

Consulting

Post Quantum Readiness

- **From Mandates to
Action for Quantum-
Resilient Utilities**

[@ElizabethGreenConsulting](#)





Post Quantum Ready

From Mandates to Action for Quantum-Resilient Utilities

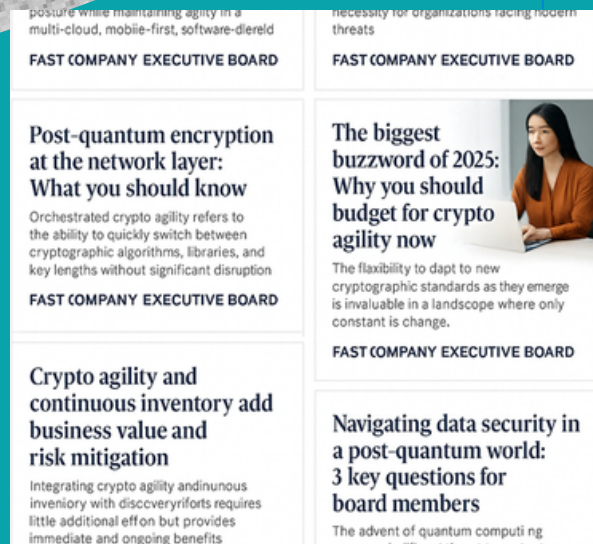
ELIZABETH GREEN

About Me

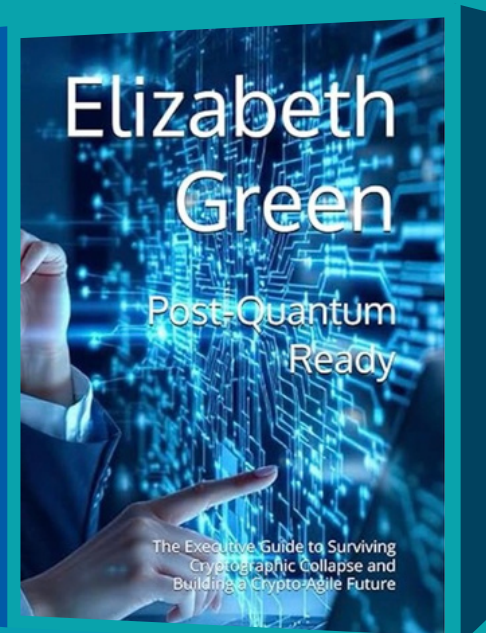
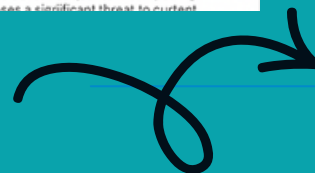
Cybersecurity executive (CISM), author of *Post-Quantum Ready: The Executive Guide to Surviving Cryptographic Collapse and Building a Crypto Agile Future*, and a frequent contributor to Fast Company.

I have held leadership roles at global firms including Accenture, IBM, Wipro, and QuSecure, and am a recognized voice on post-quantum security and crypto-agility, advising organizations on how to prepare their infrastructures for the coming quantum era.

[@ElizabethGreenConsulting](https://www.linkedin.com/company/elizabethgreenconsulting)



Visit me at:

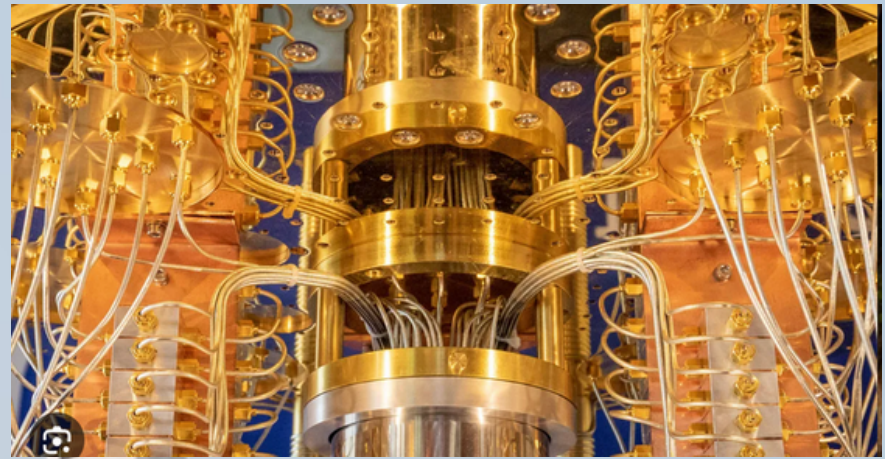


A NEW TYPE OF COMPUTING

Q U A N T U M



01010101010101010
10101010101010101
010



QUANTUM THREAT DATA

This infographic highlights data most at risk from quantum threats.



NATIONAL SECURITY

National security data is **critical** for protecting nations and allies.



FINANCIAL DATA

Financial data includes **banking transactions** and payment systems, which are essential for economic stability and trust.



