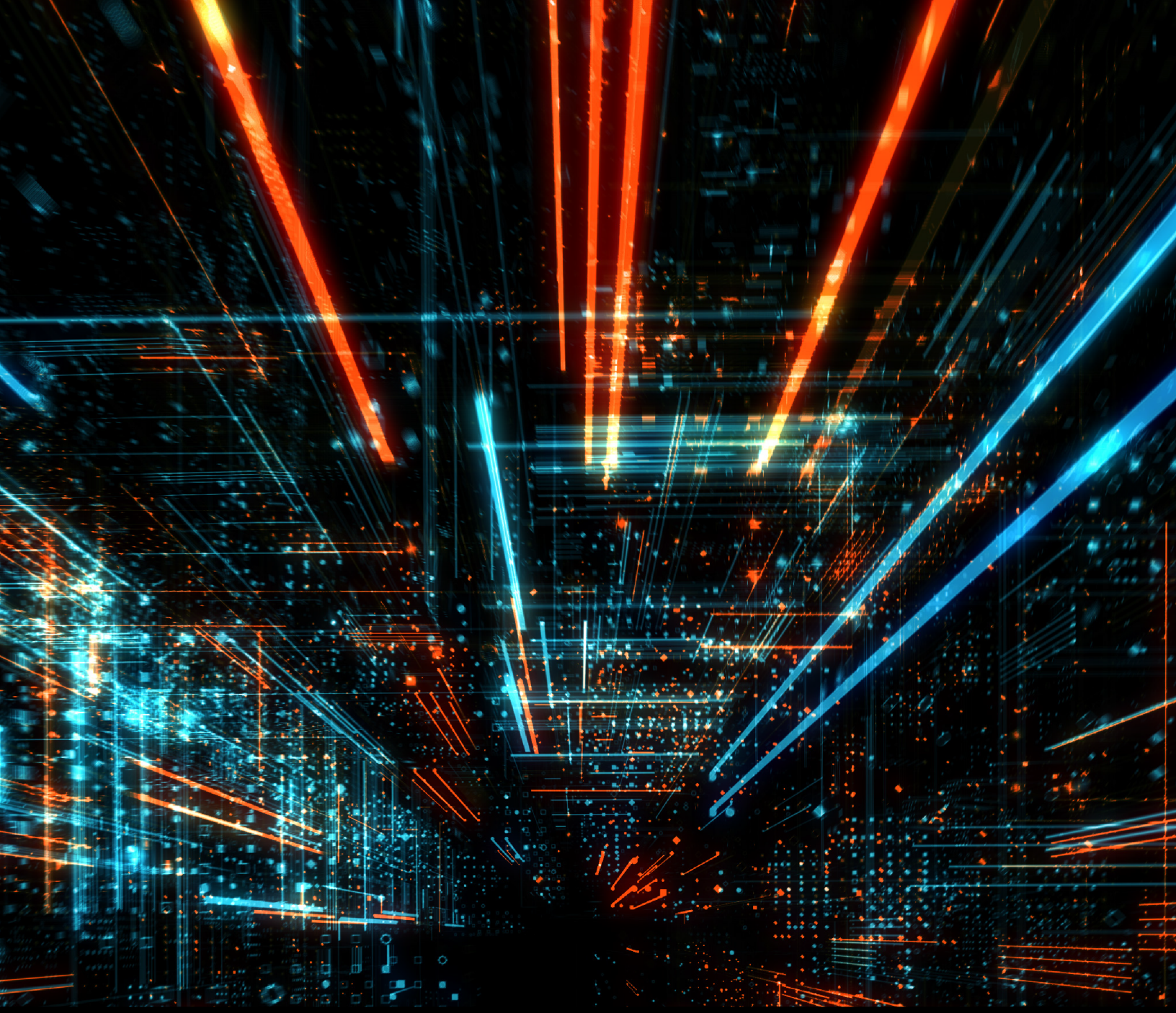

2025

APPROACHING QUANTUM DAWN:

Closing the Cybersecurity Readiness Gap Before It's Too Late

CYBER THREAT ALLIANCE

POWERED BY THE CTA

The Cyber Threat Alliance (CTA) is the industry's first formally organized group of cybersecurity practitioners who work together in good faith to share threat information and improve global defenses against cyber adversaries. CTA facilitates the sharing of cyber threat intelligence to improve defenses, advance the security of critical infrastructure, and increase the security, integrity, and availability of IT systems.

We take a three-pronged approach to this mission:

1. Protect End-Users: Our automated platform empowers members to share, validate, and deploy actionable threat intelligence to their customers in near-real-time.

2. Disrupt Malicious Actors: We share threat intelligence to reduce the effectiveness of malicious actors' tools and infrastructure.

3. Elevate Overall Security: We share intelligence to improve our members' abilities to respond to cyber incidents and increase end-user's resilience.

CTA is continuing to grow globally, enriching both the quantity and quality of the information shared among its membership. CTA is actively recruiting additional cybersecurity providers to enhance our information sharing and operation collaboration to enable a more secure future for all.

For more information about the Cyber Threat Alliance, please visit: https://cyberthreatalliance.org.

APPROACHING QUANTUM DAWN WORKING COMMITTEE MEMBERS

Cisco
Jyoti Chawla
Amy Henderson
Martin G. Lee

Fortinet
Aamir Lakhani

FS-ISAC
Michael Silverman

Institute for Security and Technology
Megan Stifel
Jennifer Tang

IT-ISAC
Ian Andriechack

McAfee
German Lancioni

Palo Alto Networks
Phillip Kwan

Rapid7
Sabeen Malik

Stealth Startup
Jaya Baloo

Cyber Threat Alliance
Emerson Johnston
Michael Daniel
Jeannette Jarvis
Linda Beverly
Kate Holseberg

This report also leverages shared data and published analysis from FS-ISAC and IT-ISAC. CTA members reviewed the document, and the report reflects our shared consensus.

This report would not be possible without the generous support from Craig Newmark Philanthropies.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This Joint Analytic Report (JAR), *Approaching Quantum Dawn: Closing the Cybersecurity Readiness Gap Before It's Too Late*, examines the emerging cybersecurity risks associated with quantum computing and the urgent need for organizational preparedness.

Quantum computing is advancing steadily, and while cryptographically relevant quantum computers (CRQCs) capable of breaking current encryption do not exist yet, adversaries are already adapting their strategies. Tactics such as **Harvest Now, Decrypt Later** (HNDL) campaigns demonstrate that long-lived sensitive data is being stolen today with the intent to decrypt it once quantum capabilities mature.

This report provides an overview of the current quantum threat landscape, debunks common misconceptions around timelines and impact, and emphasizes that quantum risk is not a future event but an evolving reality. It identifies immediate priorities for defenders: **inventorying cryptographic assets, adopting crypto-agile architectures, and initiating hybrid post-quantum pilot deployments**.

The findings highlight that:

- **Quantum progress is accelerating**, supported by government mandates and private investment.
- **Sector-specific vulnerabilities** (e.g., financial services, healthcare, critical infrastructure) will exacerbate the impact if preparation lags.
- **Cryptographic agility**, not just new algorithms, is essential for resilience given the uncertainty about future quantum breakthroughs.
- **Post-quantum cybersecurity offers opportunities**, including improved threat detection and secure communications using quantum technologies.

Organizations that proactively modernize their cryptographic environments now will maintain operational trust and regulatory compliance as the threat matures. Those who delay will face significant risk exposure with limited options for mitigation.

The window to act is open but closing. Quantum disruption is unfolding—not all at once, but steadily—and preparation must start immediately.

INTRODUCTION

In October 2019, Google announced that its 54-qubit quantum computer, Sycamore, had achieved what researchers called "quantum supremacy": the ability to solve a problem faster than any known classical supercomputer.[1] While the task performed—generating random numbers—was not immediately commercially useful, the implications were profound. It marked a milestone in the field of quantum computing, and in doing so, signaled the start of the age in which quantum devices can outpace classical computers, at least for narrow, specialized tasks. Nearly six years later, progress in the quantum computing space has steadily accelerated. New hardware breakthroughs, growing public and private sector investment, and increased government focus have made it clear that quantum computing is not a far-off future capability. It is a fast-approaching reality with significant implications for cybersecurity, privacy, and the global digital economy.

Despite the technical challenges that remain before large-scale, fault-tolerant quantum computers become available, the cybersecurity community has already entered a critical transition period. Adversaries are planning for a world where today's most trusted encryption standards can be broken, and defenders must do the same. Overemphasis on a hypothetical "Q-Day" has skewed the conversation. Real-world quantum risk is unlikely to be a thunderclap—it will unfold gradually, unevenly, and most likely, invisibly. A better understanding is emerging: it is not a Q-Day we are waiting for—it is a "**Quantum Dawn**", and it has already begun.

Early adversary strategies, such as Harvest Now, Decrypt Later (HNDL) tactics, underscore this slow-motion transition. At the same time, trust in cryptographic transition authorities has eroded. Events like the Dual EC DRBG controversy, NSA guidance reversals on ECC, and the Snowden disclosures have led some organizations to resist adopting government-approved cryptographic standards.[2] While understandable, this skepticism should not justify inertia. As with any evolving standard, cryptographic agility—not blind trust—is the safeguard.

History teaches that cryptography is cyclical—what seems unbreakable today may be obsolete tomorrow. The 2022 break of the SIKE algorithm, a NIST finalist in the post-quantum cryptography competition, underscores the ongoing uncertainty surrounding cryptographic vetting. Even schemes that undergo rigorous review can be invalidated by new mathematical insights, reinforcing the need for real-world testing and layered defenses.[3] As Bruce Schneier famously wrote:

Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can't break. It's not even hard. What is hard is creating an algorithm that no one else can break, even after years of analysis. And the only way to prove that is to subject the algorithm to years of analysis by the best cryptographers around.[4]

---

1 Martinis, John. 2019. "Quantum Supremacy Using a Programmable Superconducting Processor." Research.google. October 23, 2019. https://research.google/blog/quantum-supremacy-using-a-programmable-superconducting-processor/

2 Zetter, Kim. 2013. "How a Crypto 'Backdoor' Pitted the Tech World against the NSA." WIRED. September 24, 2013. https://www.wired.com/2013/09/nsa-backdoor/; Nadiya Kostyuk, and Susan Landau. 2022. "Dueling over Dual_EC_DRGB: The Consequences of Corrupting a Cryptographic Standardization Process | Harvard National Security Journal." Harvardnsj.org. 2022. https://harvardnsj.org/2022/06/07/dueling-over-dual_ec_drgb-the-consequences-of-corrupting-a-cryptographic-standardization-process/; National Security Agency. 2022. "NSA Details Network Infrastructure Best Practices." National Security Agency/Central Security Service. March 1, 2022. https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2949885/nsa-details-network-infrastructure-best-practices/; Smolaks, Max. 2014. "Snowden Reveals NSA's Classified Quantum Computing Project." Silicon UK. January 3, 2014. https://www.silicon.co.uk/workspace/snowden-reveals-nsas-classified-quantum-computing-project-134952.

