

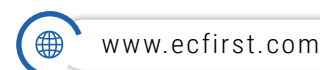
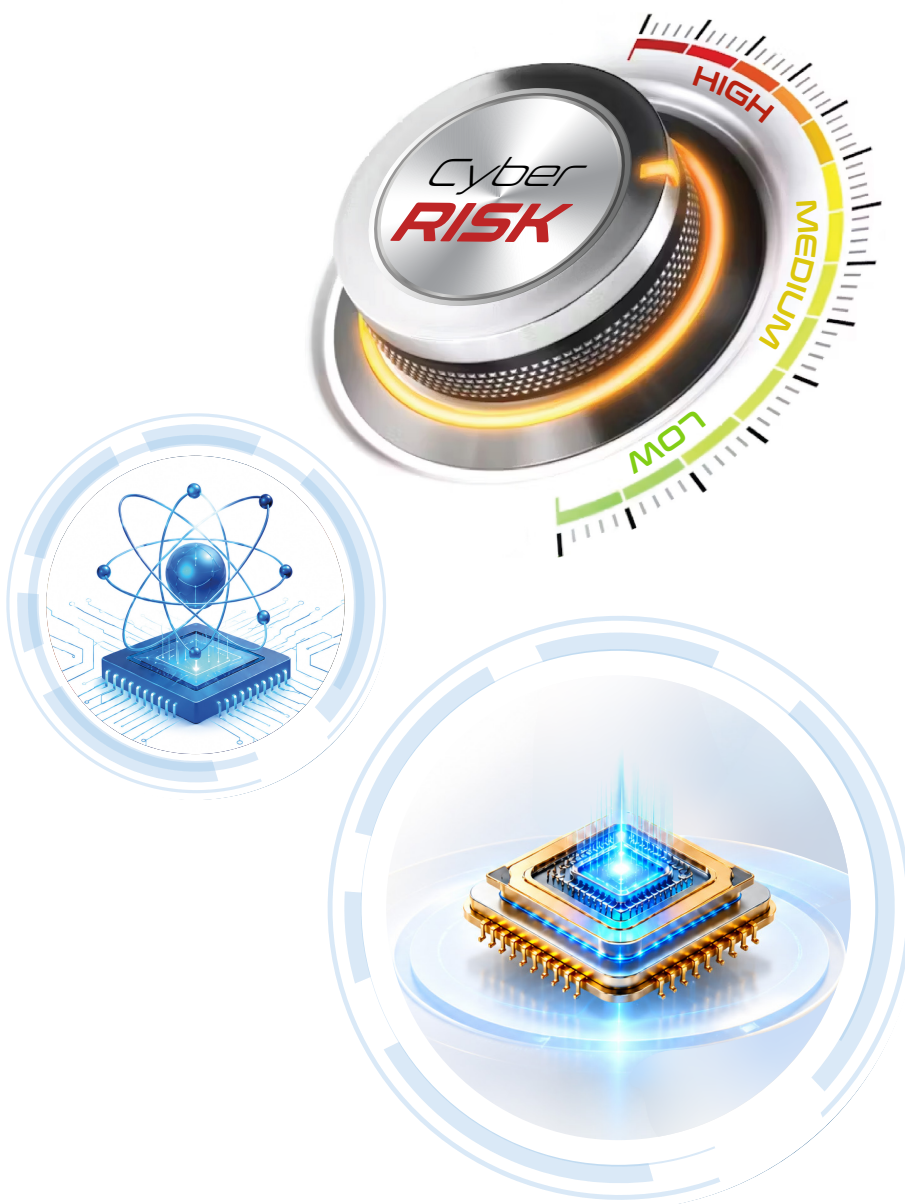
Quantum Cyber Risk

Program Catalog



Table of Contents

Quantum Cyber Risk Readiness	2
Quantum Cyber Risk Self Assessment	3
Quantum Cyber Risk Playbook	5



