Board Discussion Guide on Quantum Computing

Gregory Touhill, Director, CERT Division, Software Engineering Institute, Carnegie Mellon University
Larry Clinton, President and CEO, Internet Security Alliance

This tool presents an overview of anticipated impacts and applications of quantum technologies, and provides suggested cybersecurity-related questions for board members to discuss with management as the technology matures and transitions into the marketplace.

INTRODUCTION

Quantum computing presents both opportunity and existential risk. While its commercial applications remain nascent, its potential to break widely used cryptographic systems—including RSA and Elliptic-Curve Cryptography (ECC)—makes it one of the most significant emerging risks in cybersecurity governance. Quantum threats are not hypothetical; adversaries may already be "harvesting now, decrypting later," collecting encrypted data with the expectation of unlocking it once quantum capability matures.

Quantum computing research is advancing quickly; with many experts forecasting "Q-Day," that will likely arrive before the end of this decade. Q-Day refers to the day when quantum computers will be able to use multistate quantum bits or "qubits" to break the encryption algorithms at the heart of digital security technologies currently used to secure the internet and digital devices.

KEY TERMS

Post-Quantum Cryptography (PQC) and Post-Quantum Encryption (PQE) are closely related, often overlapping terms in the context of securing data against future quantum computer attacks. PQC refers to the creation of the mathematical algorithms, methods, and cryptographic techniques themselves (e.g. lattice-based or code-based algorithmic structures). PQE is a broader term that specifically emphasizes the application of these new quantum-resistant algorithms to encrypt data (i.e. the post-quantum resistant solution or technology.)

The National Institute for Standards and Technology (NIST) has published approved PQC standards and selected algorithms.[1] Boards should be aware that these select algorithms have been "proofed" to be post-quantum resilient, eliminating the need for most organizations to launch their own PQC creation programs. Organizations should move quickly to update the encryption of their data using PQE.

PREPARING FOR Q-DAY

The pertinent question for board members is not when will quantum computing arrive; it is rather will your organization be ready?

When Q-Day arrives, critical data—including intellectual property, banking information, personally identifiable information, personal health information, and other "secrets"—will be susceptible to decryption by quantum computers, making all current information vulnerable to exposure. The degree of quantum readiness will also likely become an audit/compliance issue.

Many experts are advising that boards should be planning for the coming quantum transition now. However, current research suggests that is not generally the case. A 2026 Bain & Company analysis found that 90 percent of companies are unprepared for quantum security threats, even though many executives expect such threats to materialize within the next five years.[2]

A 2025 Information Systems Audit and Control Association (ISACA) study found that only 4 percent of organizations have a defined quantum strategy despite growing concern about the durability of existing encryption.[3] Similarly, a survey conducted by the Trusted Computing Group found that 91 percent of businesses lack a roadmap to protect against quantum threats.[4]

Boards cannot afford to ignore quantum risk until the technology is fully realized. Transitioning a reasonably sophisticated IT system to accommodate quantum impacts could take years and substantial expense. It may cost several million dollars just to do the review and discovery of needed alterations and twice that much for planning and testing. Doing this transition retrospectively may cost many times these amounts.

Delayed preparation for Q-Day substantially increase costs, but could also make adequate and timely transition impractical due to the lack of qualified technical staff. Multiple studies indicate that quantum risk is widely recognized, yet workforce planning for post-quantum transition has barely begun.[5,6] In practice, post-quantum cryptography has moved beyond a research challenge to an execution challenge—and execution depends on people.[7]

Should a cryptographically relevant quantum computer arrive within the next few years, most organizations (including critical infrastructure providers), would be unable to transition in time—not for lack of awareness, but because the workforce needed to do so does not yet exist at scale.

THE QUANTUM OPPORTUNITY

There are several major points of consensus regarding the advent of quantum computing:

- Q-Day will occur in the foreseeable future, likely by or in the 2030s.[8]
- Q-Day will compromise almost all the current encryption/security systems. Implementing plans for quantum transition may require substantial time and expense—delayed planning and implementation will substantially increase these costs.
- There is an extreme shortage of qualified and trained people to properly implement quantum translon. Once Q-Day comes, these shortages will be magnified—there will likely not be enough for everyone who needs to do the transition.
- Organizations that have adequately prepared for the quantum transition prior to Q-Day will likely have a substantial—possibly unassailable—market advantage over competitors.

High-performing boards will prioritize preparing their organization to migrate to post-quantum cryptography at the top of their agendas to ensure their organizations will be ready to thrive in a post-quantum marketplace.

The following provides practical guidance for directors to operationalize the handbook principles in addressing quantum risk.

Principle 1: Treat Cybersecurity as a Strategic Risk

- Integrate quantum risk into the enterprise risk register and strategic technology roadmap.
- Ensure the board understands the potential disruption to customer trust, intellectual property, and national security obligations.

