McKinsey Quarterly

Risk & Resilience Practice

Quantum is almost here: Are you and your systems ready?

The biggest cyberthreat in history is already a reality. Here's an effective approach for securing data and intellectual property, future-proofing digital infrastructures, and mitigating risk.

This article is a collaborative effort by Charlie Lewis, Henning Soller, and Sebastian Schneider, with Joana Candina and Martina Gschwendtner, representing views from the Risk & Resilience Practice.

April 2026

For most people, the 2030s probably feel like a lifetime away. For those preparing for Q-Day, the clock is ticking much, much faster.

Q-Day is the point at which sensitive data and IP—and the cryptographic mechanisms that underpin digital trust—could be breached by algorithm-breaking quantum computers. Many believe it will emerge in the 2030s or sooner.

Four or five years may seem like plenty of time for leaders to develop a plan for addressing this cyberthreat. But industry experts and standards bodies say that if organizations don't study the risks and update their cybersecurity road maps *right now*, it may already be too late.

— The National Institute of Standards and Technology has recommended that organizations begin applying its new postquantum cryptography (PQC) standards.[1]

— The UK National Cyber Security Centre has issued target dates for organizations' migration to PQC through 2035, acknowledging that this massive technology shift will take several years—potentially a decade or more.[2]

— Companies' migration to PQC will be complicated given existing cryptography and standards, third-party dependencies, and system life cycles.

— Existing data and IP may already be at risk if they are harvested today for decrypting, once quantum capabilities mature.

Clearly, waiting for definitive proof of vulnerability from quantum is a high-risk strategy. And yet, research from Trusted Group Computing shows that just *over 90 percent of global businesses still lack a road map* for dealing with quantum cybersecurity threats.[3]

Short of bending the space-time continuum, how can companies catch up? Our experience suggests that corporate risk and cybersecurity teams and their providers will need to focus on more than just technology; they will need to enact structural changes in how they prioritize and organize themselves to tackle the PQC transition.

Specifically, companies must answer three core questions: Which parts of our technology infrastructure support our most critical business processes, and which of those are under the most threat from Q-Day? Given that assessment of potential risk, how should we prioritize postquantum migration plans (that is, which parts to upgrade and which to replace entirely) before Q-Day is knowable? And last, but not least, what governance model should the chief information officer or chief information security officer establish now to preserve trust in identities, certificates, and software updates during the transition? The mandate is to assess, prioritize, and reset the architecture.

In this article, we first look at the rapidly growing quantum market as well as three domains most at risk of disruption from quantum: the long-term confidentiality of data and communications,

[1] Gina Scinta, "NIST's quantum standards: The time for upgrades is now," Federal News Network, November 19, 2024.
[2] "Timelines for migration to post-quantum cryptography," NCSC, March 20, 2025.
[3] "91% of businesses do not have a roadmap in place to protect against quantum threats, finds industry survey," Trusted Computing Group, December 2, 2025.

the integrity of digital trust mechanisms, and cryptographic invisibility and accumulated technical debt. We then offer some suggestions for addressing those risks and building quantum resilience in organizations.

What's becoming increasingly clear is that quantum can no longer be positioned solely as a technical concern; it must be a leadership priority—and the time to act is now. Companies that wait to address their quantum concerns will almost certainly experience higher migration costs, a greater likelihood of disrupted operations, and less flexibility in managing this critical technical transition.

The quantum market: Fast growth; a new tech boom

Several trends point to the ongoing development of a robust market for quantum computing in the United States and elsewhere:

— *Investors:* Based on the accelerated investment in quantum technology start-ups between 2024 and 2025, confidence in the commercial viability and scaling potential of quantum technologies seems to be growing. Such investments grew from $2 billion in 2024 to $13 billion in 2025, according to our research—a sixfold increase year over year. More than 90 percent of total investment is concentrated in quantum computing hardware, systems, and enabling technologies.