Quantum Cyber Risk Self Assessment



Cryptographic Risk Register

Prioritized quantum-related risks and exposures

PQC Migration Roadmap

Sequenced actions to improve quantum resilience



Executive Summary

Leadership-ready findings and recommendations



Governance & Ownership

Encryption & Cryptographic Inventory

Sensitive Data & Harvest-Now-Decrypt-Later Exposure

Infrastructure & Network Crypto-Agility

Technical Migration & Crypto-Agility

Vendors & Supply Chain

Awareness, Policy & Training

Quick Links

[Home](#)

[FAQ | Quantum Cyber Risk](#)

[References](#)

[Glossary](#)

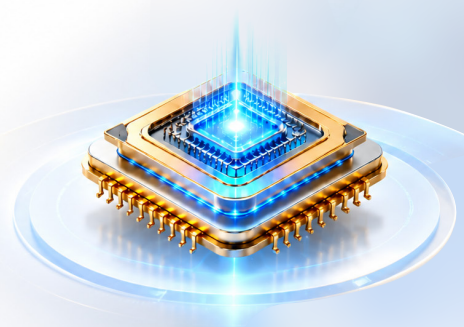
[AI-Powered Assistant Bailey](#)

Quantum Cyber Risk Playbook

[Infographics](#)

[Brief](#)

[Brochure](#)



Q-Day

The period when quantum computers can break standard encryption: a window, not a date

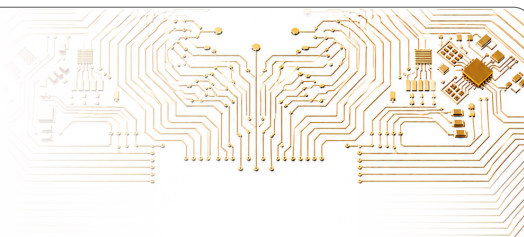
THE WALL STREET JOURNAL

Why Quantum Computing Is a Threat to Cybersecurity

The math behind standard encryption will be no match for quantum computers, forcing organizations to rethink cybersecurity.

Quantum Threat

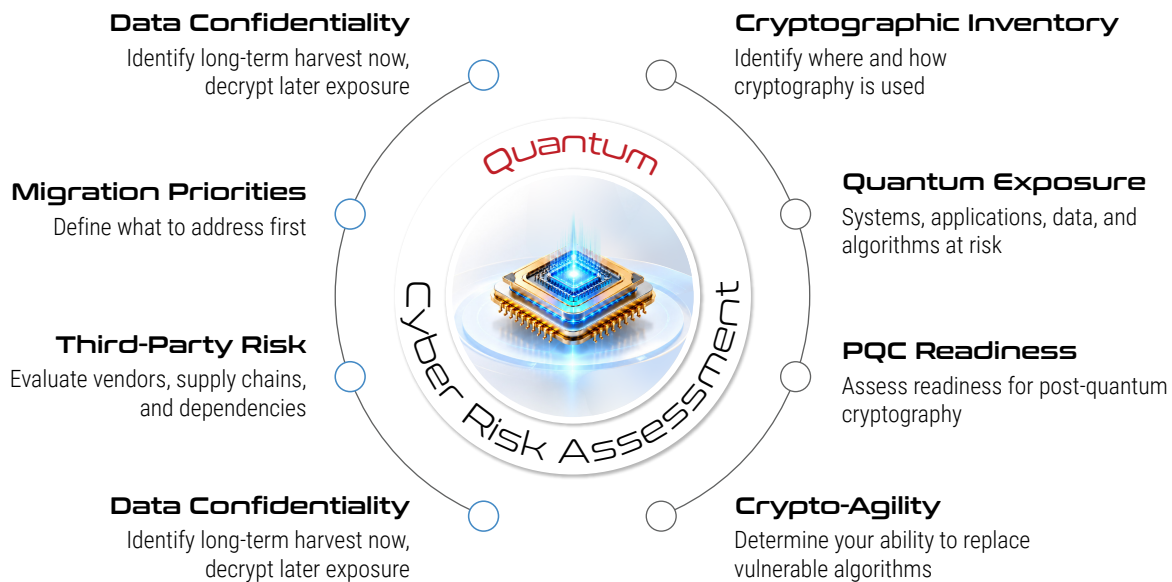
- Quantum computers solve certain math problems far faster than classical ones.
- Shor's algorithm can factor large numbers, breaking RSA, Diffie-Hellman, and ECC.
- Broken cryptography could enable fake digital signatures and undermine trust.



