Quantum Readiness Roadmap: What Technology Leaders Need to Know about the Quantum Threat

Georgianna Shea and Jordan Bass

Executive Summary

Quantum computers pose a grave threat to the encryption methods that protect our digital world. Once quantum technology fully matures, these powerful machines could render traditional encryption ineffective, enabling criminals or state adversaries to expose sensitive personal, corporate, and government data, undermining trust in digital systems. This threat demands immediate action. While it remains unclear exactly when quantum computers will break today's encryption, taking proactive steps now can significantly reduce future disruption and cost.

The federal government has mandated that all federal systems transition to new, quantum-resistant encryption standards, known as post-quantum cryptography (PQC), by 2035. Regulatory bodies and industry standards will likely soon follow suit, requiring numerous organizations to upgrade to quantum-resistant algorithms. The sooner these organizations prepare, the less disruptive and expensive the transition will be. In fact, with early preparation, the transition can give organizations a proactive edge in managing this quantum threat.

This paper offers a six-step plan to help chief information officers and other technology leaders in the private sector navigate the shift to quantum-resistant encryption. Organizations should:

1. Designate a leader to spearhead the effort

2. Inventory all encryption systems

3. Prioritize which systems to address based on potential risks

4. Understand available mitigation strategies

5. Develop a realistic transition plan

6. Regularly monitor and adjust the plan as needed

By taking action now, organizations can safeguard their data and navigate the transition to a quantum future with minimal disruption and cost.

When Will Quantum Computers Break Current Encryption?

With the ability to calculate solutions faster, quantum computers could herald significant scientific breakthroughs. This same speed, however, will enable quantum computers to compromise encryption and jeopardize the security of all data, including medical records, financial transactions, confidential communications, and government and trade secrets. Any system relying on data confidentiality, integrity, or availability will be at risk. Experts disagree, however, about when existing quantum computers will reach the status of so-called "cryptographically relevant quantum computers" (CRQCs), able to break today's encryption.[1] Much of this disagreement stems from evolving estimates of how much power CRQCs will need and a myriad of nonstandard metrics used to measure technological maturity.

Quantum computers harness the properties of quantum mechanics to create "quantum bits," or qubits. Qubits behave differently than traditional bits, including by acting as a group that can share information and act collectively. By using

1. Dr. Michele Mosca and Dr. Marco Piano, "Quantum Threat Timeline Report 2022," *Global Risk Institute*, December 2023. (https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report); Dr. Michele Mosca and Dr. Marco Piano, "2021 Quantum Threat Timeline Report," *Global Risk Institute*, January 2022. (https://globalriskinstitute.org/publication/2021-quantum-threat-timeline-report-global-risk-institute-global-risk-institute); Dr. Michele Mosca and Dr. Marco Piano, "Quantum Threat Timeline Report 2020," *Global Risk Initiative*, January 2021. (https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2020)

entangled qubits, quantum computers can employ special algorithms to calculate more accurately[2] and can find the correct answer to certain types of problems more quickly and efficiently.[3] Instead of assessing each solution individually as traditional computers do, quantum computers statistically predict the correct process, allowing them to take shortcuts.[4]

Companies and research organizations are pursuing different technological approaches to create quantum computers. Quantum technology company PsiQuantum, for example, is developing a photonics-based quantum computer that uses the quantum state of photons and light to create qubits.[5] Meanwhile, Microsoft,[6] IBM,[7] and Google[8] are trying to develop physical qubits by creating trapped ions, superconducting qubits, or semiconductor quantum dots. It is too early to say which method will ultimately become standard practice.

Today, while capable of basic computations using qubits, most quantum computers remain severely limited in power and overall capability. Some companies, including IBM and Amazon,[9] are beginning to create commercially relevant quantum computers that can run quantum algorithms that complete specific tasks faster or better than traditional computers. While these companies offer cloud-based quantum computing services, these computers are not powerful enough to be considered CRQCs.

Power is difficult to measure in quantum computing because the industry has not agreed on a standard of measurement. The number of qubits is often touted as a key metric, but hybrid approaches that combine classical and quantum computing can use a smaller number of qubits to outperform a pure quantum machine.

Physical qubits, the fundamental hardware components, are sensitive and prone to mistakes due to interference from their surroundings. This makes them unreliable, as they do not always perform at peak capacity. A more accurate measure of a quantum computer's capability is its ability to generate logical qubits. Logical qubits, which are error-corrected and constructed from multiple physical qubits, offer significantly improved reliability and stability. The advancement of quantum computing technology hinges on developing sufficient logical qubits to perform meaningful and error-free computations rather than merely increasing the raw number of physical qubits.

2. Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, and San Vo, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *National Institute of Standards and Technology*, April 2010. (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf)

3. Author interview with William Clark, June 28, 2024.

4. Ajay Narayanan, "Quantum Superposition and What That Means to Quantum Computation," *Becoming Human: Artificial Intelligence Magazine*, October 23, 2019. (https://becominghuman.ai/quantum-superposition-and-what-that-means-to-quantum-computation-3fbb5a711b9a)

5. "Big Technology Reveal: PsiQuantum's Previously Secret Q1 Photonic Quantum Computer With GlobalFoundries," *PsiQuantum*, 2021. (https://www.psiquantum.com/news-import/big-technology-reveal-psiquantums-previously-secret-q1-photonic-quantum-computer-with-globalfoundries)

6. "Azure Quantum," *Microsoft,* accessed August 14, 2024. (https://quantum.microsoft.com)

7. "Quantum," IBM, accessed August 14, 2024. (https://www.ibm.com/quantum)

8. "Explore Quantum AI," *Google,* accessed August 14, 2024. (https://quantumai.google)

9. "Quantum Technologies at AWS," *Amazon Web Services/Amazon*, accessed August 14, 2024. (https://aws.amazon.com/products/quantum)