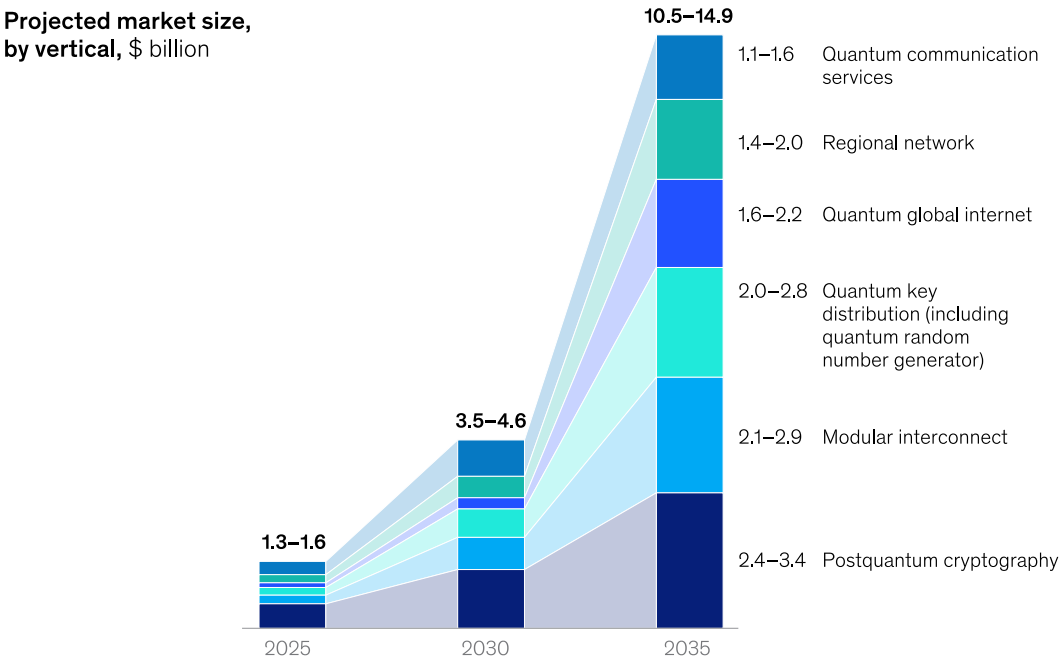
— *Key verticals:* Given their role in enabling scalable, quantum-safe infrastructure, we expect PQC and modular connectors to emerge as the largest of the quantum communication verticals by 2035 (Exhibit 1).

  Indeed, our research shows that by 2035, the market for PQC is projected to reach between $2.4 billion and $3.4 billion before leveling off as the market matures. Meanwhile, the market for modular connectors, or the mechanisms that enable interfaces between phone systems, data networks, and other systems, is still developing but is forecast to be between $2.1 billion and $2.9 billion, driven by assumed technological breakthroughs that will enable higher scalability and performance.

  Other verticals are also likely to grow meaningfully over the next five to ten years, including quantum key distribution (QKD) and related quantum random number generator technology, regional quantum networks, and the quantum global internet.

Exhibit 1

Postquantum cryptography and modular interconnects are projected to have the largest market size across verticals by 2035.



Note: Median values plotted in chart.

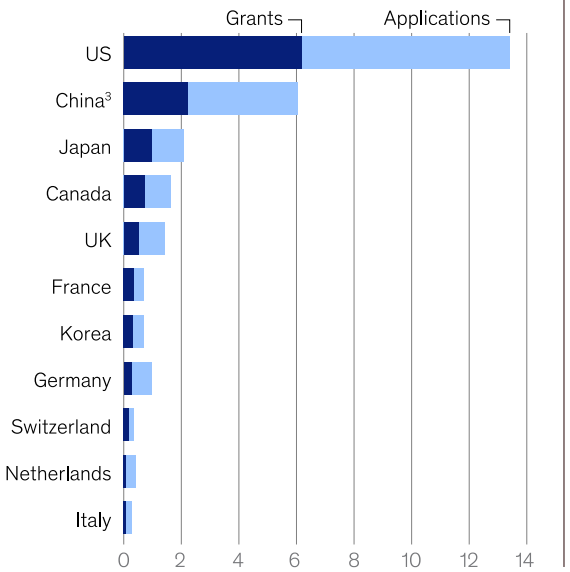
McKinsey & Company

— *Innovation:* Quantum innovation to date has been concentrated in just a few countries, led by China and the United States. In fact, over the past few years, those two countries have accounted for roughly 70 percent of global patent applications. The United States has been granted the most patents, while China leads in global research publications (Exhibit 2).