3 Teske, Edlyn. 2022. "NIST Post-Quantum Cryptography: SIKE's Standardization Failure." Cryptomathic.com. Cryptomathic. August 9, 2022. https://www.cryptomathic.com/blog/nist-post-quantum-cryptography-standardization-sike-bites-the-dust.

4 Schneier, Bruce. 1998. "Crypto-Gram." Schneier on Security. October 15, 1998. https://www.schneier.com/crypto-gram/archives/1998/1015.html#cipherdesign.

This arms race between encryption and cryptanalysis stretches back centuries, and quantum computing is simply the logical next step in its escalation. Just as public-key cryptography reshaped security in the 1970s, quantum computing now promises to disrupt it again.

While quantum computing's effects on cryptography may be the most important and profound, it also has the potential to provide significant cybersecurity benefits, from key distribution to routing security. Defenders should be prepared to leverage these capabilities. As a result, cybersecurity providers should plan to incorporate quantum capabilities into their suite of tools.

This Joint Analytic Report (JAR), developed by the Cyber Threat Alliance (CTA) and informed by a working group of cybersecurity and quantum computing experts, is designed to cut through hype and hesitation. It aims to provide defenders with a sober, evidence-based assessment of quantum computing's emerging impact on cybersecurity. It examines what quantum computing is, how it threatens today's digital security foundations, and what practical steps defenders must take to prepare.

The message is not just "prepare for quantum." It is this: building cryptographic agility and resilience now delivers security dividends regardless of whether quantum decryption becomes a reality. The threats are real. The timeline is uncertain. The window to act is open.

QUANTUM COMPUTING AND ITS CYBERSECURITY IMPLICATIONS

Quantum computing represents a fundamentally different model of computation from classical systems. The principles underlying this model are derived directly from quantum mechanics, the branch of physics that governs the behavior of matter and energy at the smallest of scales, and where phenomena such as superposition and entanglement enable radically new modes of information processing.[5]

While classical computers process information in binary bits, each representing either a 0 or a 1, quantum computers use quantum bits, or qubits, that can represent 0, 1, or both simultaneously through a property known as superposition.[6] This feature allows them to explore a vast computational space in parallel, rather than sequentially. Entangled qubits further enable coordinated operations at scale, facilitating tasks that exceed the capacity of classical machines.[7] Together, superposition and entanglement allow quantum computers to solve classes of problems that are intractable for classical computers, such as factoring large integers or accurately modeling the quantum behavior of complex molecular systems.

These capabilities are not just scientific milestones—they carry direct cybersecurity implications. Most affected are asymmetric encryption schemes, such as public-key cryptography. PKC, such as RSA and elliptic curve cryptography (ECC), relies on the fact that factoring large integers or solving discrete logarithm problems is computationally infeasible.[8] Quantum algorithms challenge that assumption. Once scaled, a cryptographically relevant quantum computer (CRQC)—a system capable of reliably executing these algorithms at scale—could break these schemes exponentially faster than classical machines, compromising digital signatures, secure web traffic, and authentication protocols across the internet.

5 Schneider, Josh, and Ian Smalley. 2024. "Quantum Computing." Ibm.com. August 5, 2024. https://www.ibm.com/think/topics/quantum-computing.

6 Schneider, Josh, and Ian Smalley. 2024. "Qubit." Ibm.com. February 28, 2024. https://www.ibm.com/think/topics/qubit.

7 Giles, Martin. 2019. "Explainer: What Is a Quantum Computer?" MIT Technology Review. January 29, 2019. https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/.

8 Miele, Andrea. 2015. "On the Analysis of Public-Key Cryptologic Algorithms," January. https://doi.org/10.5075/epfl-thesis-6603.

Symmetric encryption, like AES, is less affected than asymmetric schemes[9], such as public-key cryptographic algorithms, but it is still weakened, requiring significantly longer keys to maintain equivalent levels of protection.[10] These risks are compounded by the long upgrade cycles typical of critical infrastructure and embedded systems, making early preparation essential.

Industry and standards bodies have already begun responding. For example, OpenSSL, OpenSSH, and Google Chrome have all implemented hybrid cryptographic schemes, blending classical and post-quantum algorithms.[11] Similarly, the X.509 certificate standard now supports hybrid, composite, and chameleon formats to facilitate flexible and forward-compatible authentication.[12] These shifts reflect the growing urgency and complexity of transitioning global systems to post-quantum security.

In parallel, Quantum Key Distribution (QKD) has emerged as a specialized method for secure key exchange.[13] Unlike traditional public-key infrastructure (PKI), which relies on mathematical hardness assumptions, QKD leverages the physical laws of quantum measurement to detect eavesdropping.[14] While promising in theory, QKD remains limited by scalability, infrastructure demands, and compatibility constraints. It is best understood as a niche complement to post-quantum cryptographic modernization—not a substitute.[15]

With this in mind, real-world preparedness remains uneven. Surveys by GDIT,[16] Venafi (now CyberArk),[17] IDEMIA,[18] and NCSA[19] reveal that many organizations have yet to inventory their cryptographic assets or begin migration planning. Adoption of PQC remains low—fewer than 0.03% of OpenSSH sessions currently use post-quantum protocols—while concern about outages and interoperability continues to delay action.[20]

Ultimately, the quantum threat is not about a single breakthrough moment. It is about long-term exposure to a class of emerging capabilities that render today's cryptographic systems fragile. The

---

9 See Daniel 2023 for an explanation of the difference between symmetric and asymmetric encryption.

10 Yassein, Muneer Bani, Shadi Aljawarneh, Ethar Qawasmeh, Wail Mardini, and Yaser Khamayseh. 2017. "Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms." 2017 International Conference on Engineering and Technology (ICET), August, 1–7. https://doi.org/10.1109/icengtechnol.2017.8308215.

11 Sowa, Jakub, Bach Hoang, Advaith Yeluru, Steven Qie, Anita Nikolich, Ravishankar Iyer, and Phuong Cao. 2024. "Post-Quantum Cryptography (PQC) Network Instrument: Measuring PQC Adoption Rates and Identifying Migration Pathways." ArXiv.org. 2024. https://arxiv.org/abs/2408.00054; Help Net Security. 2025. "OpenSSL Prepares for a Quantum Future with 3.5.0 Release - Help Net Security." Help Net Security. April 9, 2025. https://www.helpnetsecurity.com/2025/04/09/openssl-3-5-0-released/

12 Ricchizzi, Nino, Christian Schwinne, and Jan Pelzl. 2025. "Applied Post Quantum Cryptography: A Practical Approach for Generating Certificates in Industrial Environments." ArXiv.org. 2025. https://arxiv.org/abs/2505.04333v1.

13 Olaoye, Godwin. "Quantum Key Distribution (QKD) and the Future of Secure Communications." Sage Advance. Last modified April 2025. https://advance.sagepub.com/doi/full/10.22541/au.174431281.12939966/v1.

14 Scarani, Valerio, and Christian Kurtsiefer. 2025. "The Black Paper of Quantum Cryptography: Real Implementation Problems." ArXiv.org. 2025. https://arxiv.org/abs/0906.4547.

15 Ibid.

16 Alder, Madison. 2024. "Cyber Officials Cite Legacy Systems as Post-Quantum Readiness Challenge." FedScoop. October 16, 2024. https://fedscoop.com/cyber-officials-cite-legacy-systems-as-post-quantum-readiness-challenge/

17 CyberArk Software. 2024. Organizations Largely Unprepared for the Advent of Shorter than 90-Day TLS Certificates. Research Report. CyberArk Software. https://www.cyberark.com/resources/white-papers/organizations-largely-unprepared-for-the-advent-of-90-day-tls-certificates

18 "Post-Quantum Cryptography (PQC) - Challenges and Obstacles to Adoption | IDEMIA." 2025. IDEMIA. February 26, 2025. https://www.idemia.com/insights/key-obstacles-post-quantum-cryptography-pqc-adoption

19 Sowa, Jakub, Bach Hoang, Advaith Yeluru, Steven Qie, Anita Nikolich, Ravishankar Iyer, and Phuong Cao. 2024. "Post-Quantum Cryptography (PQC) Network Instrument: Measuring PQC Adoption Rates and Identifying Migration Pathways." ArXiv.org. 2024. https://arxiv.org/abs/2408.00054.

20 Ibid.

task ahead is not only to adopt new algorithms, but to build systems that can adapt and ensure defenders stay one step ahead, no matter when or how the disruption arrives. The following section expands on the nature and timeline of these threats, including what constitutes a CRQC and how its emergence might unfold.

THE QUANTUM THREAT LANDSCAPE

While quantum computing is often portrayed as an imminent cybersecurity crisis or a speculative future concern, neither extreme is useful for defenders. The reality is more complex: quantum capabilities are progressing steadily, but unevenly. Research breakthroughs, federal mandates, and increased private sector investment are accelerating development, yet significant technical hurdles remain before general-purpose, CRQCs become operational.

UNDERSTANDING CRYPTOGRAPHICALLY RELEVANT QUANTUM COMPUTERS (CRQCS)

A CRQC is not just a quantum processor that has the ability to process information via qubits—it is a system robust enough, scalable enough, and fault-tolerant enough to break today's public-key cryptographic systems reliably.[21] CRQCs are often judged based on their qubit count, which reflects a device's theoretical processing capacity; current systems range from a few dozen to over 1,000 qubits, depending on architecture. This distinction matters. Small, unstable quantum prototypes do not pose a meaningful risk. However, a quantum system capable of sustaining large-scale factorization or discrete logarithm computations would undermine the foundational cryptographic assumptions upon which the security of global digital infrastructure depends

This threat is rooted in two well-established quantum algorithms:

- Proposed by Peter Shor in 1994, Shor's algorithm enabled efficient factorization or large integers and computation of discrete logarithms—both core to RSA, DSA, and ECC.[22] It's implications are profound: once a CRQC becomes available, these systems would no longer be secure.[23]

- Proposed by Lov Grover in 1996, Grover's algorithm improves search efficiency in unsorted databases, reducing the effective strength of symmetric encryption.[24] For instance, a 256-bit key would offer a post-quantum security level roughly equivalent to 128 bits.[25]

Together, these algorithms make clear that both public-key and symmetric cryptographic systems must be reconsidered in a quantum future, although the risks are disproportionately higher for public-key systems.