Quantum Readiness Roadmap: What Technology Leaders Need to Know about the Quantum Threat

Beyond Qubit Count: Metrics to Measure a Quantum Computer's Capability

Quantum Volume, a metric developed by IBM, is an efficiency rating that considers the number of qubits, their error rate, and how efficiently they work together.[10]

The Mirror Circuit Test, developed at Sandia National Laboratory, measures quantum efficiency by comparing a quantum computer's ability to perform a set of operations with its ability to perform those same operations in reverse.[11]

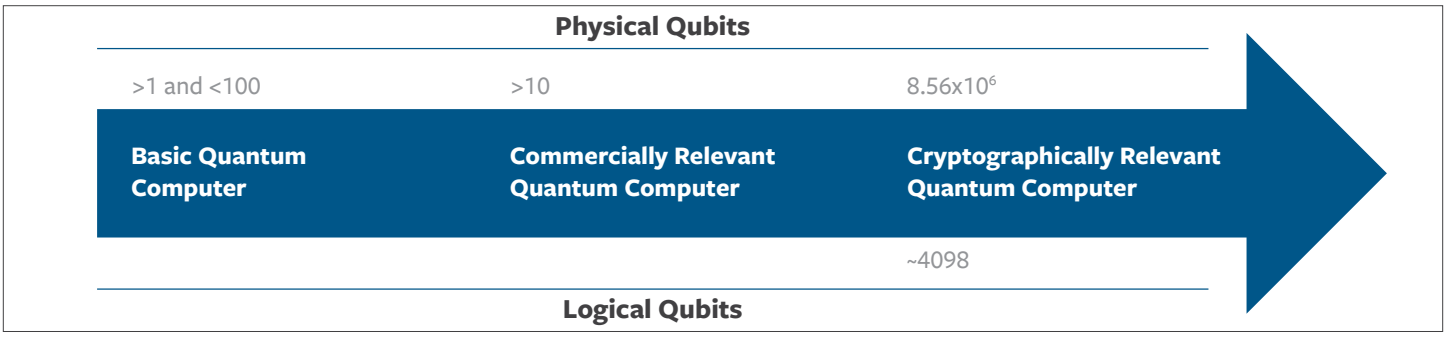
Gate Count defines the number and type of operations a quantum computer can perform. The number and complexity of quantum gates used in a particular quantum algorithm directly influence a quantum computer's processing power and capabilities. As researchers develop methods for using more numerous and sophisticated quantum gates, the processing power of these computers increases.[12]

Coherence Time measures how long a qubit can remain in a useful state before its environment disrupts it.[13]

Gate Fidelity reflects the accuracy of quantum gate operations.[14]

Readout Fidelity measures the accuracy of reading out the final state of a qubit after a computation.[15]

Focusing on the number of logical qubits rather than the raw number of qubits provides a more precise representation of progress toward practical and scalable quantum computing. However, the number of logical qubits needed for a CRQC is still debated. Estimates range around 4,000, but technological advancements could significantly lower this number.[16]



Moreover, there is also no consensus on how many physical qubits would likely be necessary to create 4,000 logical qubits. Some sources estimate that it would require 8,560,000 physical qubits to create 4,098 logical qubits, while IBM estimates that as few as 100,000 physical qubits are necessary.[17]

Companies such as Infleqtion are leading the charge toward a CRQC by developing qubit technology and error-correction techniques. This progress is fueled by advances in supporting technologies such as microlasers and qubit stabilization techniques. Infleqtion is targeting a 40,000 physical qubit machine by 2028.[18]

10. "Updating how we measure quantum quality and speed," *IBM*, accessed August 14, 2024. (https://www.ibm.com/quantum/blog/quantum-metric-layer-fidelity)

11. Sandia National Laboratories, Press Release, "Measuring a quantum computer's power just got faster and more accurate," December 20, 2021. (https://newsreleases.sandia.gov/quantum_benchmarking)

12. Omar Ghoniem, Hatem Elsayed, Hassan Soubra, "Quantum Gate Count Analysis," *Inspire HEP*, November 21, 2023. (https://inspirehep.net/literature/2759796)

13. IonQ Staff, "Quantum Computing 101: Introduction, Evaluation, and Applications," *IonQ*, January 18, 2024. (https://ionq.com/resources/quantum-computing-101-introduction-evaluation-applications)

14. Ibid.

15. Alice Heather Burrell, "High Fidelity Readout of Trapped Ion Qubits," *Exeter College, Oxford,* 2010. (https://www2.physics.ox.ac.uk/sites/default/files/Burrell_Thesis.pdf)

16. Mark Horowitz and Emily Grumbling, *Quantum Computing: Progress and Prospects* (National Academies Press, 2019). (https://nap.nationalacademies.org/catalog/25196/quantum-computing-progress-and-prospects)

17. Ibid.

18. Infleqtion, Press Release, "Infleqtion Unveils 5-year Quantum Computing Roadmap, Advancing Plans to Commercialize Quantum at Scale," February 8, 2024. (https://www.infleqtion.com/news/infleqtion-unveils-5-year-quantum-computing-roadmap-advancing-plans-to-commercialize-quantum-at-scale)

Quantum Readiness Roadmap: What Technology Leaders Need to Know about the Quantum Threat

Researchers at the California Institute of Technology, meanwhile, have demonstrated a method for trapping and manipulating over 6,100 qubits using a specialized "tweezer array" made of lasers that can keep qubits stable and functional for extended periods.[19] The Caltech group suggests that building a powerful quantum computer with thousands of qubits might be achievable by demonstrating long coherence times and high-fidelity control.

What Government Efforts Are Underway to Promote Quantum-Safe Encryption?