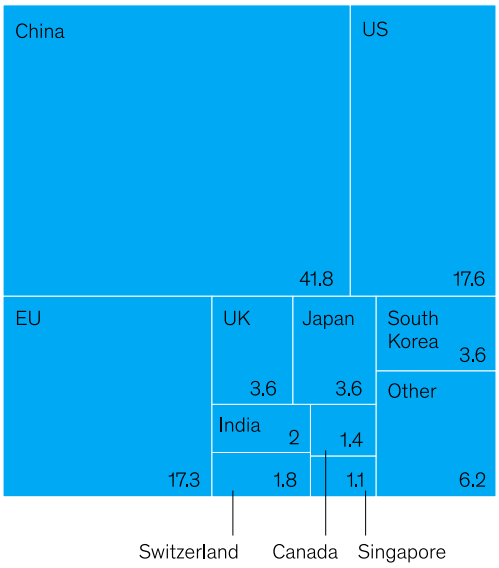
Exhibit 2

The United States and China lead in both quantum communication patents granted and share of scientific publications released.

Quantum communication patent applications and grants, by HQ country,[1] 2000–24, thousand



Share of quantum communication scientific publications,[2] 2024, %



Note: The number of granted patents in 2024 is not fully complete due to the time it takes to publish patents.
[1]The approved outcome of a patent application, giving the inventor exclusive legal rights. Only granted patents are legally recognized and enforceable in the industry. HQ refers to headquarters country.
[2]Data reflects authors from a country's research institutions contributing to publications in the physical sciences, based on share of publications, which is a fractional measure that splits credit among coauthoring institutions. Includes publications from Jan 1, 2024, to Dec 31, 2024.
[3]China's current patent activity does not accurately reflect the ongoing efforts in patent applications aimed at gaining market access.
Source: Nature Index; PatSnap, retrieved Mar 2025

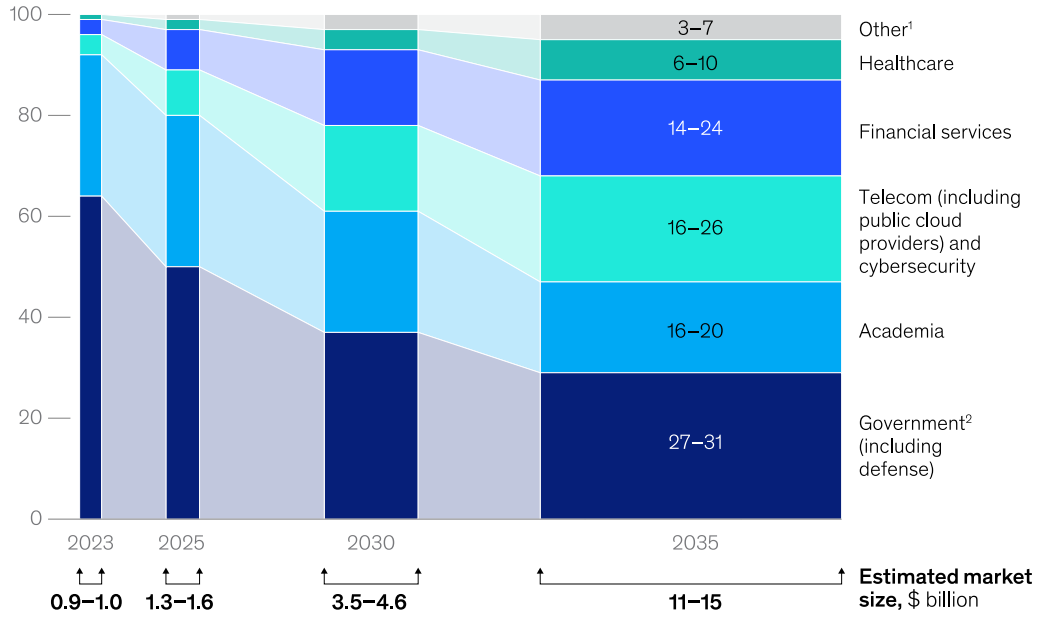
McKinsey & Company

— *Commercial customers:* The quantum communications market sits at the intersection of cybersecurity, national security, and next-generation infrastructure. While governments anchor the market today, we anticipate that future growth will come from the telecommunications and financial-services sectors. Our research shows that the overall quantum communication market is projected to reach between $11 billion and $15 billion by 2035 (Exhibit 3).