HEALTHCARE DATA

Healthcare data encompasses **medical records** and genomic information, pivotal for patient care and research advancements.



INDUSTRIAL DATA

Industrial data involves **utilities and energy grids**, crucial for maintaining infrastructure and national security.



PERSONAL DATA

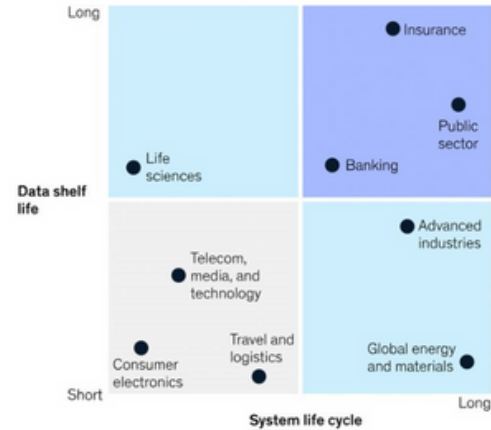
Personal and identity data includes **PII and credentials**, making it vulnerable to malicious attacks.

Quantum Risk Zone

McKinsey Reports Key Industries Most at Risk for Quantum-Powered Attacks

Risk of quantum-powered attack by industry

■ At risk before ~2025 ■ At risk between ~2025 and ~2030 ■ At risk after ~2030



McKinsey
& Company

CURRENT ATTACKS

Store-now-decrypt-later (SNDL)

Targeting sensitive data with long shelf life.



Financial Information

Money movement from a quantum attack on a U.S. financial institution could cost **\$2.0T**



Trade Secrets & Intellectual Property



Health Records

PENDING ATTACKS

Breaking communication sessions and controlling transaction sessions midstream.



Manufacturing, Infrastructure & Logistics



National Security

"A quantum attack could result in over \$3 trillion in damages to the US economy"

Quantum Alliance Initiative | 2021



WHY PQC MATTERS NOW



Utilities rely on encryption for every function (SCADA, telemetry, customer data).



NIST deprecates RSA & ECC by 2030 (SP 800-131A).



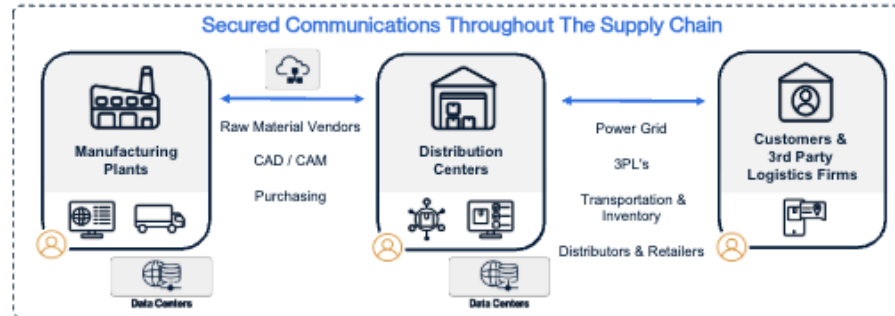
Quantum threat shortens the event horizon: 'Harvest Now, Decrypt Later'.



Quantum machines advancing faster than predicted.

Critical Infrastructure, Manufacturing, and Logistics Insights

Protect for the unforeseen threat



PUBLICLY OBSERVED

DHL, Federal Express, Alibaba, JSR Group and NEC are currently looking into protection from the quantum threat.

Quantum Computing Report | 2022

QUSECURE SME SPOTLIGHT

**Aaron
Wentzel**

Chief Technical Officer,
Translational Analytics & Statistics
Aaron has nearly 30 years of experience
working as a product and services leader.
Most recently Aaron was the Principal Cloud
/ Dev Ops Architect at Microsoft where he
led cloud architecture, developer operations,
and compliance for the Microsoft Web
Platform team.



Econometric Study - the Impact of a Quantum Attack on Critical Infrastructure

"Our study indicates the direct economic cost of this quantum-led electricity outage would be over \$8.6 trillion, with a disruptive impact extending over six fiscal quarters."

Forbes and The Hudson Institute

QuSecure Confidential and Proprietary © 2023 QuSecure, Inc.