To visualize the asymmetry quantum computers introduce, consider this example: solving 9 x 8 = 72 is trivial for any computer. But reversing it—finding two prime numbers that multiply to 72—requires more work. Classical machines perform this reversal through trial and error. Quantum computers, using Shor's algorithm, effectively test all possibilities

21 Townsend, Kevin. 2025. "Cyber Insights 2025: Quantum and the Threat to Encryption." SecurityWeek. February 3, 2025. https://www.securityweek.com/cyber-insights-2025-quantum-and-the-threat-to-encryption/.

22 Shor, P.W. 2002. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," December, 124–34. https://doi.org/10.1109/sfcs.1994.365700.

23 Ibid.

24 Grover, Lov K. 1996. "A Fast Quantum Mechanical Algorithm for Database Search." Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing - STOC '96, 212–19. https://doi.org/10.1145/237814.237866.

25 Ibid.

simultaneously, collapsing the search into one step. This dynamic reshapes assumptions about what is 'hard' to compute.

WHY VOLUME, NOT QUBIT COUNT, SIGNALS THREAT MATURITY

Understanding progress toward CRQCs requires more than counting qubits. Quantum Volume (QV)—a metric proposed by IBM—offers a more accurate view of quantum capabilities by accounting for other relevant factors such as qubit coherence time, gate fidelity, crosstalk, initialization and calibration errors, and the effectiveness of circuit optimization.[26] Additional variables—including coupling maps, spectator errors, and gate parallelism—impact whether a system can run deep, entangled circuits reliably. QV reflects a composite view of scale and stability, emphasizing how well a quantum device performs complex algorithms, not just how large it is.

Figure 1 illustrates how Quantum Volume captures this interplay of fidelity and scale.

Practical quantum attacks, such as breaking RSA-2048, are estimated to require thousands of logical qubits, which translates to millions of physical qubits when error correction is factored in.[27] However, factoring in the other metrics of quantum volume, such as gate fidelity, coherence time, error rates, and circuit depth, reveals that raw qubit count is only one dimension of readiness. A system with a high qubit count but low fidelity or high error rates remains operationally irrelevant for cryptanalytic purposes. These interdependent factors mean that reaching a cryptographically relevant threshold is not merely a matter of scaling—it requires consistent control across the full computation stack.

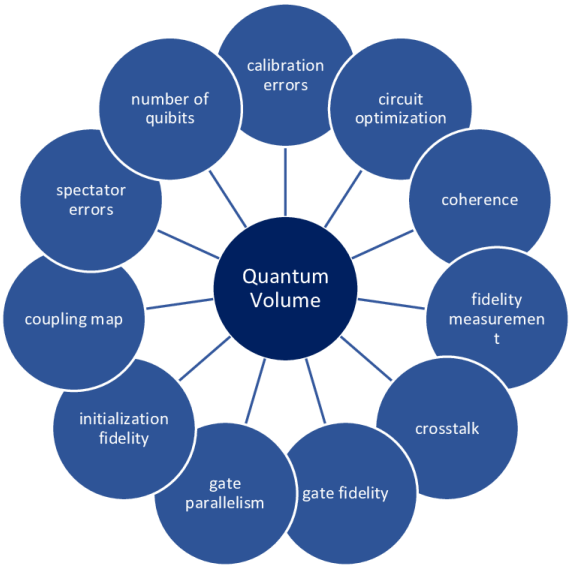

Figure 1. Quantum Volume. Adapted from Forbes (2019), based on IBM Research (2017). From Silvestri (2020).[28]

While all known machines remain below this threshold, hardware developments are advancing quickly. For example, IBM's latest system, the 1,121-qubit Condor processor, released in late 2023, marks the first superconducting chip to surpass the 1,000-qubit barrier.[29] In parallel, IBM has publicly committed to delivering a modular quantum system exceeding 4,000 qubits by the end of 2025—an ambitious milestone that, if achieved, will represent a new scaling frontier.[30]

26 Wheeler, Andrew. 2019. "IBM Achieves Highest Quantum Volume to Date - Engineering.com." Engineering.com. March 4, 2019. https://www.engineering.com/ibm-achieves-highest-quantum-volume-to-date/.

27 Ibid.

28 Silvestri, Riccardo. 2020. "Business Value of Quantum Computers: Analyzing Its Business Potentials and Identifying Needed Capabilities..." ResearchGate. unknown. August 16, 2020. https://www.researchgate.net/publication/343683519_Business_Value_of_Quantum_Computers_analyzing_its_business_potentials_and_identifying_needed_capabilities_for_the_healthcare_industry.

29 Gambetta, Jay. 2023. "IBM Quantum System Two: The Era of Quantum Utility Is Here | IBM Quantum Computing Blog." IBM. December 4, 2023. https://www.ibm.com/quantum/blog/quantum-roadmap-2033.

30 Morrison, Ryan. 2022. "IBM Quantum Computer Could Reach 4,000 Qubits by 2025." Tech Monitor. November 9, 2022. https://www.techmonitor.ai/technology/emerging-technology/ibm-quantum-supercomputer.

QUANTUM PROGRESS AND THE MYTH OF PREDICTABLE WARNING

This uncertainty is central to strategic planning. Optimistic projections place CRQC capability within the next 10–15 years, but some experts argue the bottlenecks, especially around scalable error correction, may delay disruption for several decades.[31] Both views are credible and reinforce the case for implementing cryptographic agility. Whether the next major vulnerability emerges from quantum breakthroughs or advances in classical cryptanalysis, and whether it materializes tomorrow or decades from now, the cryptographic layer must be ready to evolve.

To that end, governments are already acting. The U.S. National Security Memorandum 10 (NSM-10) mandates a complete post-quantum transition by 2035, the U.S. Department of Homeland Security is targeting 2030 to migrate high-impact systems, and the NSA's CNSA 2.0 suite recommends using quantum-resistant algorithms as early as 2025.[32] These are not just symbolic deadlines; they reflect a growing recognition that set-it-and-forget-it cryptography must be replaced with agile systems.

Yet, misconceptions remain persistent. One is the belief that defenders will have a clear warning when a CRQC emerges. However, as the historical example of Enigma shows, cryptographic breakthroughs are often exploited in secret, especially by nation-states, before becoming public knowledge. Another myth is that quantum risk is uniformly distributed. In reality, the most acute danger lies in asymmetric compromise of high-value targets whose encrypted data has long-term utility.

Lower costs of stage and compute make long-term collection strategies increasing feasible. The "Harvest Now, Decrypt Later" (HNDL) threat model—exfiltrating encrypted data now to decrypt once CRQCs emerge— is already viable for state-level actors.[33] Though indexing and storing large datasets poses non-trivial burdens, the payoff for compromising diplomatic cables, biomedical IP, or classified archives can justify the investments.[34]

What makes HNDL thefts especially concerning is their stealth; organizations may never know it has occurred, because nothing is "broken" at the moment of exfilitration. Detection becomes possible only after decryption—when it's too late. Still, defenders are not powerless. Behavior analytics systems (e.g. SIEMs and UEBA platforms) can detect suspicious encrypted bulk transfers and other anomalies, even without decrypting payloads.[35] Continued investment in encrypted traffic telemetry and quantum-aware threat modeling will be critical to proactive defense.

Ultimately, HNDL threats highlight a broader imperative; organizations must accelerate crypto modernization efforts—not in response to a fixed date when a CRQC might appear, but to reduce systemic fragility. The real challenge is uncertainty. Quantum risk is probabilistic, cascading, and difficult to reverse. In that context, cryptographic agility is not

---

31 Chen, Sophia. 2025. "Drama over Quantum Computing's Future Heats Up." The Verge. March 21, 2025. https://www.theverge.com/tech/633248/beyond-the-hype-of-quantum-computers

32 National Security Agency. 2024. "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ." Cybersecurity Information Sheet, U/OO/194427-22 | PP-24-4014, Version 2.1, December 2024. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF.

33 The Biden White House. 2022. "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems | the White House." The Biden White House. May 4, 2022. https://bidenwhitehouse.archives.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/; Ivezic, Marin. 2023. "Harvest Now, Decrypt Later (HNDL) Risk." PostQuantum - Quantum Computing, Quantum Security, PQC. June 8, 2023. https://postquantum.com/post-quantum/harvest-now-decrypt-later-hndl/.

34 Ibid.

35 Palo Alto Networks. 2015. "What Is UEBA (User and Entity Behavior Analytics)?" Palo Alto Networks. 2015. https://www.paloaltonetworks.com/cyberpedia/what-is-user-entity-behavior-analytics-ueba.

just a mitigation tactic—it's an operational obligation.

THE CRYPTOGRAPHIC AGILITY IMPERATIVE

Preparing for the quantum future is not simply a matter of adopting new cryptographic algorithms once they become available. Instead, organizations must restructure their cryptographic environments to prioritize adaptability, visibility, and control regardless of the quantum adoption timeline. This approach requires embracing **cryptographic agility**—the capacity to rapidly identify, upgrade, and, if necessary, replace cryptographic algorithms and protocols in response to emerging threats without disrupting broader systems.[36] The cybersecurity industry has an important role to play in helping organizations implement cryptographic agility.

WHAT IS CRYPTOGRAPHIC AGILITY?

The concept of cryptographic agility, introduced by Brian LaMacchia and John Manferdelli in 2006, anticipated a core cybersecurity truth: cryptographic systems must evolve faster than the threats against them.[37] Importantly, cryptographic agility is not simply the ability to swap algorithms. Rather, it is the engineered capacity to maintain trust under uncertainty, when neither the threat model nor the cryptographic defense is stable. LaMacchia and Manferdelli's work on Microsoft's Crypto Next Generation (CNG) API highlighted that resilience isn't achieved through algorithm strength alone—it depends on how quickly systems can pivot when assumptions fail.

Today, this principle has become critical for cybersecurity providers. As the timeline for CRQCs compresses and distrust in centralized standards bodies persists (e.g., Dual EC DRBG, ECC guidance reversals),[38] organizations need agility as a safeguard.

At its core, cryptographic agility rests on two pillars:

- **Design modularity**: Agile cryptographic systems isolate algorithm logic behind APIs and avoid hard-coding protocols, like fixed key sizes or specific handshake types.[39] This abstraction allows smoother transitions to emerging paradigms such as lattice-based signatures, hash-based authentication, or hybrid certificate chains.

- **Operational readiness**: Agility requires visibility into cryptography across applications, systems, and supply chains.[40] Organizations must be capable of testing, deploying, and rolling back changes to cryptographic protocols at speed, across distributed environments.

This mandate is not just technical. It also involves an organizational transformation which must be resourced, governed, and maintained. Cryptographic agility acknowledges uncertainty. It assumes that no standard is permanently secure, future breakthroughs (quantum or classical) are inevitable, and resilience must be engineered in advance.