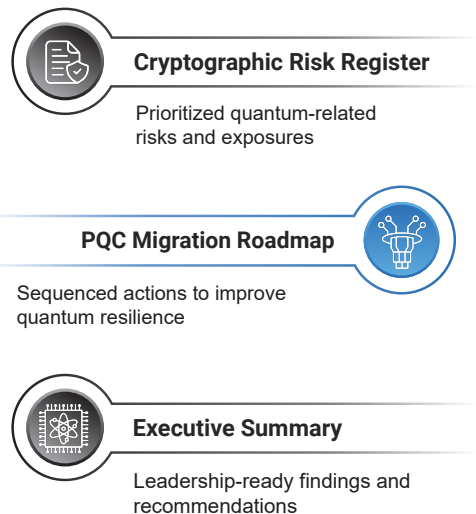
Is Your Encryption Ready for the Quantum Era?

Today's public-key cryptography protects your VPNs, TLS sessions, applications, and sensitive data. Quantum cyber risk assessment will eventually threaten these protections—and adversaries may already be harvesting encrypted data for future decryption.

Quantum Cyber Risk Readiness Assessment



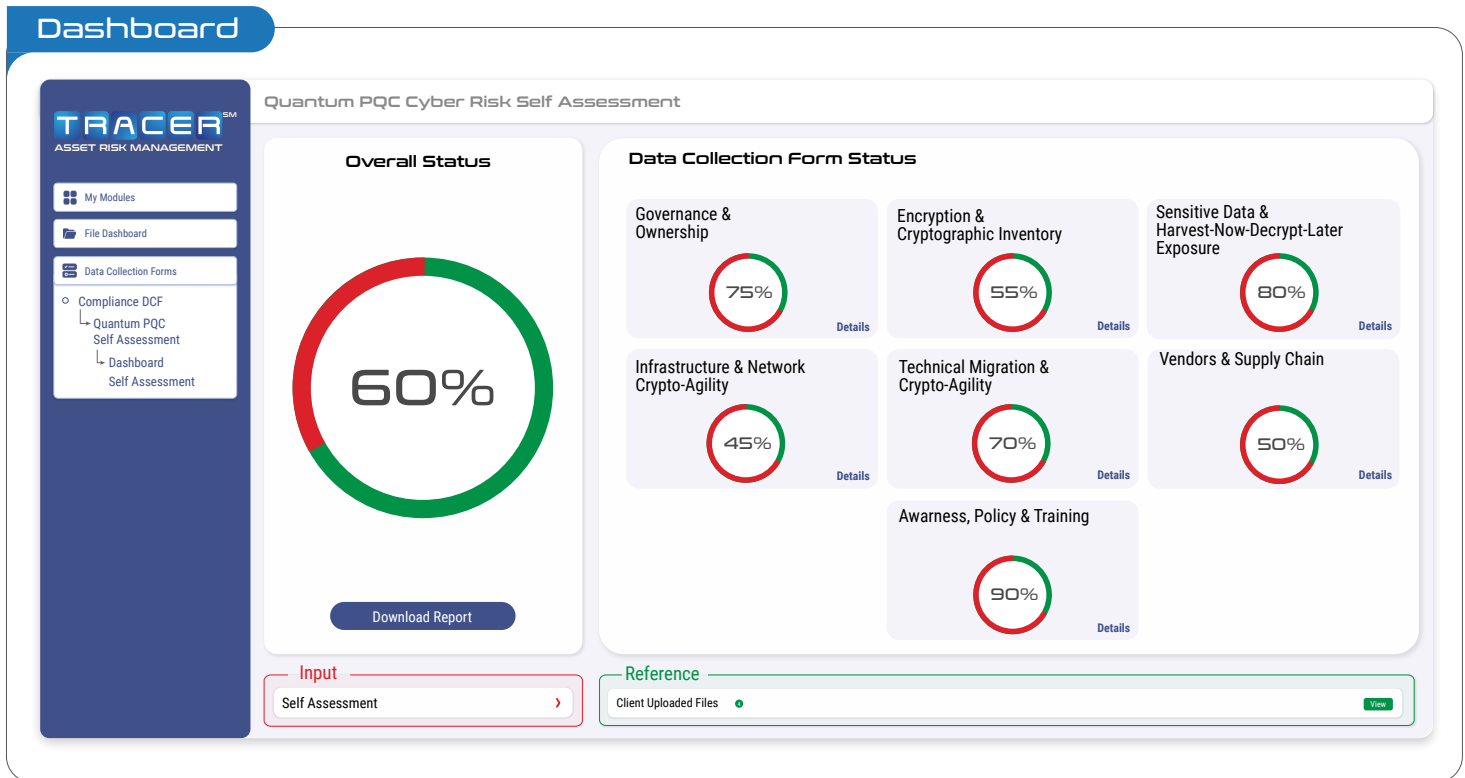
Quantum Cyber Risk Readiness Report



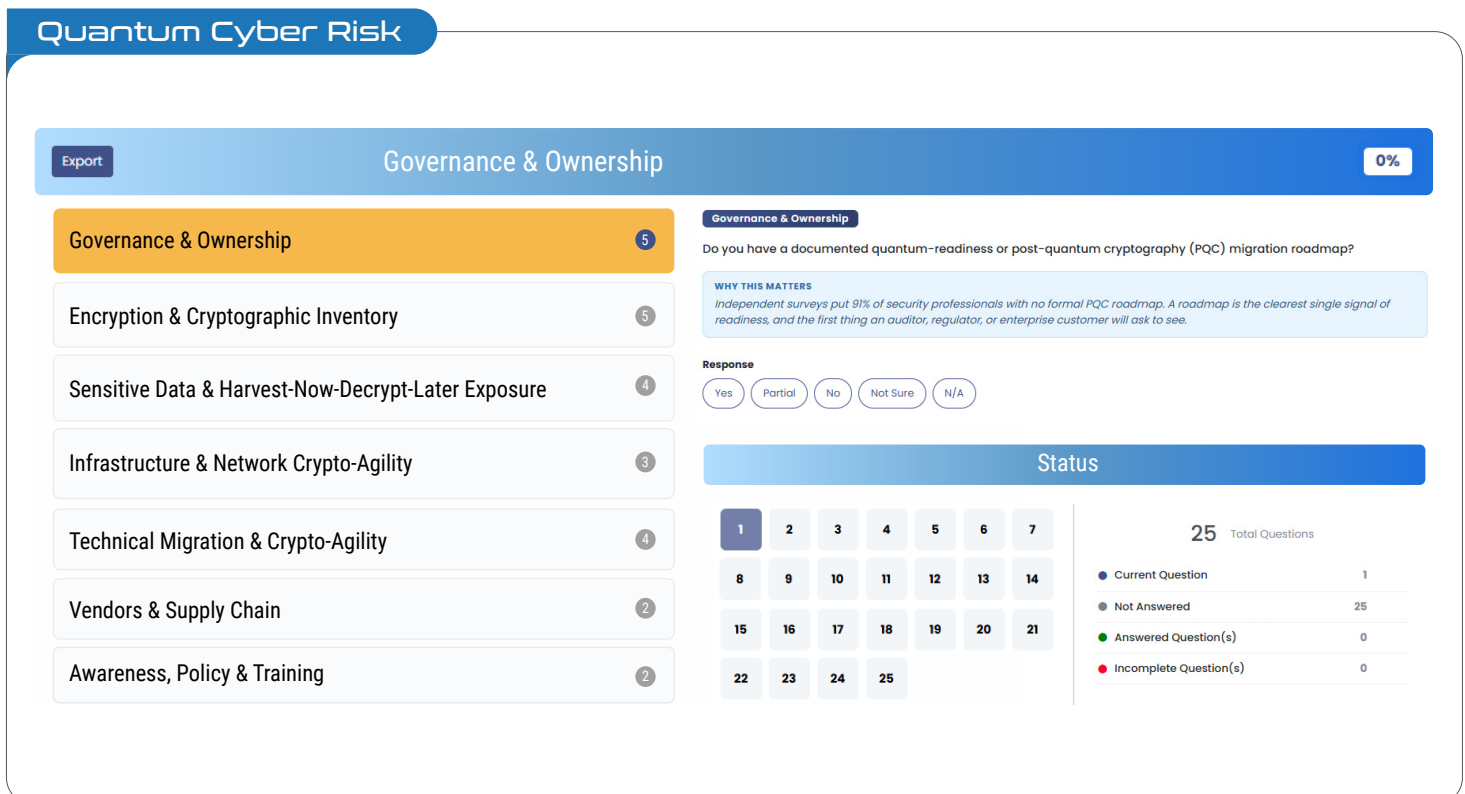
Why Quantum Cyber Risk Matters?