Principle 2: Monitor Legal and Disclosure Implications

- Oversee alignment with regulatory requirements such as NIST's post-quantum cryptography (PQC) standards and anticipated disclosure expectations.
- Ensure the organization discloses material risks related to quantum vulnerabilities in financial filings if applicable.

Principle 3: Establish Board Oversight Structures and Access to Expertise

- Confirm that at least one director or advisor has expertise in emerging technologies, including quantum.
- Assign oversight of quantum risk to an innovation, risk, or technology committee.

Principle 4: Adopt an Enterprise Framework for Managing Cyber-Risk

- Require quantification of the potential impact of quantum-enabled decryption on sensitive data.
- Assess the cost-benefit trade-offs of early adoption of PQC versus delayed transition.

Principle 5: Guide Cybersecurity Risk Measurement and Reporting

- Ensure management has assessed risk exposure to the organization arising from quantum computing technologies.
- Assess and receive updates on management's progress in migrating to PQC.

Principle 6: Encourage Systemic Resilience and Collaboration

- Encourage management to participate in cross-industry collaboration on PQC adoption.
- Require evidence of alignment with government and industry standards bodies (e.g., National Institute of Standards and Technology [NIST] and ETSI).

Questions the Board Can Ask to Assess Their Quantum Understanding

- Do we thoroughly understand the implications of this potentially market disrupting technology and its impacts on our business and its strategy?
- Does our board have the right literacy to address quantum technology issues? What is this quantum literacy, and is it sufficient to meet our needs?
- Do we need to add a board member with deeper expertise on this topic to our board or bring in outside consultants?
- Do we have adequate and diverse sources of technical expertise to present the board with sufficient knowledge to make informed decisions on this topic?
- Do we have the right people in place on our executive team to lead the incorporation of quantum technology to support our strategy? Is our CEO capable of successfully overseeing such a project and integrating it with our strategy?
- Do we understand the risks and opportunities to our business and how quantum technology impacts our business strategy and ultimately its long-term growth and viability?
- Are we able to effectively interpret and assess management and third-party presentations on quantum technologies, as well as their answers to our questions?

Questions the Board Can Ask Management to Assess Quantum Readiness

- How prepared are we to thrive in a quantum-enabled marketplace?
- What is our risk exposure if all our data can be decrypted by quantum computers? How much will it cost in time and resources to implement PQC?
- What decisions do we need to make to remain competitive in a quantum-enabled marketplace?
- How will the introduction of quantum technologies support our existing strategy or force a change in strategy? How can we use quantum technology to improve our business?
- How will our risk posture be affected by the introduction of quantum technologies?
- What are our competitors doing in the quantum technology space?

- Who are the leaders in quantum technology? Who is delivering the best results? How do you know?
- Who has the best quantum technology adoption roadmap?
- Do we have the right talent to be successful?
- What effect will the introduction of practical quantum technologies into the marketplace have on our business? What is the impact on our business if a quantum computer can decrypt all our data?
- What means of modeling and simulation are there to assess our current strategy's effectiveness in a post-quantum world?

FURTHER READING

- National Security Agency (NSA) Post-Quantum Cybersecurity Resources
  https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

ENDNOTES

1. National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography," Computer Security Resource Center, www.nist.gov, effective December 15, 2025, https://csrc.nist.gov/projects/post-quantum-cryptography.
2. Nicole Kobie, "90% of Companies Are Woefully Unprepared for Quantum Security Threats—Analysts Say They Need to Get a Move On," ITPro, January 22, 2026. https://www.itpro.com/security/90-percent-of-companies-are-woefully-unprepared-for-quantum-security-threats-analysts-say-they-need-to-get-a-move-on.
3. ISACA, "Quantum Computing's Rapid Rise Is a Risk to Cybersecurity and Business Stability," Press release, April 28, 2025. https://www.isaca.org/about-us/newsroom/press-releases/2025/quantum-computings-rapid-rise-is-a-risk-to-cybersecurity-and-business-stability.
4. Trusted Computing Group, "91% of Businesses Do Not Have a Roadmap in Place to Protect Against Quantum Threats, Finds New Industry Survey," December 2, 2025. https://trustedcomputinggroup.org/91-of-businesses-do-not-have-a-roadmap-in-place-to-protect-against-quantum-threats-finds-new-industry-survey/
5. Kobie, 2026.
6. ISACA, 2025.
7. ISC2, "2025 ISC2 Cybersecurity Workforce Study," Cybersecurity Certifications and Continuing Education, December 4, 2025. https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study
8. Tran Duc Le and Phuc Hao Do and Truong Duy Dinh and Van Dai Pham, "Are Enterprises Ready for Quantum-Safe Cybersecurity," arXiv, (2025): https://doi.org/10.48550/arXiv.2509.01731