---

36 LaMacchia, Brian, and John Manferdelli. 2006. "New Vistas in Elliptic Curve Cryptography." Inf. Secur. Tech. Rep. 11 (December): 186–92. https://www.microsoft.com/en-us/research/publication/new-vistas-in-elliptic-curve-cryptography/.

37 Ibid.

38 Green, Matthew. 2013. "The Many Flaws of Dual_EC_DRBG." A Few Thoughts on Cryptographic Engineering. September 18, 2013. https://blog.cryptographyengineering.com/2013/09/18/the-many-flaws-of-dualecdrbg/.

39 Ivezic, Marin. 2022. "Mitigating Quantum Threats beyond PQC." PostQuantum - Quantum Computing, Quantum Security, PQC. September 2022. https://postquantum.com/post-quantum/mitigating-quantum-threats-pqc/.

40 Harishankar, Ray, Michael Osborne, Jai Arun, John Buselli, and Jennifer Janechek. 2024. "Crypto-Agility and Quantum-Safe Readiness | IBM Quantum Computing Blog." IBM. June 19, 2024. https://www.ibm.com/quantum/blog/crypto-agility.

CRYPTOGRAPHIC AGILITY IN PRACTICE

Several early adopters offer compelling examples of cryptographic agility in practice. In 2023, Apple updated its iMessage protocol to incorporate post-quantum cryptographic algorithms (PQ3), enabling a hybrid cryptographic model that combines classical and post-quantum primitives.[41] This shift occurred without disruption, a strong signal that cryptographic agility can scale to consumer systems.

Similarly, Cloudflare, one of the largest providers of internet security services, has integrated hybrid key exchange mechanisms based on post-quantum algorithms into its TLS 1.3 deployments, allowing secure communications to resist both classical and future quantum attacks.[42] OpenSSH, the widely used secure shell (SSH) protocol implementation, has introduced default support for hybrid key exchanges, blending classical and post-quantum algorithms to safeguard remote administration activities.[43]

These examples provide early signals of the technical, regulatory, and market shifts underway. As one participant in the working group put it, “Cryptographic agility isn’t theoretical anymore. It’s table stakes.”

Another noteworthy case is Samsung. Similar to Cloudflare and Apple, Samsung has taken a proactive stance in post-quantum preparedness. However, their approach takes the form of implementing PQC across its device ecosystem not for customer marketing, but for internal protection.[44] This neutral posture, absent direct commercial PQC products, adds credibility to its messaging.

Samsung’s public technical documentation and press materials clearly articulate why waiting for final standards is a mistake, and why early action is essential. Citing assessments from the Global Risk Institute, they note that experts estimate a 33% to 54% probability that a disruptive quantum event could occur within the next 15 years.[45] Crucially, they emphasize that this forecast is not a reason to delay action until quantum computers are fully operational. Rather, the growing risk of "Harvest Now, Decrypt Later" (HNDL) attacks—where adversaries steal encrypted data today to decrypt it in the future—demands urgent countermeasures.[46] Even without current decryption capability, sensitive user data is already vulnerable.

Samsung’s approach mirrors a broader industry pattern. From Apple’s PQ3 update to Cloudflare’s default PQC integration (recognized by a Quantum Readiness Award in 2024), leading organizations consistently use “Harvest Now, Decrypt Later” (HNDL) threats to justify their early adoption.[47]

Together, these cases reinforce a common theme: credible justification for action exists, and organizations across sectors are operationalizing it. Highlighting this consistency in motivation and approach can help demystify PQC adoption and reduce perceived barriers to initial engagement.

---

41 Apple Security Engineering and Architecture (SEAR). 2024. “IMessage with PQ3: The New State of the Art in Quantum-Secure Messaging at Scale - Apple Security Research.” Apple Security. February 21, 2024. https://security.apple.com/blog/imessage-pq3/.

42 Westerbaan, Bas. 2024. “The State of the Post-Quantum Internet.” The Cloudflare Blog. March 5, 2024. https://blog.cloudflare.com/pq-2024/.

43 Kunz, Dr Christopher. 2025. “OpenSSH 10 Relies on Standards for Quantum-Safe Key Exchange.” Security, April. https://heise.de/-10346176.

44 “The First Step to a Quantum-Ready Future with Samsung Knox.” 2025. Samsung.com. 2025. https://news.samsung.com/ca/the-first-step-to-a-quantum-ready-future-with-samsung-knox.

45 “S3SSE2A: Hardware PQC Locks in Security for the Quantum Era.” 2025. Samsung Semiconductor USA. March 4, 2025. https://semiconductor.samsung.com/us/news-events/tech-blog/s3sse2a-hardware-pqc-locks-in-security-for-the-quantum-era/.

46 Ibid.

47 Apple Security Engineering and Architecture (SEAR). 2024. “IMessage with PQ3: The New State of the Art in Quantum-Secure Messaging at Scale - Apple Security Research.” Apple Security Research. February 21, 2024. https://security.apple.com/blog/imessage-pq3/; “Cloudflare Named Winner of the 2024 DigiCert Quantum Readiness Award.” 2024. Digicert.com. December 19, 2024. https://www.digicert.com/news/digicert-announces-quantum-readiness-award-winner.

Ultimately, cryptographic agility requires not only technical foresight but organizational commitment. Building abstraction layers, modular key management systems (KMS), and upgrade-ready certificate authorities demands sustained investment. But the cost of inaction—rigid infrastructure with no pivot path—will be much greater.

TOWARD A UNIVERSAL CRYPTOGRAPHIC AGILITY MATURITY MODEL

Measuring an organization's cryptographic agility is no longer a theoretical consideration but a strategic necessity. Over the past several years, a range of frameworks—both maturity models and scorecards—have been developed to support this effort. While maturity models typically describe staged progressions along a capability curve (e.g., from basic to advanced practices), scorecards emphasize real-world diagnostic tools for identifying current posture, assessing risk, and guiding immediate investment. Each plays a complementary role.[48]

The CTA working group reviewed a representative set of these frameworks, including:

- the NIST CSWP 15 White Paper (April 2021), a foundational strategic overview that outlines cryptographic transition challenges and sets the stage for post-quantum migration planning in federal and enterprise systems; [maturity model]
- the Cryptographic Agility Maturity Model (CAMM) by Hohm, Heinemann, and Wiesmaier (September 2022), which proposes a structured, rubric-based model focusing on modularity, visibility, and operational agility; [maturity model]
- the AgileSec Analytics Cryptographic Scorecard by InfoSec Global (June 2023), which provides a high-resolution enterprise scorecard for auditing cryptographic assets, algorithm use, and agility posture across systems; [scorecard]
- the Strategic Framework for Crypto Agility and Quantum Risk Assessment by ATIS (January 2024), which frames crypto agility from a telecommunications infrastructure perspective and emphasizes harmonized governance and lifecycle planning; [maturity model]
- the FS-ISAC's Building Cryptographic Agility Maturity Model (October 2024), which outlines a four-tiered maturity pathway ("Possible," "Prepared," "Practiced," "Sophisticated") tailored to financial services institutions; [maturity model]
- the NIST CSWP 39 White Paper (March 2025), a technical blueprint titled "Considerations for Achieving Crypto Agility: Strategies and Practices" that offers detailed recommendations for interoperability, protocol transitions, and operational integration; [maturity model].[49]

These models converge on a shared insight: agility is a spectrum, not a switch. They each recognize that cryptographic agility spans technical design, operational practices, and governance structures. They emphasize modular architectures, continuous visibility, and migration readiness—all underpinned by organizational commitment.

---

48 Eby, Kate. 2022. "IT Maturity Models, Scorecards & Assessments | Smartsheet." Smartsheet. March 9, 2022. https://www.smartsheet.com/content/it-maturity?srsltid=AfmBOormXhvn85ZuiLiydn8XR1cNJJvAQg5sr6QuTCHQfAe3BAbRyva8.

49 National Institute of Standards and Technology (NIST). Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms. NIST CSWP 04282021, April 2021. https://doi.org/10.6028/NIST.CSWP.04282021; Hohm, C., Heinemann, A., & Wiesmaier, A. Cryptographic Agility Maturity Model (CAMM). ArXiv preprint arXiv:2202.07645v3, September 2022. https://arxiv.org/pdf/2202.07645; InfoSec Global. AgileSec™ Analytics Cryptographic Scorecard. June 2023. https://www.infosecglobal.com/posts/agilesec-analytics-cryptographic-scorecard; Alliance for Telecommunications Industry Solutions (ATIS). Strategic Framework for Crypto Agility and Quantum Risk Assessment. ATIS-I-0000098, January 2024. https://atis.org/resources/strategic-framework-for-crypto-agility-and-quantum-risk-assessment/; Financial Services Information Sharing and Analysis Center (FS-ISAC). Building Cryptographic Agility in the Financial Sector. October 2024. https://www.fsisac.com/pqc-crypto-agility; National Institute of Standards and Technology (NIST). Considerations for Achieving Crypto Agility: Strategies and Practices. NIST CSWP 39 (IPD), March 2025. https://doi.org/10.6028/NIST.CSWP.39.ipd

After reviewing these models, the CTA working group created the **Consolidated Cryptographic Agility Maturity Scorecard** as a unified baseline assessment tool. It brings together common insights and practical criteria from these resources into a single reference point. The intent is not to replace sector-specific models, but to offer cybersecurity organizations a diagnostic tool—one that can support benchmarking across multiple domains and be adapted as needed to reflect specific industry or partner requirements.

CTA Cryptographic Agility Maturity Scorecard

A multidimensional progress matrix for benchmarking post-quantum cryptographic readiness.