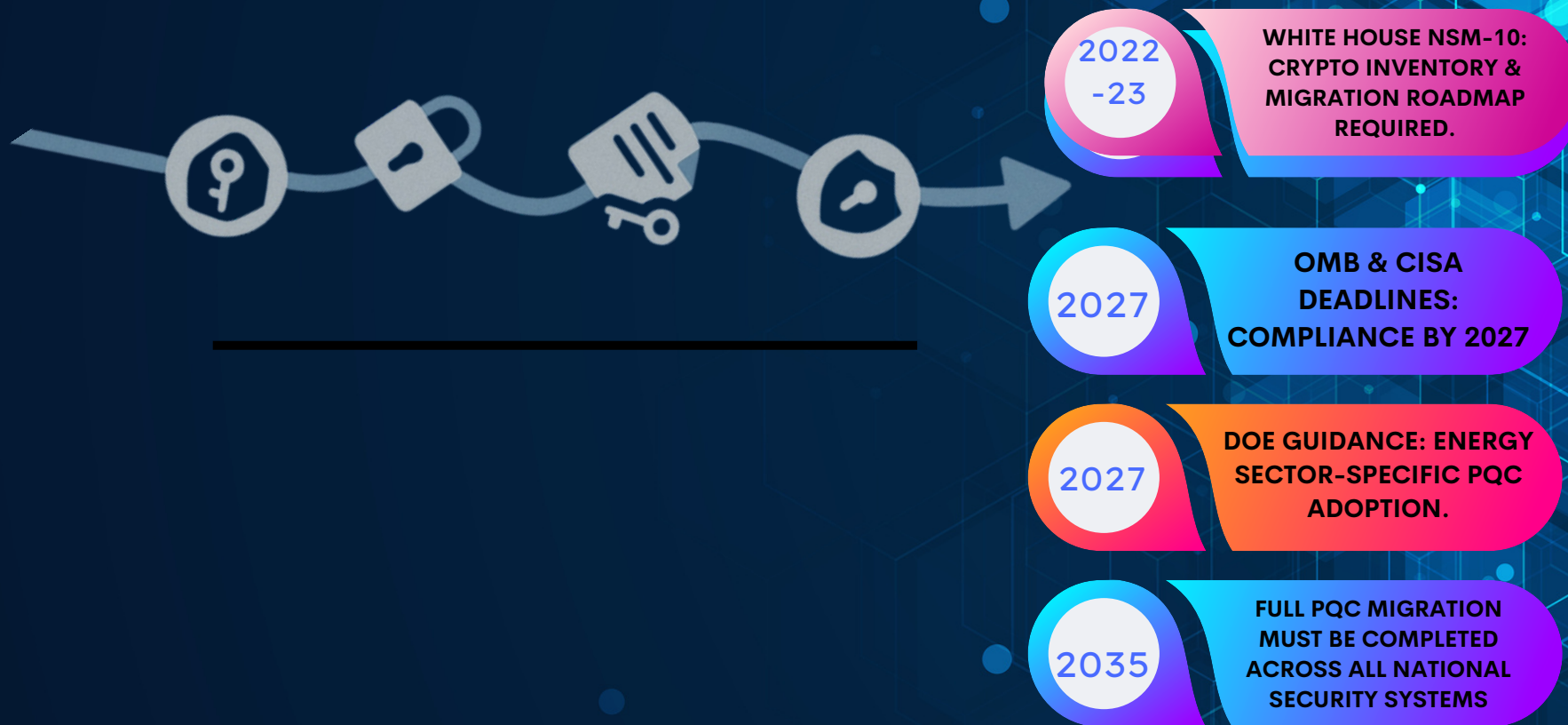
Countdown to PQC Transition - 2030

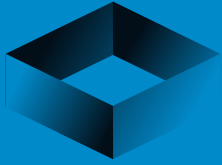


[@ElizabethGreenConsulting](https://www.elizabethgreenconsulting.com)

U.S. Standards & Mandates

AND INTRO TO CRYPTO AGILITY





GLOBAL STANDARDS & MANDATES

EU Cyber Resilience Act:
secure cryptography
mandated.



Germany BSI & UK NCSC
frameworks for PQC
migration



Japan: crypto-agile
energy grid strategies.



Canada: PQC pilots in
critical infrastructure.





CRYPTO AGILITY: A PRACTICAL SOLUTION



-  Swap cryptography without ripping out systems.
-  Avoids forklift OT/SCADA replacements.
-  Minimizes downtime & operational disruption.
-  Future-proofed with orchestrated crypto agility.





Benefits of Crypto Agility

- Risk reduction against quantum disruption
- Compliance with NIST, DOE, CISA, and global mandates
- Cost efficiency vs. wholesale rip-and-replace

Actionable Roadmaps and Results

Post-Quantum Management Checklist



- ☐ Form a transition team
- ☐ Inventory cryptographic assets
- ☐ Assess quantum risk
- ☐ Implement crypto agility
- ☐ Select PQC algorithms
- ☐ Govern cryptography
- ☐ Develop a transition plan

Post-Quantum Management Checklist

- ☐ Conduct CBOM inventory
- ☐ Identify quantum-vulnerable algorithms
- ☐ Prioritize long-lived data and assets
- ☐ Test PQC in network-layer systems
- ☐ Upgrade TLS, VPN, and certificates
- ☐ Establish crypto governance roles
- ☐ Report risk to CISO, CIO, and board
- ☐ Engage vendors on PQC readiness
- ☐ Monitor NIST, NSA, and global guidance

LEARN MORE NOW

Quantum disruption is within your
planning horizon today



Consulting

Thank
you ♥

WORKING TOGETHER TO KEEP OUR WORLD A LITTLE SAFER