Exhibit 3

The quantum communications market is projected to reach $11 billion to $15 billion by 2035.

Market breakdown, by customer type, %



Note: Median values plotted in chart.
[1]Includes manufacturing, automative, insurance, etc.
[2]Includes civil government and defense.
Source: Expert interviews; press search; McKinsey analysis

McKinsey & Company

Government organizations, including defense-related ones, currently account for between 48 percent and 52 percent of the total market for quantum communications, reflecting these early adopters' focus on national security and critical infrastructure needs. Academia accounts for 28 percent to 32 percent of the market, driven by research-based deployments in schools and universities. But over time, our research shows, market share will shift to commercial players (see sidebar, "What quantum risk means for your industry").

Telecom operators are expected to see the strongest increase in market share for quantum communications, growing from between 2 and 6 percent in 2023 to between 16 and 26 percent by 2035. The rollout of quantum networks and integration with public cloud and cybersecurity offerings will compel this growth. Financial-services organizations will likely become another set of power users: We project this sector will account for between 14 percent and 24 percent of market share by 2035, as institutions seek quantum-safe communication for high-value transactions.

What quantum risk means for your industry

Quantum exposure is universal, but where it bites first will vary. In financial services, the primary risk is transaction integrity; forged digital signatures could undermine payment systems and market infrastructure. The priorities for organizations in this sector should be securing transaction validation, long-term financial records, and client data. In healthcare and pharmaceuticals, risk and cybersecurity teams must contend with threats to patient data, genomic data, and decades-long R&D assets, where long-term confidentiality is critical.

Infrastructure and manufacturing sectors use operational technology and industrial control systems that rely on trusted software updates and identity certificates. If trust is compromised here, expect to see significant physical disruption—potentially catastrophic. And, of course, quantum readiness is a national security imperative for government and defense players, given that sophisticated state actors are likely already harvesting encrypted communications.

Immediate areas of risk from quantum

The industry numbers and growth opportunities are promising, but quantum also presents significant cryptographic exposures for organizations. Most immediately, global businesses will need to shore up the confidentiality of data, trust mechanisms, and cryptographic foundations. Here's why.

Confidentiality of data and communications

Bad actors can already harvest encrypted data now and decrypt it later as quantum capabilities mature. So, current encryption protecting data in transit and at rest may no longer guarantee long-term privacy—thereby putting health and financial records, trade secrets, long-term contracts, and other proprietary business information in harm's way.

Integrity and trust

Digital signatures, identity systems, and processes for updating software all rely on public-key cryptography. If this assurance is weakened, attackers could impersonate trusted entities, manipulate transactions, or compromise software supply chains—undermining confidence in digital platforms and interactions. In this case, quantum could irrevocably destroy trust as much as it could disrupt systems.

Cryptographic inventory and technical debt

Many organizations lack a comprehensive inventory of where cryptography is embedded (including within legacy platforms and third-party solutions). The technology is already difficult to modify or replace; quantum only amplifies the operational risk of that "cryptographic blind spot," slowing migration and increasing the likelihood of rushed or incomplete transitions.

Three critical moves to build quantum resilience

To address these and future risks from quantum, cybersecurity and risk teams should target the following three critical actions. Doing so can help them maintain trust throughout the quantum transition and develop functional and organizational adaptability and resilience.

Move 1: Assess potential quantum risks and exposures—and prioritize the PQC transition accordingly

As pressured as they are, cyber and risk teams must take time to determine which assets and parts of the technology infrastructure are most at risk and prioritize the PQC transition accordingly. A simple but structured risk assessment can help organizations prioritize where to strengthen data protection. Four factors matter most: how long data needs to remain secure, how sensitive it is, how exposed it is, and how critical the supporting system is to the business.

Using these criteria, teams can focus first on the highest-risk assets—for example, long-lived customer records or intellectual property—rather than short-term operational data. Once priorities are clear, cyber and risk teams can phase in encryption upgrades alongside planned changes such as cloud migrations, system upgrades, or contract renewals. This can help reduce disruption while improving security.