Dimension	Beginner	Intermediate	Advanced	Leader
Inventory and Visibility	No active cryptographic inventory; cryptographic use is undocumented, ad hoc, and embedded in legacy systems with no visibility across software or hardware layers.	Partial inventory exists; some cryptographic components are cataloged, often limited to externally facing applications or manually tracked systems. No automation.	Full asset inventory maintained across major systems; cryptographic algorithms, key lengths, and libraries are tracked using static scanning or limited automation tools.	Real-time, continuously updated cryptographic bill-of-materials (CBOM) integrated into configuration management databases (CMDB); covers all environments including embedded, cloud, and third-party APIs.
Modular Design	Cryptographic logic is hard-coded within application source code; changes require source-level rewrites and full redeployment.	Select systems use wrapper libraries or abstracted interfaces in pilot applications; however, design patterns are inconsistent across the codebase.	Modular cryptographic APIs deployed in mission-critical systems; most new development adheres to separation-of-concerns design. Library versioning and upgrade paths are documented.	Enterprise-wide standardization of modular cryptographic frameworks; algorithm substitution supported without code change; SDKs and CI/CD pipelines enforce compliance with crypto-agile design templates.
Migration Readiness	No formal strategy for post-quantum migration; no identified owners, funding, or timeline. Assumes NIST publication alone will drive change.	Initial planning underway; working groups formed, high-value systems identified, preliminary impact assessments conducted, but no testing yet.	Pilot migrations implemented for selected high-value systems; hybrid cryptographic modes tested in production-adjacent environments. Findings documented for future scaling.	PQC migration program in execution across business units; cryptographic lifecycle integrated into enterprise architecture reviews; live PQC use in production with fallback mechanisms and rollback validation.
Governance and Policy	No formal governance mechanisms; decisions made ad hoc by individual teams or based on historical vendor defaults. No audit trails or policy documentation.	Draft policies exist but are inconsistently applied; crypto lifecycle risk acknowledged but not embedded into broader IT or security governance frameworks.	Formal governance framework established; cryptographic standards and transitions reviewed by central authority (e.g., CISO office); roles, responsibilities, and escalation paths defined.	Governance embedded into enterprise risk management; regular audits and KPIs track cryptographic compliance; board-level oversight; crypto resilience included in business continuity and third-party risk.
Operational Testing	No testing of cryptographic components; assumptions about security remain unvalidated; reliance on legacy penetration tests or vendor claims.	Manual cryptographic verification conducted sporadically, typically during audits or incident response. Static analysis tools used inconsistently.	Automated testing of cryptographic algorithms and implementations embedded in QA processes; hybrid and PQC algorithms tested for performance and compatibility.	Continuous integration of cryptographic validation into DevSecOps pipelines; fault injection, rollback testing, and algorithm failover simulation included in regression testing; test coverage mapped to inventory.
Vendor Management	Vendors selected without regard for cryptographic posture; cryptographic choices opaque and uncontracted; vendor dependencies undocumented.	Vendors queried about cryptographic standards and PQC roadmaps; responses used in risk assessments but not binding; crypto-related SLAs absent.	Vendors contractually commit to support PQC transitions; clauses include disclosure of cryptographic dependencies and timelines for compliance with new standards.	Contracts include enforceable agility provisions: e.g., mandatory CBOM disclosure, algorithm substitution SLAs, automated reporting of crypto health, and right to audit PQC readiness. Vendors ranked by cryptographic maturity in procurement scoring.

DIMENSION ANALYSIS

Each dimension in the CTA Cryptographic Agility Maturity Scorecard reflects a state of readiness, not a checklist of tasks. These descriptions are meant to help organizations locate themselves along a maturity continuum across six key domains. The scorecard is intentionally state-based to preserve comparability with existing maturity models—such as those from NIST, CAMM, and FS-ISAC—while incorporating expanded dimensions including vendor dependencies, architectural modularity, and automated validation.

Inventory and Visibility

- **Why It Matters:** Without cryptographic asset visibility, cybersecurity providers cannot quantify exposure, assess algorithmic risk, or plan transitions.
- **Path to Leadership:** Implement automated cryptographic bill-of-materials (CBOMs), integrate them into continuous monitoring systems, and ensure real-time updates across infrastructure.

Modular Design

- **Why It Matters:** Cryptographic agility is infeasible in monolithic systems. Modularity enables rapid replacement of compromised algorithms.
- **Path to Leadership:** Refactor systems to decouple cryptographic logic from business logic using crypto-abstracted APIs, support dynamic negotiation of algorithms, and deploy cryptographic agility toolkits.

Migration Readiness

- **Why It Matters:** Delayed planning leads to high-stakes migrations under pressure. Early engagement mitigates operational risks and ensures strategic phasing.
- **Path to Leadership:** Complete cryptographic risk assessments, conduct hybrid deployments with NIST-selected PQC candidates, and execute controlled rollouts with rollback mechanisms.

Governance and Policy

- **Why It Matters:** Without formal policy, crypto transitions lack resourcing, prioritization, and cross-functional accountability.
- **Path to Leadership:** Integrate cryptographic agility into enterprise risk management, allocate budget for algorithm transitions, and formalize oversight at the board or CISO level.

Operational Testing

- **Why It Matters:** Testing validates assumptions. Manual processes are prone to error and lack coverage; automated tools ensure scalable, consistent verification.
- **Path to Leadership:** Embed crypto-aware testing into CI/CD pipelines, validate compatibility of new primitives, and run simulations of algorithm substitution events.

Vendor Management

- **Why It Matters:** Most organizations depend on vendors for cryptographic infrastructure. Inflexible contracts and opaque supply chains create systemic risk.
- **Path to Leadership:** Demand transparency in cryptographic dependencies, include agility clauses in procurement contracts, and require evidence of PQC roadmap adoption.

APPLYING THE SCORECARD

The Progress Scorecard is designed to serve as a "first-stop" diagnostic tool. It consolidates insights from a range of industry and government models—

including those by NIST, CAMM, FS-ISAC, ATIS, and InfoSec Global—into a single, multidimensional matrix. While state-based, its structure supports action by revealing gaps and asymmetries across functional areas.

Organizations and cybersecurity providers can use the scorecard in the following ways:

- **Gap Analysis:** Score current posture in each dimension. Identify asymmetries—e.g., high visibility but low migration planning—that may create systemic vulnerabilities.
- **Investment Planning:** Use maturity levels to inform budget allocation and resourcing. Early-stage organizations should prioritize visibility and governance; advanced ones should focus on testing and vendor enforcement.
- **Benchmarking:** As sector-specific metrics emerge (e.g., FS-ISAC or NCSC readiness indices), this model allows for internal benchmarking and cross-industry comparison.
- **Governance Reporting:** Include maturity scores in executive dashboards to elevate cryptographic risk from a technical concern to a board-level priority.

Cryptographic agility is not merely a best practice but the precondition for surviving the coming transition. When a CRQC becomes operational, organizations without agility will face only two choices: accept exposure or halt operations for emergency remediation.

This scorecard offers a structured path to avoid that binary. Leadership in this space does not mean achieving cryptographic perfection. It means institutionalizing adaptability, baking readiness into architecture, and embedding crypto evolution into security and procurement culture.

BARRIERS TO TRANSITION

Despite growing awareness of the quantum threat, many organizations remain stalled in achieving cryptographic agility and preparing for post-quantum migration. This delay reflects not only technical inertia but the cumulative weight of operational complexity, competing priorities, and fractured responsibility. The CTA Maturity Scorecard identifies multiple dimensions of readiness precisely to make these interdependencies legible. What may appear as a cryptographic problem is frequently a governance or vendor issue in disguise.

One of the most persistent obstacles is **vendor lock-in**. Cryptographic algorithms are often deeply embedded in proprietary systems, firmware, or legacy hardware—sometimes in undocumented ways but also in ways tightly bound to regulated vendor environments.[50] In many cases, transitioning to post-quantum algorithms requires not only rewriting code but renegotiating vendor contracts, replacing infrastructure, or waiting for third-party providers to support new standards.[51] While vendor dependence is not inherently problematic, it becomes a barrier in jurisdictions lacking clear procurement mandates or upgrade incentives.

Compounding the vendor lock-in problem is the lack of **cryptographic visibility**. Most organizations cannot say with confidence where and how cryptography is used across their environments, let alone which systems depend on vulnerable algorithms.[52] This oversight is not just a technical

50 Mantas, Georgios, Firooz Saghezchi, Jonathan Rodriguez, and Victor Sucasas. 2024. Security and Privacy for 6G Massive IoT. John Wiley & Sons. https://www.usenix.org/conference/usenixsecurity21/presentation/meijer.

51 Ibid.

52 Hiremath, Omkar. 2021. "Introduction to Cryptographic Failures | USA." Software Secured. 2021. https://www.softwaresecured.com/post/introduction-to-cryptographic-failures.

problem; it's a systemic gap in asset management and risk governance. This blind spot becomes especially consequential in Harvest Now, Decrypt Later (HNDL) scenarios, where encrypted data is exfiltrated long before decryption becomes feasible.

Governance shortfalls further slow progress. Without executive sponsorship, dedicated budgets, or integration into enterprise risk frameworks, cryptographic agility remains a "back office" concern, competing for attention against louder operational or compliance demands. To correct this, organizations must elevate cryptographic resilience to the same tier as business continuity or disaster recovery. Achieving this goal means establishing cross-functional ownership, embedding crypto strategy into digital transformation programs, and securing long-term commitment to continuous modernization.

Finally, protocol-level constraints introduce complex technical barriers that even well-resourced teams struggle to address. Core internet standards such as Domain Name System Security (DNSSEC) rely on fixed-size signature formats that are incompatible with many PQC candidates, requiring significant redesign to accommodate the more extended key sizes and hash outputs.[53] The same holds for embedded and operational technology (OT) systems, where low compute power, outdated firmware, and long hardware life cycles make upgrades infeasible or cost-prohibitive.[54]

Moreover, cryptographic readiness must extend beyond just adopting quantum-safe algorithms. Implementation matters, because side-channel vulnerabilities, flawed hybrid implementations, and layering missteps can all compromise post-quantum transitions. For example, one way to mitigate risk is to use a "hybrid" approach, which means combining different cryptographic algorithms. However, each hybrid approach carries different risks: PQC+PQC may hedge algorithm-specific vulnerabilities but lacks a classical fallback; PQC+classical risks downgrade attacks through fallback exploitation; PQC+QKD combines physical and mathematical layers but suffers from scalability and compatibility constraints. Careful architecture is needed to mitigate chained or cascading failures. Importantly, these challenges cannot be solved at the organizational level alone. They demand coordinated R&D, standards development, and policy alignment across sectors and government.

SECTOR-SPECIFIC READINESS: IMPLICATIONS FOR THE CYBERSECURITY INDUSTRY

While quantum disruption is a global challenge, its impact is not evenly distributed. Sector-specific differences in cryptographic exposure, infrastructure flexibility, and regulatory posture create divergent timelines and complexities for mitigation. However, rather than each industry solving these challenges independently, the cybersecurity community should provide scalable solutions integrated across verticals, particularly in detection, inventory, agility, and resiliency.

The following heat map in Figure 2 summarizes sectoral variance in exposure, complexity, and urgency for post-quantum preparedness over the 2025–2030 horizon:

53 Mueller, Moritz, Jins De Jong, Maran Van Heesch, Benno Overeinder, and Roland Van Rijswijk-Deij. 2020. "Public Review for Retrofitting Post-Quantum Cryptography in Internet Protocols: A Case Study of DNSSEC." ACM SIGCOMM Computer Communication Review. https://conferences.sigcomm.org/sigcomm/2021/files/papers/3431832.3431838.pdf.

