McKinsey Digital

When—and how—to prepare for post-quantum cryptography

While quantum computers may not be able to crack conventional encryption protocols until 2030, many cybersecurity and risk managers should evaluate their options now.

This article is a collaborative effort by Lennart Baumgärtner, Benjamin Klein, Niko Mohr, Anika Pflanzer, and Henning Soller, representing views from McKinsey Digital.

May 2022

Quantum computing holds promise for problems that are out of reach for currently available high-performance computers, potentially fueling progress in areas such as the development of life-saving pharmaceuticals or green-battery technology.[1] However, the technology's power also poses a significant cybersecurity risk. Fully error-corrected quantum computers (which can provide highly accurate results) will be capable of overpowering commonly used traditional encryption protocols. And experts estimate that the first fully error-corrected quantum computers could be available as soon as 2030.[2]

It might seem as though cyberrisk management leaders have time to prepare, but the post-quantum cryptography (PQC) era has already begun for many companies, whether they realize it or not. For instance, increasingly connected vehicles will need to meet high security standards to protect user safety and privacy for their usable lives—which could easily extend past 2040, by which time experts believe error-corrected quantum computers will be available.[3] While previous cyberthreats required updates to key security protocols, quantum computing will render some protocols fundamentally unsafe. Companies will need to change their protection protocols significantly, which will require time and resources to implement. However, the precise path forward is unclear because PQC solutions are still taking shape.

While most of the data that are currently in use—and stored—will not be affected, the security of vast volumes of data, critical systems, and flagship products is still at stake. Security leaders can get started by answering two significant questions: When precisely should they begin mitigation efforts, and what steps can they take to protect their organizations' data and systems? Optimal timing varies across industries as well as within organizations and dictates the options for mitigating threats from PQC. In this article, we'll share relevant considerations that can help decision makers think through these issues.

The nature of the quantum threat

When fully error-corrected quantum computers become available, the threat level for current protocols will vary. These quantum systems will be able to decrypt widely used asymmetric security protocols, such as the commonly used RSA or elliptical curve algorithms. Such protocols are mostly used to distribute secure messages (or keys) through public networks such as the public internet. With these protocols, anyone can encrypt a message, but only the original sender has the key for decrypting it. However, quantum computing will make it possible to decode an encrypted message without this key, rendering encrypted messages legible.[4]

It might seem as though cyberrisk management leaders have time to prepare, but the post-quantum cryptography era has already begun for many companies, whether they realize it or not.

[1] For a discussion of some of the key implications of quantum computing, see "Quantum computing use cases are getting real—what you need to know," McKinsey, December 14, 2021.
[2] Ibid.
[3] Ibid.
[4] While quantum computers will be able to break some asymmetric cryptography algorithms by means of Shor's algorithm, this does not imply that all asymmetric protocols can be broken (for more, see sidebar, "Overview of post-quantum cryptography solutions").

On the other hand, symmetric encryption protocols, in which the sender and receiver exchange encryption and decryption keys before trading information, are currently assumed to be safe from quantum threats. Unfortunately, it isn't always practical to use these protocols for the speedy exchange of information through public networks, because they rely on correspondents securely trading cryptography keys before exchanging data. Managing the substantial number of keys necessary when exchanging large amounts of messages also comes with considerable computing costs. Consequently, efficiently sharing such symmetric keys is a critical issue that needs to be addressed before using these protocols.