- ✓ Establish a defensible quantum-readiness baseline
- ✓ Uncover cryptographic risk hidden in legacy and third-party systems
- ✓ Protect data requiring confidentiality beyond today's encryption lifecycle
- ✓ Turn quantum cyber risk into a prioritized, actionable program
- ✓ Prepare before customers, regulators, or auditors ask

Dashboard



Quantum Cyber Risk



Quick Links

Home

FAQ | Quantum Cyber Risk

References

Glossary

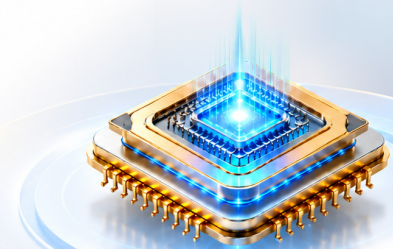
AI-Powered Assistant Bailey

Quantum Cyber Risk Playbook

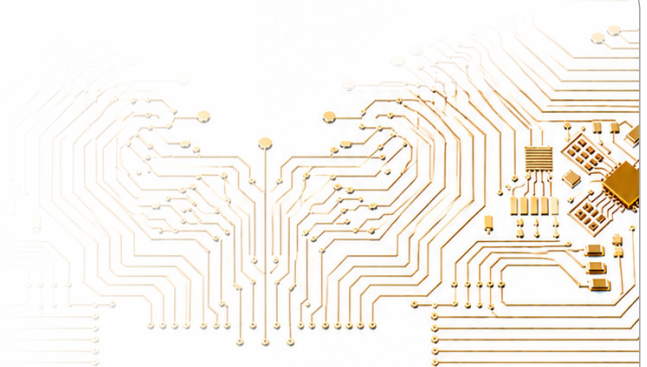
Infographics

Brief

Brochure



The period when quantum computers can break Standard encryption
a window, not a date



References



FAQ | Quantum Cyber Risk

Start Here: The 90-Second Version	Q1 What is encryption doing right now?	▼
Fundamentals	Q2 Why does public-key encryption break?	▼
"Q-Day" and the Timeline	Q3 Why can a quantum computer do that?	▼
Harvest-Now, Decrypt-Later (HNDL)	Q4 The actual risk today, in one sentence	▼
Post-Quantum Cryptography (PQC): The Fix		
Regulation and Compliance		
Assessing and Managing the Risk		



Peter.Harvey@ecfirst.com



www.ecfirst.com