54 Cybersecurity and Infrastructure Security Agency, Post-Quantum Considerations for Operational Technology (October 2024), https://www.cisa.gov/sites/default/files/2024-10/Post-Quantum%20Considerations%20for%20Operational%20Technology%20%28508%29.pdf.

Sector	Threat Exposure	Migration Complexity	Urgency
Financial Services	High	High	High
Government and Defense	High	Medium	High
Healthcare and Data Custodians	High	High	Medium
Critical Infrastructure and OT	Medium	High	High
Small and Medium Enterprises	Medium	Medium	Medium

Figure 2: Sector Quantum Risk Readiness Heatmap (2025–2030 Outlook)[55]

Despite differences in threat posture, sectors share core readiness gaps that cybersecurity vendors must help address. Foremost is cryptographic visibility: asset management tools need built-in capabilities to detect cryptographic usage, highlight legacy algorithms, and assess protocol readiness. Organizations cannot plan or prioritize transitions effectively without clear visibility into where and how cryptography is implemented.

Vendors must also provide real-time detection and telemetry for cryptographic protocols in use. This telemetry should include identifying deprecated or quantum-vulnerable schemes and flagging whether hybrid or post-quantum cryptographic mechanisms, such as those added to OpenSSL or Google Chrome, are operational. These capabilities are essential for enterprises seeking to map readiness or conduct compliance assessments.

Managed transition services are vital for under-resourced sectors such as SMEs and certain public agencies. Cloud providers and MSSPs should bundle quantum resilience into baseline offerings, eliminating the need for internal cryptographic expertise. Post-quantum migration should be available "as a service," with tooling abstracted, vendor-neutral, and aligned with readiness frameworks such as the CTA Scorecard.

Importantly, vendors should not assume universal trust in cryptographic standards. While NIST's PQC algorithms have undergone extensive review, skepticism remains due to past controversies such as Dual EC DRBG and mixed signals on ECC.[56] To maintain resilience amid evolving threats and emerging insights, security tools must be designed to accommodate algorithm substitution and multi-algorithm configurations by default, ensuring adaptability remains integral to cryptographic defense.

Regulatory momentum is also accelerating. Financial regulators in the EU and the U.S. are already requesting cryptographic impact assessments. Similarly, healthcare compliance frameworks are beginning to include cryptographic life-cycle considerations. These pressures further validate the use of multi-dimensional scorecards like the CTA model, which aid both operational triage and regulatory reporting. With this context in mind, cybersecurity vendors must embed support for short-lived certificates, Cryptographic Bills of Materials (CBOM) generation, and automated compliance reporting across toolsets.

CAPABILITIES THE INDUSTRY MUST DELIVER

To bridge readiness gaps, cybersecurity vendors should prioritize the following capabilities:

- **Certificate infrastructure evolution:** With hybrid, composite, and chameleon certificate formats now included in X.509, tooling must support deployment and validation across TLS, VPN, and identity platforms.

- **Seamless Key Management System (KMS) modernization:** Post-quantum transitions will demand flexible KMS and Hardware Security

55 Note: Small and Medium Enterprises (SMEs) are not a discrete sector but span across all others, including finance, healthcare, and critical infrastructure. Their categorization here reflects resource-specific limitations that amplify baseline sectoral challenges.

56 Gable, Jim, Shannon Gray, and Denis Mandich. 2023. "Is PQC Broken Already? The Break of a NIST Finalist." Cloud Security Alliance. April 3, 2023. https://cloudsecurityalliance.org/blog/2023/04/03/is-pqc-broken-already-implications-of-the-successful-break-of-a-nist-finalist.

Module (HSM) support for new algorithms like Kyber and Dilithium, including within Continuous Integration/Continuous Deployment (CI/CD) environments and secure enclave architectures.

- **Modular crypto interfaces:** Software and Software Development Kits (SDKs) must support dynamic algorithm negotiation and modular cryptographic abstraction. Fixed key sizes and hard-coded schemes are future liabilities.
- **Cryptographic supply chain insights:** Visibility into cryptographic dependencies must extend beyond the enterprise to encompass third-party libraries, vendor APIs, and firmware components.
- **Threat detection tuned for HNDL:** Behavioral analytics and telemetry platforms should be updated to detect large-scale encrypted data exfiltration, a potential signal of Harvest Now, Decrypt Later strategies.

Additionally, vendors should contribute to developing and operationalizing quantum-readiness metrics and preparedness indicators. Given the uncertainty surrounding quantum timelines, defensible risk management requires the ability to quantify exposure and benchmark progress. This includes:

- **Quantum Volume Threshold Mapping:** Security platforms should track quantum hardware benchmarks, such as IBM's Quantum Volume or superconducting qubit coherence threshold, as contextual indicators of cryptographic risk relevance.
- **PQC Adoption Telemetry:** Vendors should report deployment metrics (e.g., PQC-enabled TLS sessions, hybrid cert usage rates) to create longitudinal baselines across sectors.
- **Readiness Scorecards:** Integrating crypto-agility maturity models into enterprise dashboards will help quantify posture across inventory, modularity, governance, and vendor resilience.
- **Warning Thresholds:** Define concrete cryptographic exposure thresholds—e.g., percent of non-agile key infrastructure remaining—as triggers for accelerated response plans.
- **Industry-wide Transparency Benchmarks:** Encourage public reporting or anonymized aggregation of PQC readiness metrics to support cross-sector benchmarking, similar to existing practices in vulnerability disclosure or patching cadence.

These readiness indicators are not abstract diagnostics—they are early warning systems. By embedding multi-dimensional maturity metrics into operations, vendors enable measurable, sector-specific progress that scales across public and private environments.

OPPORTUNITIES BEYOND DEFENSE

While much of the quantum security discourse rightly focuses on the risk posed by quantum computing to cryptography, it is equally essential to highlight the strategic opportunities quantum technologies offer cybersecurity providers. When strategically integrated, quantum technologies can enhance cryptographic strength, advance threat detection, and catalyze security innovation across sectors.

QUANTUM-BACKED TRUST INFRASTRUCTURE

Emerging solutions like Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG) create new foundations for digital trust. While scalability remains challenging, QKD offers physics-based eavesdropping detection, a feature particularly relevant for sectors requiring prolonged confidentiality and high-integrity communications. QRNGs, meanwhile, generate entropy from quantum noise, offering genuine unpredictability. Replacing

flawed pseudo-random generators with QRNGs eliminates a historically exploited weakness across cryptographic systems.[57] Vendors that embed certified QRNGs into hardware security modules, secure communications platforms, and key management systems will gain trust advantages with high-assurance buyers.[58]

QUANTUM-ENHANCED DETECTION AND RESPONSE

Quantum computing also opens new frontiers in detection and analytics. Quantum-enhanced machine learning has the potential to process complex, multidimensional data patterns faster and more accurately than classical systems.[59] While still experimental, quantum algorithms could significantly improve anomaly detection, threat attribution, and adversary behavior modeling.[60] As attackers increasingly leverage AI for stealthy operations, quantum-enhanced defenses may offer an effective counter.

Vendors investing early in quantum-driven threat detection will be positioned to lead an emerging tier of autonomous, adaptive cybersecurity tools. Quantum-enriched SIEM systems may, for example, identify suspicious bulk encrypted traffic patterns that classical systems overlook—an essential signal for detecting HNDL strategies.[61]

PQC AS A STRATEGIC ENABLER, NOT JUST A RISK MITIGATOR

Leading cybersecurity companies are already implementing hybrid cryptographic schemes (e.g., combining CRYSTALS-Kyber with classical algorithms) in TLS, VPN, and messaging protocols.[62] This shift creates an opportunity to re-architect cryptographic infrastructure with resilience and agility built in.

Tools that support hybrid X.509 certificates, chameleon certificate extensions, and modular key management APIs are becoming market differentiators. Providers who offer agile, multi-algorithm platforms, including pre-integrated PQC in OpenSSL and OpenSSH, will not only meet evolving standards, but define best practices. They can also develop service lines in PQC certification, cryptographic bill of materials (CBOM) generation, and secure algorithm rotation.

QUANTUM ADVANTAGE AS A MARKET DIFFERENTIATOR

Quantum-enabled cybersecurity capabilities should be framed not only as defensive responses, but as avenues for market leadership and strategic alignment. As PQC adoption remains slow across the market (e.g., less than 0.03% of OpenSSH sessions currently use PQC), early adopters can

57 Corrigan-Gibbs, Henry, Wendy Mu, Dan Boneh, and Bryan Ford. 2013. “Ensuring High-Quality Randomness in Cryptographic Key Generation.” Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS ’13, 685–96. https://doi.org/10.1145/2508859.2516680; Palo Alto Networks. 2015. “What Is a Quantum Random Number Generator (QRNG)?” Palo Alto Networks. 2015. https://www.paloaltonetworks.com/cyberpedia/what-is-a-quantum-random-number-generator-qrng.

58 Ibid.

59 Yocam, Eric, Anthony Rizi, Mahesh Kamepalli, Varghese Vaidyan, Yong Wang, and Gurcan Comert. 2024. “Quantum Adversarial Machine Learning and Defense Strategies: Challenges and Opportunities.” ArXiv.org. 2024. https://arxiv.org/abs/2412.12373v1.

60 Moure-Garrido, Marta, Celeste Campo, and Carlos Garcia-Rubio. 2023. “Real Time Detection of Malicious DoH Traffic Using Statistical Analysis.” Computer Networks 234 (June): 109910–10. https://doi.org/10.1016/j.comnet.2023.109910.

61 Ibid.

62 National Institute of Standards and Technology (NIST). "NIST Releases the First 3 Finalized Post-Quantum Encryption Standards." National Institute of Standards and Technology, August 2024. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards; Fedorov, Aleksey K. 2023. “Deploying Hybrid Quantum-Secured Infrastructure for Applications: When Quantum and Post-Quantum Can Work Together.” Frontiers in Quantum Science and Technology 2 (April). https://doi.org/10.3389/frqst.2023.1164428.

signal leadership and readiness. Firms that embed quantum-enabled capabilities today—whether through entropy validation, quantum-proof communication layers, or enhanced detection—will become trusted suppliers to security-conscious sectors and governments.

STRATEGIC ROADMAP

Quantum resilience will not come from a single product or one-time fix. Instead, it will come from a phased, systemic shift across technologies, governance structures, and market behaviors. Cybersecurity providers should enable this shift in the digital ecosystem by taking a series of near-term (2026) and medium-term (2030) actions, anchored in readiness metrics and sector collaboration.