In 2018, Congress passed the National Quantum Initiative Act (NQI Act) on a bipartisan basis. The legislation aimed to "ensure the continued leadership of the United States in quantum information science and its technology applications" for a period of five years. This legislation's major accomplishment was to assign responsibility for the success and advancement of quantum technologies to various federal agencies, including the National Institute of Standards and Technology (NIST) and the National Science Foundation.[20]

The NQI Act has led to a substantial increase in quantum information science (QIS) research and development funding at the Department of Energy, National Science Foundation, and NIST. Since fiscal year (FY) 2019, the QIS research and development budget has almost doubled, reaching $1.031 billion in FY 2022. The requested budget for FY 2024 remains strong at $968 million. This funding is allocated across several areas: quantum sensing and metrology to enhance sensors using quantum mechanics; quantum computing to develop quantum computers and related software; quantum networking to create communication networks using entangled quantum states; QIS for advancing fundamental science to improve understanding in other scientific disciplines; and quantum technology to deploy quantum technologies, support technology development, and mitigate risks, such as post-quantum cryptography.[21]

The NQI Act emphasizes workforce development and collaboration between government, industry, and academia. NIST leads these efforts, conducting QIS research and partnering with the Quantum Economic Development Consortium, an industry-led organization focused on advancing the quantum information science and technology sector in the United States, to accelerate the growth of the U.S. quantum industry.

The statute, however, expired in September 2023. Follow-on legislation, the National Quantum Initiative Reauthorization Act (H.R. 6213), cleared the House Committee on Science, Space, and Technology in November 2023.[22] If passed into law, the bill would provide over $100 million annually toward quantum technology advancements, employee re-training, and domestic manufacturing capabilities.[23]

The 2022 CHIPS and Science Act also supports the development and implementation of quantum technologies on a national scale, and the legislation designated quantum technology as a key focus area.[24] Under the act, Congress appropriated hundreds of millions of dollars for research into quantum data science and required the Department of Energy[25] to accelerate the development of quantum network infrastructure.

---

19. Hannah J. Manetsch, Gyohei Nomura, Elie Bataille, Kon h. Leung, Xudong Lv, and Manuel Endres, "A tweezer array with 6100 highly coherent atomic qubits," *California Institute of Technology*, March 19, 2024. (https://arxiv.org/pdf/2403.12021); Matt Swayne, "Making It Look Tweezy: Caltech Researchers Use Optical Tweezer Arrays To Trap Over 6,100 Neutral Atoms," *The Quantum Insider*, March 20, 2024. (https://thequantuminsider.com/2024/03/20/making-it-look-tweezy-caltech-researchers-use-optical-tweezer-arrays-to-trap-over-6100-neutral-atoms)

20. National Quantum Initiative Act, Pub. L. 115-368, 132 Stat. 5092, codified as amended at 15 U.S.C. §8801. (https://www.congress.gov/115/plaws/publ368/PLAW-115publ368.pdf)

21. U.S. National Science and Technology Council, Subcommittee on Quantum Information Science, Committee on Science, "National Quantum Initiative Supplement to the President's FY 2024 Budget," December 2023. (https://www.quantum.gov/wp-content/uploads/2023/12/NQI-Annual-Report-FY2024.pdf)

22. National Quantum Initiative Reauthorization Act, H.R. 6213, 118th Congress (2023). (https://www.congress.gov/bill/118th-congress/house-bill/6213/all-actions)

23. Alexandra Kelley, "House Science chairman looks to pass quantum bill," *NextGov/FCW*, March 8, 2024. (https://www.nextgov.com/emerging-tech/2024/03/house-science-chairman-looks-pass-quantum-bill/394811)

24. CHIPS and Science Act, Pub. L. 117-167, 136 Stat. 1576. (https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf)

25. U.S. National Science and Technology Council, Subcommittee on Quantum Information Science, Committee on Science, "National Quantum Initiative Supplement to the President's FY 2024 Budget," December 2023. (https://www.quantum.gov/wp-content/uploads/2023/12/NQI-Annual-Report-FY2024.pdf)

Quantum Readiness Roadmap: What Technology Leaders Need to Know about the Quantum Threat

While Congress has primarily focused on advancing U.S. leadership in this critical technology, the Biden administration is actively working to address the potential negative impacts and challenges that may arise from quantum breakthroughs. In 2022, the White House issued a national security memorandum detailing requirements for federal agencies to mitigate risks to vulnerable systems.[26] The memorandum outlines a roadmap for federal systems to transition to PQC by 2035. (See Appendix B.)

The national security memorandum also requires the Office of Management and Budget (OMB) to work with the Cybersecurity and Infrastructure Security Agency, NIST, the Office of the National Cyber Director, and the National Security Agency (NSA) to "establish requirements for inventorying all currently deployed cryptographic systems."[27] While OMB's guidance on transitioning to quantum-resistant systems is directed at federal agencies, its criteria for determining systems and assets that organizations should prioritize are broadly applicable.[28] OMB notes that agencies should have an inventory of high-impact information systems, high-value assets, and data likely to remain mission-sensitive after 2035.

While OMB's guidance focused on civilian systems, the NSA has issued guidance on preparations that owners, operators, and vendors of national security systems (NSS) should take.[29] Although narrowly focused on NSS requirements, the document's recommendations are broadly applicable and offer detailed technical advice.

For its part, CISA has partnered with the NSA and NIST to put out a short fact sheet to help private industry understand the impact of quantum and to "encourage the early planning for migration to post-quantum cryptographic standards by developing a Quantum-Readiness Roadmap."[30] The fact sheet notes, "A successful post-quantum cryptography migration will take time to plan and conduct." As a first step, CISA encourages organizations to create an inventory that identifies quantum-vulnerable technology involving critical data so that organizations can conduct risk assessments and prioritize migration to PQC. The fact sheet then provides additional recommendations about making that inventory and considering vendors and supply chains.

