this visibility supports risk assessment and informed decision-making.

The session will highlight the role of the Chief Information Security Officer (CISO) in preparing for the post-quantum transition, translating emerging risks into actionable priorities, and establishing a roadmap for cryptographic resilience. Using email security as a practical case study, it will demonstrate how cryptographic dependencies can create real-world challenges and why organizations should assess their readiness before quantum-capable threats become a reality.

Key takeaway:
Participants will gain a practical understanding of how to identify cryptographic exposure, build an inventory of cryptographic assets and dependencies, improve crypto-agility, and define the immediate steps security leaders can take to prepare their organizations for the post-quantum era.

The message is clear: quantum readiness starts with understanding your cryptography—and the time to act is now.



Dimitri van Esch

Founder & CEO, Eoncore

Dimitri van Esch is the founder and CEO of Eoncore (Quantum Gateway Solutions B.V.), an Amsterdam-based company focused on practical quantum-safe security. He began programming at sixteen and has spent more than 30 years working across IT infrastructure, network security and software development. Today, he helps organizations understand their cryptographic exposure, establish a clear baseline and prepare a transition to post-quantum cryptography. His work is driven by a simple conviction: robust security and privacy should be the default, not a premium feature. This conviction led to Eon Phoenix, an open-source email client—currently in beta—that adds post-quantum encryption to existing mailboxes and is free for everyone to use. Dimitri is a member of the Crypto Agility working group of the Dutch Ministry of the Interior (BZK).

From 2018 to 2023, Dimitri was Quantum Lead and Solution Architect at ABN AMRO Group Innovation, where he launched and led the bank's Quantum Program. Its work included MDI-QKD with QuTech and TNO across combined free-space and fiber links; quantum algorithms for finance with QuSoft; and a business case for space-based QKD for ESA. He is the lead inventor of ABN AMRO's Orchestrated Quantum Key Distribution patent: a key-management protocol combining quantum and classical technologies. Dimitri also served on the NAQT sounding board that preceded Quantum Delta NL, and has been involved with the Quantum Software Consortium's industry council and the World Economic Forum's Quantum Computing network.

Dimitri began his career in the 1990s as a system administrator and internet-security consultant at XS4ALL. He went on to hold infrastructure, security and project-management roles at Telegraaf, Cendris (PostNL) and Dataman, as well as CTO and business-development positions at several startups. Since 2020, he has also been a Quantum Business Consultant at Quantum Amsterdam, where he organizes events and workshops and develops quantum games. A frequent speaker, he addresses quantum-safe migration for governments, financial institutions and critical-infrastructure organizations.