A critical component of any strategic roadmap is planning for a phased, manageable approach to post-quantum cryptographic (PQC) adoption. The InterNetX guide on quantum readiness for future-proof security highlights two particularly pragmatic strategies.[63] First, organizations should implement hybrid encryption systems, which combine traditional and quantum-safe algorithms to reduce migration risk. This method enables gradual transition—prioritizing outdated or mission-critical cryptographic infrastructure—rather than attempting a full organizational overhaul in one effort. It helps reduce the inertia often associated with the "titanic task" of quantum migration.

Second, the roadmap must include continuous standards monitoring. As NIST continues refining its post-quantum cryptographic recommendations, staying current ensures that implementations remain aligned with evolving security expectations. It is important not to assume that today's standards will remain static for the next decade. Organizations that build in flexibility to adapt to future updates will be best positioned for long-term resilience.

With these principles—and others identified throughout this report—in mind, the CTA working group has distilled a set of practical objectives aligned to the Cryptographic Agility Maturity Scorecard. These objectives reflect a synthesis of industry best practices, expert recommendations, and real-world implementation insights. Together, they provide a phased pathway for organizations to begin or accelerate their post-quantum readiness efforts.

SHORT-TERM OBJECTIVES: WHAT YOU SHOULD DO TODAY

The first technical readiness milestone is cryptographic inventory visibility. Planning migration efforts is impossible without comprehensive knowledge of where cryptography is embedded in applications, network protocols, embedded systems, and third-party integrations. Cybersecurity providers should help organizations establish dynamic cryptographic bills of materials (CBOMs) that are continuously updatable as systems evolve.

The second milestone is crypto-agile architecture deployment. Legacy systems with hard-coded cryptographic algorithms must be replaced to use modular, swappable cryptographic components. Applications, APIs, and protocol stacks should support flexible algorithm negotiation, hybrid cryptographic schemes, and rapid failover to alternative protocols if vulnerabilities are discovered.

The third milestone is post-quantum pilot implementations. Before large-scale migrations, organizations should select a subset of critical systems (e.g., VPN gateways, email encryption platforms, secure communication tunnels) to implement hybrid post-quantum cryptography using NIST-selected candidate algorithms. Pilot

63 Berrisford, Natalie. 2024. "Quantum Readiness. For Future-Proof Security." Snapshot Hub by InterNetX. July 30, 2024. https://snapshot.internetx.com/en/quantum-readiness-for-future-proof-security/

deployments provide practical feedback on performance, compatibility, and operational integration challenges.

Finally, cybersecurity providers should help organizations modernize their cryptographic key and certificate management processes. Key management systems (KMS), certificate authorities (CAs), and device identity infrastructures must be updated to support post-quantum key formats and signature schemes, ensuring that the chain of trust across ecosystems remains unbroken through the quantum transition.

Each of these milestones aligns to specific readiness "states" reflected in the Cryptographic Agility Scorecard. Organizations that meet these objectives before adversaries achieve operational quantum capabilities will secure a durable advantage in risk mitigation and operational trust.

MEDIUM-TERM OBJECTIVES: WHAT YOU SHOULD DO TOMORROW

Cryptographic transitions resemble past infrastructure shifts like IPv6 adoption: slow, uneven, and often delayed by cost and inertia despite long-term necessity. Planning must account for extended dual-stack periods and the persistence of legacy dependencies. By 2030, quantum readiness must evolve into quantum resilience, which would include:

- **Full Cryptographic Agility Across Critical Systems:** All major applications, services, and device infrastructures should be capable of algorithm swaps without system redesigns. Protocols must support hybrid and PQC-only configurations.

- **Post-Quantum Algorithm Migration Completed for Tier 1 Assets:** Systems handling sensitive data with long retention periods (classified communications, customer financial records, healthcare data, intellectual property archives) must have transitioned to NIST-selected post-quantum algorithms.

- **Crypto-Agility Governance Fully Operationalized:** Migration to new cryptographic standards should become a standard operational capability, managed by risk management and IT security governance structures.

- **Vendor Ecosystem Quantum-Ready:** Procurement policies should mandate that suppliers, cloud providers, and technology partners support PQC standards and provide evidence of compliance.

- **Zero-Trust Architectures Revalidated for Quantum Threats:** Zero-trust models must account for quantum-era authentication vulnerabilities, and quantum-resilient identity, authentication, and encryption layers must be deployed. Quantum-resilient credentials and identity mechanisms must become baseline.

Achieving these benchmarks ensures that organizations are not merely reacting to quantum threats but proactively shaping a defensive environment where adversaries cannot exploit cryptographic lag. These objectives should be tracked using scorecard-aligned milestones and readiness indicators.

CROSS-SECTOR COLLABORATION AND SUPPLY CHAIN DEPENDENCIES

Quantum resilience cannot be achieved in isolation. Most enterprises are embedded within intricate supply chains, cloud ecosystems, telecommunications infrastructures, and regulatory frameworks. Collaboration across sectors and supply chains is essential to ensure that quantum migration is synchronized and systemic.

- **Cloud providers** must integrate post-quantum cryptographic support into standard services. Organizations must demand and verify that cloud-hosted data stores, API endpoints,

authentication gateways, and edge services adopt hybrid or PQC-only modes within defined timelines.

- **Telecommunications providers** (Telcos) must upgrade backbone authentication protocols (e.g., DNSSEC, BGP security extensions) to prevent quantum-vulnerable interception attacks. Sector-level standards and coordinated rollouts will be necessary to avoid fragmentation and interoperability failures.

- **Original Equipment Manufacturers** (OEMs) must retrofit or redesign device firmware, embedded systems, and industrial control technologies to support post-quantum cryptographic operations. Enterprises should insist on PQC compliance as a baseline in RFPs and procurement agreements.

- **Industry consortia** must influence interoperability standards, reduce transition friction, and protect critical dependencies from becoming systemic vulnerabilities.

- **Supply chain visibility tools** must also evolve to track the cryptographic posture of third-party vendors, enabling proactive risk management in a quantum-computing world.

Effective quantum resilience will not stem from the accuracy of predictions, but from the maturity of preparation. Early movers will gain technical resilience, regulatory credibility, customer trust, and market differentiation.

CONCLUSION

Quantum computing introduces a complex, accelerating risk that cybersecurity leaders must manage with foresight, discipline, and agility. The challenge ahead will not be defined by a sudden Q-Day event, but rather by a creeping erosion of today's cryptographic security, amplified by adversaries increasingly investing in long-term decryption capabilities, regardless of sophistication level.

Organizations that act early will reduce their exposure to cryptographic compromise and lead the next era of trust. They will earn reputational and regulatory advantages. Cybersecurity providers that act early will shape the standards that others adopt and have the chance to become market leaders. They will also avoid the cost of outdated crypto systems becoming silent liabilities.

Distrust of standardization authorities—whether due to past controversies like Dual EC DRBG or broader governance concerns—must not justify delay. Schneier's Law reminds us that all cryptography is ultimately provisional. What matters most is the ability to pivot quickly, transparently, and at scale when assumptions break.

The mandate for cybersecurity professionals and vendors alike is clear: don't wait to be convinced. Build cryptographic agility as a default. Monitor for quantum-exploitable weak points in systems and supply chains. Security consumers should push vendors to deliver post-quantum roadmaps and pilot real-world deployments, especially in infrastructure that protects long-lived, high-value data. Security providers should normalize agility as a baseline capability—not a premium feature.

Taking the steps outlined in this report won't eliminate the quantum threat. But they will dramatically improve preparedness, reducing friction in the years ahead and insulating the digital ecosystem from surprise.

The post-quantum cryptography era does not start at a single moment in time.

It is incremental, already unfolding, and unevenly distributed.

The only question left is who will be ready.

REFERENCES

"Post-Quantum Cryptography (PQC) - Challenges and Obstacles to Adoption | IDEMIA." 2025. IDEMIA. February 26, 2025. https://www.idemia.com/insights/key-obstacles-post-quantum-cryptography-pqc-adoption

"S3SSE2A: Hardware PQC Locks in Security for the Quantum Era." 2025. Samsung Semiconductor USA. March 4, 2025. https://semiconductor.samsung.com/us/news-events/tech-blog/s3sse2a-hardware-pqc-locks-in-security-for-the-quantum-era/

"The First Step to a Quantum-Ready Future with Samsung Knox." 2025. Samsung.com. 2025. https://news.samsung.com/ca/the-first-step-to-a-quantum-ready-future-with-samsung-knox

Alder, Madison. 2024. "Cyber Officials Cite Legacy Systems as Post-Quantum Readiness Challenge." FedScoop. October 16, 2024. https://fedscoop.com/cyber-officials-cite-legacy-systems-as-post-quantum-readiness-challenge/

Alliance for Telecommunications Industry Solutions (ATIS). Strategic Framework for Crypto Agility and Quantum Risk Assessment. ATIS-I-0000098, January 2024. https://atis.org/resources/strategic-framework-for-crypto-agility-and-quantum-risk-assessment/

Apple Security Engineering and Architecture (SEAR). 2024. "IMessage with PQ3: The New State of the Art in Quantum-Secure Messaging at Scale - Apple Security Research." Apple Security. February 21, 2024. https://security.apple.com/blog/imessage-pq3/

Chen, Lily. 2025. "Considerations for Achieving Cryptographic Agility": https://doi.org/10.6028/nist.cswp.39.ipd

Chen, Sophia. 2025. "Drama over Quantum Computing's Future Heats Up." The Verge. March 21, 2025. https://www.theverge.com/tech/633248/beyond-the-hype-of-quantum-computers

"Cloudflare Named Winner of the 2024 DigiCert Quantum Readiness Award." 2024. Digicert.com. December 19, 2024. https://www.digicert.com/news/digicert-announces-quantum-readiness-award-winner

Corrigan-Gibbs, Henry, Wendy Mu, Dan Boneh, and Bryan Ford. 2013. "Ensuring High-Quality Randomness in Cryptographic Key Generation." Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS '13, 685–96. https://doi.org/10.1145/2508859.2516680

CyberArk Software. 2024. Organizations Largely Unprepared for the Advent of Shorter than 90-Day TLS Certificates. Research Report. CyberArk Software. https://www.cyberark.com/resources/white-papers/organizations-largely-unprepared-for-the-advent-of-90-day-tls-certificates

Cybersecurity and Infrastructure Security Agency, Post-Quantum Considerations for Operational Technology (October 2024), https://www.cisa.gov/sites/default/files/2024-10/Post-Quantum%20Considerations%20for%20Operational%20Technology%20%28508%29.pdf

Daniel, Brett. 2023. "Symmetric vs. Asymmetric Encryption: What's the Difference?" Trentonsystems.com. Trenton Systems, Inc. September 25, 2023. https://www.trentonsystems.com/en-gb/blog/symmetric-vs-asymmetric-encryption