To help federal agencies and other organizations implement guidance from OMB and other agencies, IBM has created a robust but simple method for upgrading cryptographic systems to post-quantum encryption. The company calls it a Cryptography Bill of Materials, or CBOM.31 The methodology focuses on identifying all cryptography in use and the value and criticality of related data, developing a prioritized remediation plan, and upgrading to quantum-safe cryptography.

Meanwhile, in the federal space, technical work on PQC is housed within NIST.[32] Two years ago, NIST announced the four winners of a multi-year competition to identify new algorithms that can withstand attempted decryption by quantum computers.[33] Last summer, NIST issued draft standards for three of these algorithms, namely Module-Lattice-Based Key-

26. The White House, Press Release, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," May 4, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems)

27. Ibid.

28. Letter from Director Shalanda D. Young, Executive Office of the President, Office of Management and Budget, November 18, 2022. (https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf)

29. National Security Agency, "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ," April 2024. (https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF)

30. Cybersecurity and Infrastructure Security Agency, National Security Agency, and National Institute of Standards and Technology, "Quantum-Readiness: Migration to Post-Quantum Cryptography," August 17, 2023. (https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf)

31. Alessandro Curioni and Michael Osborne, "IBM's Cryptography Bill of Materials to speed up quantum-safe assessment," *IBM*, December 8, 2022. (https://research.ibm.com/blog/cryptographic-bill-of-materials); IBM's CBOM tool is available for free on GitHub. This software is an extension of their Quantum Safe Explorer services. "IMB/CBOM," *Github*, accessed August 14, 2024. (https://github.com/IBM/CBOM)

32. National Institute of Science and Technology, Press Release, "NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers," August 24, 2023. (https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers)

33. National Institute of Science and Technology, Press Release, "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," July 5, 2022. (https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms)

Encapsulation Mechanism, or ML-KEM, formally known as CRYSTALS-KYBER;[34] Module-Lattice-Based Digital Signature, or ML-DSA, formally known as CRYSTALS-Dilithium;[35] and Stateless Hash-Based Digital Signature, or SLH-DSA, formally known as SPHINCS+.[36] In August 2024, NIST released the completed quantum-resistant cryptography standards.[37]

Why Take Action Now?

Acting now to transition to a quantum-resistant architecture is not merely about mitigating future risks. It is also about seizing strategic advantages, safeguarding critical data, and positioning organizations for long-term success.

A well-planned transition to quantum-resistant architecture will minimize disruption and cost. Organizations that integrate quantum-safe architectures early can phase in changes gradually, testing systems and training staff incrementally. This approach reduces the risk of sudden, costly overhauls and avoids the financial strain of emergency fixes for organizations unprepared for the time when quantum computing becomes a reality.

Early adopters of quantum-safe practices may gain a competitive edge, positioning themselves as leaders in cybersecurity. For companies in the technology and security space, this reputation can enhance customer trust while attracting new customers and partners who prioritize data security. A tech company that markets itself as quantum-ready can differentiate itself from competitors, appealing to clients seeking robust, future-proof data protection.

A timely transition to quantum-resistant architecture can also be a strategic investment. Companies incorporating quantum-safe technology into their innovation roadmaps can leverage it to develop new products and services, creating value and staying ahead in a competitive market.

For all companies, staying ahead of regulatory requirements is another critical reason for early adoption. Regulatory bodies and industry standards are moving toward mandating quantum-resistant algorithms. Organizations that act now can avoid a scramble to comply with new regulations.

Finally, implementing quantum-resistant solutions remediates a current threat: attacks deploying a Store-Now-Decrypt-Later strategy.[38] Malicious actors are already stockpiling encrypted data they have acquired illicitly, intending to decrypt it once CRQCs become available. Encrypting data with quantum-resistant algorithms ensures that data pilfered today will remain secure against future quantum decryption attempts.

What Can Companies Do Now to Prepare for the Future?

Despite the uncertainty surrounding exactly when quantum computers will be capable of breaking current forms of encryption, the threat is real. Once a CRQC is developed, anything and everything that has ever been encrypted will be readable as plain text. No one's historical data will be safe. Taking proactive steps now can prevent disaster down the road.

Organizations should develop a quantum readiness roadmap to address future challenges and minimize quantum security risks posed by the impending arrival of CRQCs. Every organization will have different needs and means, but all can benefit from having a plan.

---

34. National Institute of Science and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," NIST FIPS 203, August 2023. (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf)

35. National Institute of Science and Technology, "Module-Lattice-Based Digital Signature Standard," NIST FIPS 204, August 2023. (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.ipd.pdf)

36. National Institute of Science and Technology, "Stateless Hash-Based Digital Signature Standard," NIST FIPS 205, August 2023. (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.ipd.pdf)

37. National Institute of Science and Technology, Press Release, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," August 13, 2024. (https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards)

38. David Joseph, Raphael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Oliver Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, and Royal Hansen, "Transitioning organizations to post-quantum cryptography," *Nature 605, 237-423*, May 2022. (https://doi.org/10.1038/s41586-022-04623-2)

Quantum Readiness Roadmap: What Technology Leaders Need to Know about the Quantum Threat

The following section outlines the major steps involved in creating a quantum readiness plan. A detailed list of the steps and sub-steps is provided in Appendix A: Readiness Roadmap.

Step 1: Designate a Quantum Champion

Organizations need a point person, or "quantum champion," to spearhead efforts to understand the impact of this new technology. This person's primary role should be to assess potential vulnerabilities in the organization's cryptographic systems, collaborate with IT and security teams to develop a mitigation plan, and educate stakeholders about the implications of quantum computing. Together, these steps will help ensure the organization is ready to leverage the potential of quantum computing while mitigating the risks to its security and sensitive information.

This champion should be keenly aware of NIST's ongoing efforts to develop PQC standards and should stay informed about industry trends. While becoming a full-fledged quantum expert is unnecessary, fostering a basic understanding of vulnerabilities to CRQCs is crucial. This awareness allows an organization to develop targeted strategies to mitigate these risks and take a proactive stance toward the quantum future.