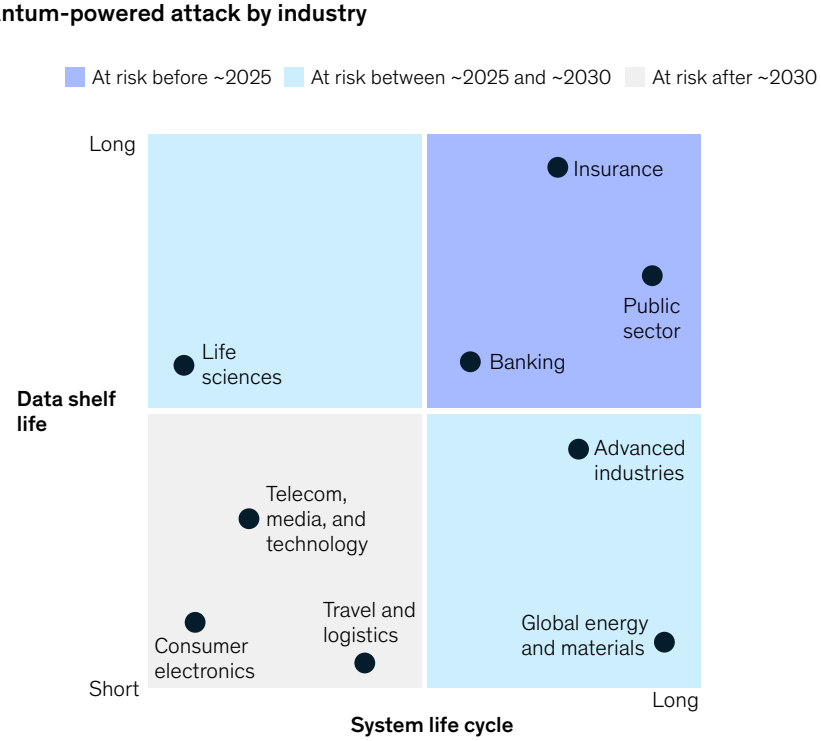
When to act: Two factors to assess

Understanding the value of cybersecurity for an organization is typically the first step in traditional security assessments, both in general and for the protection of specific systems and products. Measuring the value exposed to these risks is key to formulating appropriate strategies against threats and responses to potential security breaches. Since fully error-corrected quantum computers are not available yet, quantum security strategies start with the question of timing. Risk managers will need to examine two key characteristics of high-priority assets—data shelf life and system life and development cycles—in detail to determine when to begin quantum mitigation measures (Exhibit 1).

These two factors should be considered together. Broadly speaking, organizations with substantial value at risk that have data with long shelf lives and systems or products with extended life or development cycles should formulate their responses to PQC now. Those possessing either data or systems with longer lives may have a bit more time to act. Organizations with data and systems of shorter duration have longer still.

Exhibit 1

Industries should prepare for post-quantum cryptography based on data shelf life and system lifetime.



Consider data shelf life. Some data produced today—such as classified government data, personal health information, or trade secrets—will still be valuable when the first error-corrected quantum computers are expected to become available. For instance, a long-term life insurance contract may already be sensitive to future quantum threats because it could still be active when quantum computers become commercially available. Any long-term data transferred now on public channels will be at risk of interception and future decryption.

Because regulations on PQC do not yet exist, the possibility of data transferred today being decrypted in the future does not yet pose a compliance risk. For the moment, far more significant are the future consequences for organizations, for their customers and suppliers, and for those relationships. However, regulatory considerations will also become relevant as the field develops, which could speed up the need for some organizations to act.[5]

Just as with data, some critical physical systems developed today—the hardware and, to a lesser extent, software used to collect, process, and store data and a company's products—will still be in use when the first fully error-corrected quantum computer is expected to come online. This applies particularly to systems and products with long development timelines and operational lifetimes of more than ten years, as well as products with long manufacturing schedules.

For example, automotive manufacturers are developing highly connected vehicles that must meet high security standards to protect users' safety and privacy. With development cycles of approximately five years, production cycles of about seven years, and vehicle lifetimes of roughly ten years, a car developed today will likely still be on the road after 2040. As a result, over-the-air updates for these vehicles will be particularly sensitive to quantum threats. Many government systems have long lifetimes as well, often because they can be difficult to update due to the associated costs and regulations.

Before deciding on a mitigation pathway, data, system, and product owners should create a shared internal understanding of how sensitive their various data types and systems are to quantum threats based on these two factors. Ideally, this would be done as part of standardized data cataloging and risk assessment.

Mitigating quantum threats

At a high level, decision makers can pursue one of three paths to mitigate the threats posed by capable quantum systems: adopt PQC solutions today, retrofit existing systems to PQC standards at a later date, or take action only to enhance the efficacy of traditional encryption protocols—all while monitoring evolving industry standards and regulations (Exhibit 2). The precise decisions will depend largely on when organizations need to begin mitigation, on the performance requirements of cryptography protocols, and on the number and distribution of connected devices and systems that require protection (Exhibit 3).

Option 1: Adopt post-quantum cryptography solutions today

Many start-ups and a few established cryptography players already offer provisional commercial PQC solutions. While adopting one of these solutions might seem to be the best path for any company that needs to act today, there are trade-offs and drawbacks to consider (for more on these PQC solutions, see sidebar, "Overview of post-quantum cryptography solutions").

The first consideration is cost. PQC solutions currently make up only about 2 percent of the global cryptography market.[6] Without the benefits of deep penetration and scale, PQC solutions cost more than traditional cryptography solutions.

[5] The US National Institute of Standards and Technology (NIST) is currently evaluating different post-quantum public-key cryptographic algorithms, with the final results expected to be published in 2022.
[6] Based on the Quantum Insider's 2022 *Quantum security market report*; "The Quantum Insider report forecasts quantum security market worth $10 billion by 2030," Quantum Insider, February 2, 2022.