Eby, Kate. 2022. "IT Maturity Models, Scorecards & Assessments | Smartsheet." Smartsheet. March 9, 2022. https://www.smartsheet.com/content/it-maturity?srsltid=AfmBOormXhvn85ZuiLiydn8XR1cNJJvAQg5sr6QuTCHQfAe3BAbRyva8

Fedorov, Aleksey K. 2023. "Deploying Hybrid Quantum-Secured Infrastructure for Applications: When Quantum and Post-Quantum Can Work Together." Frontiers in Quantum Science and Technology 2 (April). https://doi.org/10.3389/frqst.2023.1164428

Financial Services Information Sharing and Analysis Center (FS-ISAC). Building Cryptographic Agility in the Financial Sector. October 2024. https://www.fsisac.com/pqc-crypto-agility

Gable, Jim, Shannon Gray, and Denis Mandich. 2023. "Is PQC Broken Already? The Break of a NIST Finalist." Cloud Security Alliance. April 3, 2023. https://cloudsecurityalliance.org/blog/2023/04/03/is-pqc-broken-already-implications-of-the-successful-break-of-a-nist-finalist

Gambetta, Jay. 2023. "IBM Quantum System Two: The Era of Quantum Utility Is Here | IBM Quantum Computing Blog." IBM. December 4, 2023. https://www.ibm.com/quantum/blog/quantum-roadmap-2033

Giles, Martin. 2019. "Explainer: What Is a Quantum Computer?" MIT Technology Review. January 29, 2019. https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/

Green, Matthew. 2013. "The Many Flaws of Dual_EC_DRBG." A Few Thoughts on Cryptographic Engineering. September 18, 2013. https://blog.cryptographyengineering.com/2013/09/18/the-many-flaws-of-dualecdrbg/

Grover, Lov K. 1996. "A Fast Quantum Mechanical Algorithm for Database Search." Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing - STOC '96, 212–19. https://doi.org/10.1145/237814.237866

Harishankar, Ray, Michael Osborne, Jai Arun, John Buselli, and Jennifer Janechek. 2024. "Crypto-Agility and Quantum-Safe Readiness | IBM Quantum Computing Blog." IBM. June 19, 2024. https://www.ibm.com/quantum/blog/crypto-agility

Help Net Security. 2025. "OpenSSL Prepares for a Quantum Future with 3.5.0 Release - Help Net Security." Help Net Security. April 9, 2025. https://www.helpnetsecurity.com/2025/04/09/openssl-3-5-0-released/

Hiremath, Omkar. 2021. "Introduction to Cryptographic Failures | USA." Software Secured. 2021. https://www.softwaresecured.com/post/introduction-to-cryptographic-failures

Hohm, Julian, Andreas Heinemann, and Alexander Wiesmaier. 2023. "Towards a Maturity Model for Crypto-Agility Assessment." Lecture Notes in Computer Science, January, 104–19. https://doi.org/10.1007/978-3-031-30122-3_7

InfoSec Global. AgileSec™ Analytics Cryptographic Scorecard. June 2023. https://www.infosecglobal.com/posts/agilesec-analytics-cryptographic-scorecard

Ivezic, Marin. 2022. "Mitigating Quantum Threats beyond PQC." PostQuantum - Quantum Computing, Quantum Security, PQC. September 2022. https://postquantum.com/post-quantum/mitigating-quantum-threats-pqc/

Kunz, Dr Christopher. 2025. "OpenSSH 10 Relies on Standards for Quantum-Safe Key Exchange." Security, April. https://heise.de/-10346176

LaMacchia, Brian, and John Manferdelli. 2006. "New Vistas in Elliptic Curve Cryptography." Inf. Secur. Tech. Rep. 11 (December): 186–92. https://www.microsoft.com/en-us/research/publication/new-vistas-in-elliptic-curve-cryptography/

Langner, Ralph. 2011. "Stuxnet: Dissecting a Cyberwarfare Weapon." IEEE Security & Privacy 9 (3): 49–51. https://doi.org/10.1109/msp.2011.67

Mantas, Georgios, Firooz Saghezchi, Jonathan Rodriguez, and Victor Sucasas. 2024. Security and Privacy for 6G Massive IoT. John Wiley & Sons. https://www.usenix.org/conference/usenixsecurity21/presentation/meijer

Martinis, John. 2019. "Quantum Supremacy Using a Programmable Superconducting Processor." Research.google. October 23, 2019. https://research.google/blog/quantum-supremacy-using-a-programmable-superconducting-processor/

Miele, Andrea. 2015. "On the Analysis of Public-Key Cryptologic Algorithms," January. https://doi.org/10.5075/epfl-thesis-6603

Morrison, Ryan. 2022. "IBM Quantum Computer Could Reach 4,000 Qubits by 2025." Tech Monitor. November 9, 2022. https://www.techmonitor.ai/technology/emerging-technology/ibm-quantum-supercomputer

Moure-Garrido, Marta, Celeste Campo, and Carlos Garcia-Rubio. 2023. "Real Time Detection of Malicious DoH Traffic Using Statistical Analysis." Computer Networks 234 (June): 109910–10. https://doi.org/10.1016/j.comnet.2023.109910

Mueller, Moritz, Jins De Jong, Maran Van Heesch, Benno Overeinder, and Roland Van Rijswijk-Deij. 2020. "Public Review for Retrofitting Post-Quantum Cryptography in Internet Protocols: A Case Study of DNSSEC." ACM SIGCOMM Computer Communication Review. https://conferences.sigcomm.org/sigcomm/2021/files/papers/3431832.3431838.pdf

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

National Institute of Standards and Technology (NIST). Considerations for Achieving Crypto Agility: Strategies and Practices. NIST CSWP 39 (IPD), March 2025. https://doi.org/10.6028/NIST.CSWP.39.ipd

National Institute of Standards and Technology (NIST). Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms. NIST CSWP 04282021, April 2021. https://doi.org/10.6028/NIST.CSWP.04282021

National Security Agency. 2024. "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ." Cybersecurity Information Sheet, U/OO/194427-22 | PP-24-4014, Version 2.1, December 2024. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

Olaoye, Godwin. "Quantum Key Distribution (QKD) and the Future of Secure Communications." Sage Advance. Last modified April 2025. https://advance.sagepub.com/doi/full/10.22541/au.174431281.12939966/v1

Palo Alto Networks. 2015. "What Is a Quantum Random Number Generator (QRNG)?" Palo Alto Networks. 2015. https://www.paloaltonetworks.com/cyberpedia/what-is-a-quantum-random-number-generator-qrng

Palo Alto Networks. 2015. "What Is UEBA (User and Entity Behavior Analytics)?" Palo Alto Networks. 2015. https://www.paloaltonetworks.com/cyberpedia/what-is-user-entity-behavior-analytics-ueba

Ricchizzi, Nino, Christian Schwinne, and Jan Pelzl. 2025. "Applied Post Quantum Cryptography: A Practical Approach for Generating Certificates in Industrial Environments." ArXiv.org. 2025. https://arxiv.org/abs/2505.04333v1

Scarani, Valerio, and Christian Kurtsiefer. 2025. "The Black Paper of Quantum Cryptography: Real Implementation Problems." ArXiv.org. 2025. https://arxiv.org/abs/0906.4547

Schneider, Josh, and Ian Smalley. 2024. "Quantum Computing." Ibm.com. August 5, 2024. https://www.ibm.com/think/topics/quantum-computing

Schneider, Josh, and Ian Smalley. 2024. "Qubit." Ibm.com. February 28, 2024. https://www.ibm.com/think/topics/qubit

Schneier, Bruce. 1998. "Crypto-Gram." Schneier on Security. October 15, 1998. https://www.schneier.com/crypto-gram/archives/1998/1015.html#cipherdesign

Shor, P.W. 2002. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," December, 124–34. https://doi.org/10.1109/sfcs.1994.365700

Silvestri, Riccardo. 2020. "Business Value of Quantum Computers: Analyzing Its Business Potentials and Identifying Needed Capabilities..." ResearchGate. unknown. August 16, 2020. https://www.researchgate.net/publication/343683519_Business_Value_of_Quantum_Computers_analyzing_its_business_potentials_and_identifying_needed_capabilities_for_the_healthcare_industry

Sowa, Jakub, Bach Hoang, Advaith Yeluru, Steven Qie, Anita Nikolich, Ravishankar Iyer, and Phuong Cao. 2024. "Post-Quantum Cryptography (PQC) Network Instrument: Measuring PQC Adoption Rates and Identifying Migration Pathways." ArXiv.org. 2024. https://arxiv.org/abs/2408.00054

Sowa, Jakub, Bach Hoang, Advaith Yeluru, Steven Qie, Anita Nikolich, Ravishankar Iyer, and Phuong Cao. 2024. "Post-Quantum Cryptography (PQC) Network Instrument: Measuring PQC Adoption Rates and Identifying Migration Pathways." ArXiv.org. 2024. https://arxiv.org/abs/2408.00054

The Biden White House. 2022. "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems | the White House." The Biden White House. May 4, 2022. https://bidenwhitehouse.archives.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/

Townsend, Kevin. 2025. "Cyber Insights 2025: Quantum and the Threat to Encryption." SecurityWeek. February 3, 2025. https://www.securityweek.com/cyber-insights-2025-quantum-and-the-threat-to-encryption/

Westerbaan, Bas. 2024. "The State of the Post-Quantum Internet." The Cloudflare Blog. March 5, 2024. https://blog.cloudflare.com/pq-2024/

Wheeler, Andrew. 2019. "IBM Achieves Highest Quantum Volume to Date - Engineering.com." Engineering.com. March 4, 2019. https://www.engineering.com/ibm-achieves-highest-quantum-volume-to-date/

Yassein, Muneer Bani, Shadi Aljawarneh, Ethar Qawasmeh, Wail Mardini, and Yaser Khamayseh. 2017. "Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms." 2017 International Conference on Engineering and Technology (ICET), August, 1–7. https://doi.org/10.1109/icengtechnol.2017.8308215

Yocam, Eric, Anthony Rizi, Mahesh Kamepalli, Varghese Vaidyan, Yong Wang, and Gurcan Comert. 2024. "Quantum Adversarial Machine Learning and Defense Strategies: Challenges and Opportunities." ArXiv.org. 2024. https://arxiv.org/abs/2412.12373v1

Zetter, Kim. 2013. "How a Crypto 'Backdoor' Pitted the Tech World against the NSA." WIRED. September 24, 2013. https://www.wired.com/2013/09/nsa-backdoor/

APPROACHING QUANTUM DAWN:

CLOSING THE CYBERSECURITY READINESS GAP BEFORE IT'S TOO LATE

2025

CYBER THREAT ALLIANCE

POWERED BY THE CTA