Step 2: Inventory All Instances of Encryption Usage

Before developing a mitigation and transition plan, organizations must first inventory all assets using encryption, including vendor-supplied (third-party) products. The inventory should identify encryption type, key length, and specific use. To aid in developing an inventory, organizations can leverage OMB guidance for federal agencies, NSA guidance for national security system operators, and CISA guidance for critical infrastructure owners. IBM's cryptography bill of materials may also prove useful.

Step 3: Assess Risk and Prioritize Systems

Once organizations identify all cryptographic systems, they should prioritize them for mitigation efforts, using a combined risk assessment and timeline analysis. This analysis should consider the potential financial, reputational, and operational consequences of a successful attack on each system. It should also factor in the effects of potential operational delays and complexities on critical systems transitioning to a quantum-safe alternative.

Identify the Gap

If organizations delay in implementing PQC until CRQCs arrive, adversaries will have more time to collect ever-increasing stores of encrypted data for eventual decryption. Organizations should therefore prioritize reducing the available attack surface. When encrypted data was safe, there was little risk in storing it perpetually. But with Store-Now-Decrypt-Later, the more data an organization stores and the longer the data is stored, the greater the risk. Organizations must ask themselves: Do we need to store this data? And if so, for how long? At what point does the risk outweigh the benefit of storing it? For data that must be stored, organizations should consider implementing additional security measures to decrease the possibility of that data being stolen and decrypted later.[39]

Identify Compatibility of Dependencies

Adopting PQC requires a tailored approach, as PQC algorithms may not seamlessly integrate with existing systems or vendor solutions. Organizations must anticipate potential compatibility issues and plan for updates or replacements in line with vendor timelines.

39. Amara Graps, "Quantum Cryptographic Threat Timeline," *Inside Quantum Technology News*, May 2022. (https://www.insidequantumtechnology.com/news-archive/quantum-cryptographic-threat-timeline)

PQC algorithms exhibit distinct performance characteristics compared to current cryptographic solutions, potentially affecting processing speed and resource allocation. This necessitates adjustments to infrastructure and resource management. Furthermore, PQC uses different data formats for encryption and decryption, requiring system modifications to ensure smooth operations. Key sizes and management practices also differ, demanding changes in key generation, storage, and rotation strategies.

Integrating PQC into existing systems often involves significant modifications for compatibility and functionality. This can include network configuration changes, code updates, or even hardware upgrades. Like the Y2K challenge, PQC exposes underlying assumptions about cryptographic protocols within applications, such as key sizes, signature sizes, and data formats. These implicit dependencies must be identified and addressed, potentially requiring extensive code rewrites across applications and libraries.[40]

For example, the network devices called middleboxes, which help with security and traffic management, may have trouble handling the bigger data packets during the so-called "TLS handshake" when using PQC-enabled browsers and servers. The TLS handshake is a process where a browser and a server establish a secure connection, exchanging keys and agreeing on encryption methods to protect the data they send.

Although PQC follows internet communication standards, or RFCs, some middlebox manufacturers designed their devices assuming that TLS handshakes would always fit within a single packet size. This mismatch highlights the need for a thorough approach to adopting PQC. It is important to consider the new algorithm and how it might affect system resources, compatibility, and the existing infrastructure.[41]

The impact of PQC extends beyond individual applications. It affects communication protocols, network infrastructure, and hardware, which may need adjustments or upgrades to handle larger keys and different data formats. Disruptions can also occur between organizations, necessitating workarounds or complete overhauls for systems requiring interoperability between PQC-enabled and non-PQC systems. The "Y2K-like" complexity of PQC underscores the critical need for proactive planning and a comprehensive implementation strategy.[42]

Step 4: Understand Mitigation Options

Once they have a prioritized inventory of cryptographical systems and a clear understanding of potential risks, organizations can embark on cost-effective mitigation planning. This planning should consider the federal goal to transition all federal systems to new quantum-resistant encryption standards by 2035.

A crucial factor in this planning is the equipment procurement refresh rate. For instance, some systems might be nearing a planned upgrade anyway. Purchasing a quantum-safe alternative now may be more cost-effective than buying something out of date before the end of the normal product lifecycle. Conversely, a staged migration or alternative mitigation strategies may be preferable for other systems. Organizations can choose the most cost-effective solutions by leveraging their equipment procurement cycles.

Beyond upgrading encryption to new PQC standards (which are not yet available), organizations can take several approaches to protecting prioritized systems and data.

Information-Theoretic Security
Organizations could implement technologies that guarantee security regardless of an attacker's computational power.

40. David Joseph, Raphael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Oliver Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, and Royal Hansen, "Transitioning organizations to post-quantum cryptography," *Nature 605, 237-423*, May 2022. (https://doi.org/10.1038/s41586-022-04623-2)

41. Email from Phil Venables to author, June 30, 2024.

42. Ibid.

This approach offers the strongest defense against potential quantum-based attacks, but it might not be feasible for all applications due to possible limitations in performance or compatibility.

Example: Cyber Reliant, a company specializing in data security, uses an Information Theoretic Security-like approach to ensure data security and thwart the quantum threat by fragmenting data, encrypting each fragment, encrypting the keys, and then distributing all encrypted fragments among various platforms inside and outside the organization.[43] The user stores the encrypted fragments on multiple platforms, such as mobile devices, outsourced cloud storage, and internal servers. The varied platforms add layers of complexity, requiring more significant resources and skill from the hacker to penetrate all platforms to retrieve all fragments. If a quorum of fragments is not obtainable, the data remains secure.[44]

Tokenization: Stealth for Data Security — Nothing to Steal, Nothing to Compromise

Pseudonymization, also known as tokenization, offers another way to provide defense. Even if powerful quantum computers manage to break encryption, advanced tokenization substitutes sensitive data with unique, randomly selected values with no inherent meaning. This ensures that stolen data remain useless even in the hands of an adversary with a CRQC.