Taking time to assess exposures is especially important for maintaining trust. For example, one global bank reviewed its trust infrastructure—including its public key infrastructure certificates and software—to understand where cryptography was critical for preserving transaction data, personally identifiable information, and other sensitive customer data. It mapped dependencies, assessed business impact, and developed a road map to replace tens of thousands of routers without disrupting operations.

Given how many breaches of trust originate outside the organization, cyber and risk teams should work closely with supply chain and third-party partners to ensure that they, too, are building quantum resilience. They should ask suppliers to explain how updates, identities, and transactions will remain trustworthy during cryptographic transitions, and they should embed trust-based language into contracts.

Move 2: Reset the architecture—and enable crypto agility

In instances where cryptography is tightly coupled with core functionality—such as hard-coded algorithms, bespoke implementations, firmware, and legacy platforms—routine security updates may not be sufficient. Instead, teams may be forced to pursue full system redesigns. The industry's transition away from SHA-1[4] in TLS[5] certificates illustrates this challenge. Because SHA-1 was deeply embedded across browsers, certificate authorities, and enterprise systems, organizations could not simply "patch" their way out when vulnerabilities emerged. Many legacy applications and devices lacked support for stronger alternatives, requiring costly upgrades or outright replacement.

To build quantum resilience, cyber and risk teams must design future systems with replacement in mind. They should isolate cryptographic functions into shared services, standard libraries, or managed platforms so algorithms can be updated without having to rework applications or infrastructure.

It will also be important for cyber and risk teams to create and maintain a living cryptographic inventory—that is, a clear account of where cryptography is used, how tightly it is embedded

[4] Secure hash algorithm.
[5] Transport layer security.

into systems, and how difficult it is to change across systems and third-party products. In this way, teams can develop crypto agility—preserving the ability to change their security architectures even when the "perfect" cryptography solution isn't available. Teams can apply a simple risk lens to interpret this inventory, combining factors such as cryptographic coupling, business criticality, data longevity, and vendor dependency. This will allow organizations to distinguish the systems that can evolve incrementally from those that will need to be redesigned, isolated, or replaced.

These insights should directly guide leaders' investment decisions. Rather than pursuing a blanket approach to the transition, leaders can prioritize those systems with the highest business impact and lowest adaptability. For the most sensitive communications, teams may want to deploy a combination of classical and post-quantum encryption methods, helping to preserve confidentiality while maintaining interoperability as standards evolve.

Move 3: Elevate quantum readiness to a leadership priority—to sustain the transformation
Quantum readiness is not just a technical issue; it's a leadership priority that affects strategy, risk, and operations. Executives don't need to become experts on all the technical details, but they will need to pay attention to key trade-offs, business risks, and long-term exposure as a result of Q-Day.

To manage this transition effectively, organizations should create a cross-functional leadership group—bringing together technology, risk, and business leaders—to set priorities, plan the rollout of changes, and align with external partners.

At one network provider, a critical question for the C-suite was how to deal with quantum exposures for themselves and their clients: If one client is affected by a data breach, for instance, how should the provider communicate that information to other clients? If the provider itself were affected by quantum exposure, which elements of the infrastructure would absolutely need to stay open, and which would the company need to shut down? The provider intentionally set aside time in strategy sessions to account for such quantum risks, so its leaders could understand their potential impact and be prepared to act on them.

The window to prepare for Q-Day is narrower than it appears, and the cost of inaction is compounding. By proactively assessing risk exposure, prioritizing migration pathways, and establishing clear governance, leaders can turn a looming disruption into a structured transformation. The early movers will not only reduce downside risk but also gain strategic flexibility in navigating one of the most consequential technology shifts of the coming decade.

Charlie Lewis is a partner in McKinsey's Connecticut office; **Henning Soller** is a partner in the Frankfurt office; **Sebastian Schneider** is a senior partner in the Munich office, where **Martina Gschwendtner** is a consultant; and **Joana Candina** is a senior expert in the Madrid office.

The authors wish to thank Sara Ravasi and Waris Ziarkash for their contributions to this article.

This article was edited by Roberta Fusaro, an editorial director in the Boston office.