Privacy platforms offering tokenization empower data owners, controllers, and service providers with data sovereignty capabilities, allowing stakeholders to precisely segment and control data access across multiple platforms, solutions, and geophysical locations. This not only enhances security but also ensures compliance with privacy regulations. Moreover, a client-defined custom token architecture enables clients to own their unique tokenization scheme and tailor it to their specific needs. This level of control further secures against data theft and mitigates opportunities for extortion in ransomware attacks.[45]

Crypto Agility

Crypto-agile technology offers a smooth transition path. Organizations can keep using their current encryption for now and, when PQC standards are finalized, simply update the core mechanisms within the crypto-agile system. But crypto-agility goes beyond a single update. These systems are designed for continuous adaptation. They can seamlessly switch to a hybrid mode in which existing algorithms and new PQC standards work together.

This "bridge" ensures ongoing security while organizations learn the ropes of PQC. Even better, crypto-agile systems are built for swift updates. As new threats emerge, whether quantum or traditional and cryptanalysis advances, the system can be readily updated with the latest and most secure algorithms or parameters. This future-proof approach guarantees that organizations can maintain robust encryption as the world of cryptography evolves. Software-defined networks are an example of such technology.[46]

Post-Quantum Cryptography Transition

Following NIST's lead, organizations can develop a well-defined plan for transitioning systems to new PQC standards once they become available. This approach ensures the organization leverages the latest recommended cryptography advancements and will likely stay ahead of potential security vulnerabilities in the quantum era.

43. "Cyber Reliant," *Cyber Reliant*, accessed August 14, 2024. (https://www.cyberreliant.com)

44. Dr. Georgianna Shea and Annie Fixler, "Protecting and Security Data from the Quantum Threat," *Foundation for Defense of Democracies*, December 2022. (https://www.fdd.org/analysis/2022/12/16/protecting-and-securing-data-from-the-quantum-threat)

45. "Advanced Data Security and Tokenization Solutions," *Rixon*, accessed August 14, 2024. (https://rixontechnology.com); Kevin Townsend, "Beating Ransomware With Advanced Backup and Data Defense Technologies," *Security Week*, June 6, 2022. (https://www.securityweek.com/beating-ransomware-advanced-backup-and-data-defense-technologies); Kevin Townsend, "Solving the Right to be Forgotten Problem," *Security Week*, November 18, 2021. (https://www.securityweek.com/solving-right-be-forgotten-problem)

46. "American Binary: Enduring Digital Security," *American Binary*, accessed August 14, 2024. (https://www.ambit.inc)

Step 5: Develop a Transition Plan

First, organizations and their leaders should evaluate the budget and resources for the transition to CRQC-safe architecture. Then, they must select an appropriate strategy based on their risk assessment and mitigation options. Next, the quantum champion will need to secure executive support to allocate funding and personnel for the transition. The champion will then need to create a realistic and achievable timeline for implementation. Finally, the organization will need to carefully consider system compatibility, dependencies, integration requirements, and operational sustainment.

Once an organization has established its overall strategy and allocated the necessary resources, the next step is to develop a detailed implementation plan. This plan should outline how to effectively execute the strategy, considering the specific requirements of each system, such as compatibility requirements, dependencies, and integration needs. To ensure a smooth transition, organizations should consider running pilot programs. These pilot programs, ideally conducted with lower-risk systems, allow for testing different mitigation approaches and identifying unforeseen challenges.

The implementation roadmap should be continuously updated as new information emerges or system configurations change. This flexibility will ensure the plan adapts to inevitable changes and leverages any new knowledge gained during the mitigation process.

By using this multi-step approach, organizations can strategically address the challenge of quantum computing threats. Prioritizing based on risk, leveraging existing equipment lifecycles, testing with pilot programs, and maintaining a flexible plan all contribute to a cost-effective and efficient transition to a quantum-resistant future.

Step 6: Periodic Review and Update

While following a clear strategy, organizations must continuously monitor and adapt their plans to keep up with evolving threats and technology. The implementation roadmap should evolve as conditions change, not be frozen in amber. Accordingly, organizations should schedule periodic reviews at predetermined intervals to assess progress and identify any roadblocks that may have emerged since the last evaluation.

During these reviews, organizations should assess progress toward achieving goals. Are systems being transitioned as planned? Have any unforeseen challenges arisen that require adjustments to the strategy? By proactively monitoring progress and identifying potential roadblocks early on, the organization can address them swiftly and avoid delays.

The field of quantum computing is constantly evolving. New research findings, updates from NIST on PQC standards, and emerging industry best practices offer valuable insights. Organizations should incorporate this new information into their strategy. This will ensure the company can leverage the latest advancements to maximize its security posture.

Conclusion

The quantum threat is a looming reality that demands immediate attention. Organizations that fail to prepare risk severe consequences, including substantial financial losses, reputational damage, and operational disruptions. By contrast, those proactively addressing this challenge can gain a competitive edge, strengthen their security posture, and protect critical assets.

Developing a comprehensive quantum readiness plan is essential. By designating a quantum champion, conducting a thorough inventory of encryption systems, and prioritizing mitigation efforts, organizations can effectively manage the transition to post-quantum cryptography. Early adoption of quantum-resistant measures safeguards sensitive data and demonstrates a commitment to security and innovation.

The time to act is now. Organizations must seize this opportunity to build a resilient future and protect against the inevitable quantum computing era.

Quantum Readiness Roadmap: What Technology Leaders Need to Know about the Quantum Threat

Appendix A: Readiness Roadmap

Preparation Actions	Description
Internal Actions	
1. Designate a quantum champion	• Stay updated on quantum computing developments • Understand the PQC transition timeline • Assess current security measures • Research quantum-resistant technologies • Implement more robust security strategies • Educate colleagues about quantum threats • Stay connected with experts • Talk with vendors • Inform management of updates • Monitor quantum computing advancements • Ensure resources for quantum readiness

2. Inventory all instances of encryption usage	• For systems:
	  ◦ Identity of system
	  ◦ Security risk level (low, moderate, or high)
	  ◦ High-value asset (yes/no)
	• Cryptographic information:
	  ◦ List all encryption/security systems in use
	  ◦ Algorithms used by each system
	  ◦ System purpose
	  ◦ Length of the encryption keys
	• Software source:
	  ◦ Source of each cryptographic system:
	  ◦ Pre-built software (cots/gots) [vendor name]
	  ◦ Custom-built software [developer name]
	• System details:
	  ◦ List the operating system(s) used, including version details
	  ◦ Indicate where systems are hosted:
	  ◦ On-premises
	  ◦ Commercial cloud service [provider's name]
	  ◦ Government cloud service [agency name]
	  ◦ Hybrid environment [cloud service provider name(s)]
	• Data store:
	  ◦ Briefly describe the types of data stored in the system (e.g., financial records, customer information)
	  ◦ Indicate how long this data needs to be protected

Quantum Readiness Roadmap: What Technology Leaders Need to Know about the Quantum Threat

Preparation Actions	Description
Internal Actions	

3. Risk Assessment and Prioritization of Systems	• Prioritize Cryptographic Systems: After identifying all encryption systems, assess and prioritize them based on risk. This considers:
	  ◦ Potential consequences of a successful attack (financial, reputational, operational)
	  ◦ Difficulty and delays in transitioning critical systems to CRQC alternatives
	• Identify the Data Security Gap:
	  ◦ Classify data based on sensitivity (highly confidential, moderately sensitive) and required protection time (e.g., 30 years, five years)
	  ◦ Analyze the potential gap between data security needs and CRQC implementation
	  ◦ Consider additional security measures if the gap appears significant
	• Identify Dependency Compatibility:
	  ◦ Understand what cryptographic systems depend on (external suppliers, internal systems)
	  ◦ Plan for potential compatibility issues:
	  ◦ Algorithm Support: Updates or replacements might be needed for systems not supporting new PQC algorithms
	  ◦ Performance Differences: Account for potential changes in performance when transitioning to PQC
	  ◦ Data Format: Address any data format changes required for PQC algorithms
	  ◦ Key Management: Plan for managing keys used in PQC systems
	  ◦ Legacy System Integration: Ensure compatibility with existing systems
	  ◦ Interoperability: Verify smooth communication between systems using PQC

4. Understand mitigation options	• Factor in Equipment Refresh:
	  ◦ Plan mitigation based on existing refresh cycles for each system
	  ◦ Upgrade-ready systems benefit from a CRQC transition
	  ◦ Systems with longer cycles might need staged migration or alternative mitigation
	• Choose the Right Approach Based on Risk & ROI:
	  ◦ Information-Theoretic Security: Strongest defense, potentially limited by performance/compatibility
	  ◦ Tokenization: Secures the confidentiality of data even when compromised
	  ◦ Crypto Agility (Adaptability): Seamlessly swap algorithms and key management for future-proof security
	  ◦ PQC Transition (Following NIST Lead): Develop a plan to adopt NIST-approved PQC standards

Quantum Readiness Roadmap: What Technology Leaders Need to Know about the Quantum Threat

Preparation Actions	Description
Internal Actions	

5. Develop transition plan	• Evaluate budget & resources
	• Select mitigation strategy
	• Gain executive support
	• Allocate resources
	• Create implementation timeline:
	  ◦ Develop a realistic timeline considering:
	  ◦ System compatibility
	  ◦ Dependencies
	  ◦ Integration requirements
	• Develop implementation plan:
	  ◦ Considering each system's unique:
	  ◦ Compatibility requirements
	  ◦ Dependencies
	  ◦ Integration needs
	  ◦ Pilot programs: conduct pilot programs on lower-risk systems to:
	  ◦ Test mitigation approaches
	  ◦ Identify challenges
	  ◦ Maintain a living document: update the implementation roadmap as needed based on:
	  ◦ New information
	  ◦ System configuration changes

6. Periodic review and update	• Schedule regular reviews • Monitor progress & challenges • Adapt based on new information • Reassess risks & mitigation strategies • Update timeline & resource allocation

Appendix B: Federal Timeline for Mitigating Risk to Vulnerable Cryptographic Systems[47]

Target Completion Date	Activities to Mitigate Risks to Encryption		Notes about activities
July 3, 2023	Section 3(c)(i)	"Secretary of Commerce, through the Director of NIST, shall initiate an open working group with industry, including critical infrastructure owners and operators, and other stakeholders, as determined by the Director of NIST, to further advance adoption of quantum-resistant cryptography."	Can be found at: https://csrc.nist.gov/Projects/post-quantum-cryptography; https://csrc.nist.gov/Projects/post-quantum-cryptography/Email-List
July 3, 2023	Section 3(c)(ii)	"Secretary of Commerce, through the Director of NIST, shall establish a "Migration to Post-Quantum Cryptography Project" at the National Cybersecurity Center of Excellence to work with the private sector to address cybersecurity challenges posed by the transition to quantum-resistant cryptography."	Can be found at: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
November 1, 2023	Section 3(c)(iii)	"Secretary of Homeland Security, through the Director of the CISA, and in coordination with Sector Risk Management Agencies, shall engage with critical infrastructure and SLTT partners regarding the risks posed by quantum computers, and shall provide an annual report to the Director of OMB, the APNSA, and the National Cyber Director that includes recommendations for accelerating those entities' migration to quantum-resistant cryptography."	
November 1, 2023	Section 3(c)(iv)	"Director of OMB, in consultation with the Director of CISA, the Director of NIST, the National Cyber Director, and the Director of NSA, shall establish requirements for inventorying all currently deployed cryptographic systems, excluding National Security Systems (NSS)."	Can be found at: https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf.
Annually starting October 18, 2023	Section 3(c)(vi)	"National Cyber Director shall, based on the inventories described in subsection 3(c)(v) and in coordination with the Director of CISA and the Director of NIST, deliver a status report to the APNSA and the Director of OMB on progress made by FCEB Agencies on their migration of non-NSS IT systems to quantum-resistant cryptography."	

47. The White House, Press Release, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," May 4, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems)

Target Completion Date	Activities to Mitigate Risks to Encryption		Notes about activities
December 31, 2023	Section 3(c)(xiv)	"Agencies maintaining NSS shall implement symmetric-key protections (e.g., High Assurance Internet Protocol Encryptor (HAIPE) exclusion keys or VPN symmetric key solutions) to provide additional protection for quantum-vulnerable key exchanges, where appropriate and in consultation with the National Manager."	
December 31, 2023	Section 3(c)(xv)	"Secretary of Defense shall deliver to the APNSA and the Director of OMB an assessment of the risks of quantum computing to the defense industrial base and to defense supply chains, along with a plan to engage with key commercial entities to upgrade their IT systems to achieve quantum resistance."	
Annually starting May 4, 2024	Section 3(c)(v)	"Heads of all Federal Civilian Executive Branch (FCEB) Agencies shall deliver to the Director of CISA and the National Cyber Director an inventory of their IT systems that remain vulnerable to CRQCs, focusing on High-Value Assets and High Impact Systems."	
Annually starting May 4, 2024	Section 3(c)(x)	"Director of NSA, in consultation with the Secretary of Defense and the Director of National Intelligence, shall provide guidance on quantum-resistant cryptography migration, implementation, and oversight for NSS."	
Annually starting May 4, 2024	Section 3(c)(xi)	"Heads of agencies operating NSS shall identify and document all instances where quantum-vulnerable cryptography is used by NSS and shall provide this information to the National Manager."	
August 13, 2024	Section 3(a)	"Director of the NIST and the Director of the NSA, in their capacity as the National Manager for National Security Systems, are each developing technical standards for quantum-resistant cryptography for their respective jurisdictions."	Can be found at: https://csrc.nist.gov/pubs/fips/203/final
Until the release of the first set of NIST standards	Section 3(c)(ix)	"Heads of FCEB Agencies shall not procure any commercial quantum-resistant cryptographic solutions for use in IT systems supporting enterprise and mission operations."	
Within 90 days of the release of the first set of NIST standards	Section 3(c)(vii)	"Secretary of Commerce, through the Director of NIST, shall release a proposed timeline for the deprecation of quantum-vulnerable cryptography in standards with the goal of moving the maximum number of systems off quantum-vulnerable cryptography within a decade of the publication of the initial set of standards."	

Target Completion Date	Activities to Mitigate Risks to Encryption		Notes about activities
Within 180 days of the 2024 NSA standards	Section 3(c)(xii)	"National Manager shall release an official timeline for the deprecation of vulnerable cryptography in NSS, until the migration to quantum-resistant cryptography is completed."	
2025 (Within 1 year of the 2024 NSA standards)	Section 3(c)(xiii)	"Heads of agencies operating or maintaining NSS shall submit to the National Manager, and, as appropriate, the Department of Defense Chief Information Officer or the Intelligence Community Chief Information Officer, depending on their respective jurisdictions, an initial plan to transition to quantum-resistant cryptography in all NSS."	
2025 (Within 1 year of the release of the first set of NIST standards)	Section 3(c)(viii)	"Director of OMB, in coordination with the Director of CISA and the Director of NIST, shall issue a policy memorandum requiring FCEB Agencies to develop a plan to upgrade their non-NSS IT systems to quantum-resistant cryptography."	

Acknowledgments

FDD's TCIL is a nonprofit organization that relies on volunteers who are passionate about advancing cybersecurity practices. We are profoundly grateful to Peter Armstrong, Daniel Bardenstein, Rick Bueno, Dr. William Clark, Zachary Daher, Mike Davis, Rob Fuller, Kaleb Hasselstrom, Justin Hatcher Travis Hawley, Alfredo Hickman, Harold Hoang, David Johnson, Sydney Johnson, Daniel Kay, Angelo Longo, Andrew McElroy, Rachel Parkhurst, Alex Sharpe, Paul Stimers, and Phil Venables for their invaluable contributions to this paper.

Quantum Readiness Roadmap: What Technology Leaders Need to Know about the Quantum Threat

About the Authors

Dr. Georgianna "George" Shea serves as chief technologist for FDD's Center on Cyber and Technology Innovation and TCIL. In that role, she identifies cyber vulnerabilities in the U.S. government and private sector, devising pilot projects to demonstrate feasible technology and non-tech solutions that, if scaled, could move the needle in defending U.S. prosperity, security, and innovation.

Jordan Bass is a recent graduate of Texas A&M University, where he received a Bachelor of Science in physics with a business track and minors in economics and communication. He is working at the National Science Foundation on science policy issues with the Directorate for Technology, Innovation, and Partnerships as part of the Future Leaders in Public Service Internship Program.

About the Foundation for Defense of Democracies

FDD is a Washington, DC-based, nonpartisan 501(c)(3) research institute focusing on national security and foreign policy.

About FDD's Transformative Cyber Innovation Lab

TCIL finds and nurtures technologically feasible, testable pilot projects which begin to solve some of the hardest cyber problems afflicting the national security industrial base and the United States. TCIL's mission is to help shorten the lag between idea and piloting and between piloting and the adoption of potential solutions to the thorniest of cyber problems. TCIL seeks to drive revolutionary, society-wide improvement in cyber resilience through the innovative synthesis of technology, policy, and governance.

For more information, visit: https://www.fdd.org/projects/transformative-cyber-innovation-lab