Exhibit 2

Decision makers have three options for mitigating post-quantum cryptography threats.

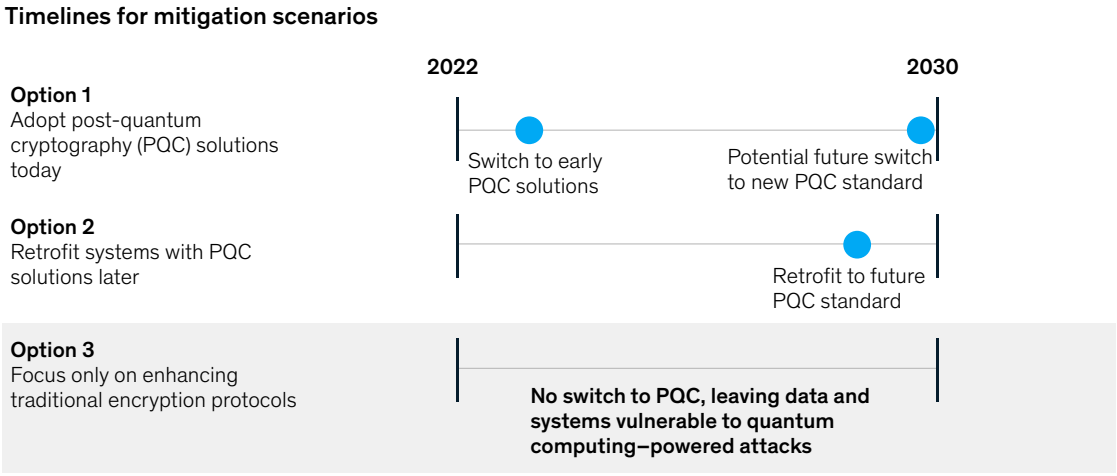
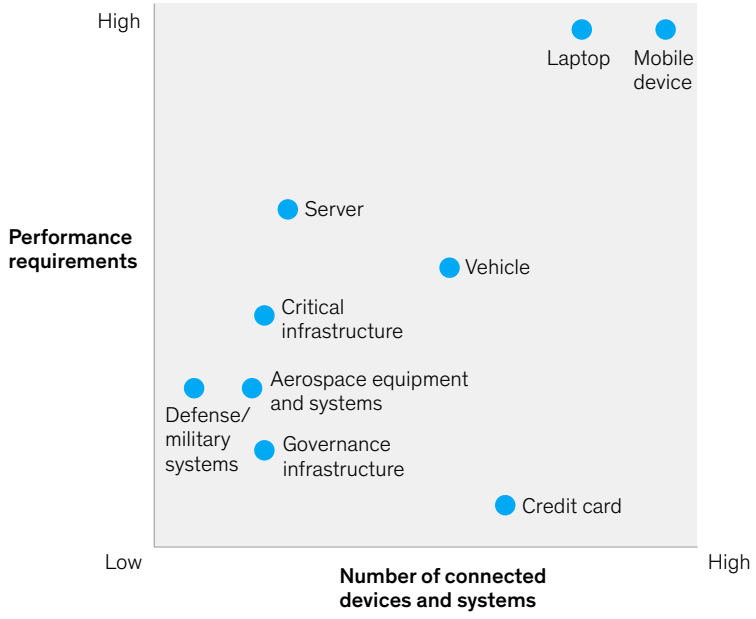


Exhibit 3

Decisions about adopting post-quantum cryptography should account for performance requirements and the number of devices and systems that need protection.



Overview of post-quantum cryptography solutions

The adjustments and investments security leaders will need to make depend on the type of post-quantum cryptography solution that becomes dominant in the market. The two most viable candidates are the following:

1. In quantum key distribution (QKD), two parties exchange a symmetric key through a secure quantum channel. This solution requires additional quantum hardware to transmit, process, and store quantum information. QKD is theoretically safe from decryption by quantum computers, but current implementations remain relatively impractical due to cost and scalability issues.[1]
2. In classical post-quantum cryptography (CPQC), two parties use quantum methods, such as lattice-based encryption, to encrypt messages over classical channels (such as fiber-optic cable). Based on what we currently know, this approach is safe from quantum-computing decryption, but it requires new hardware—albeit similar to what is required for traditional encryptions—for some applications and currently entails a performance trade-off.

Both of these solutions are available today. However, neither is fully commercialized, and both require additional user- and infrastructure-level investment.

[1] The situation is still developing, but the National Security Agency prefers to avoid QKD. For more, see "Quantum key distribution (QKD) and quantum cryptography (QC)," National Security Agency/Central Security Service, 2022.

Organizations that need to secure large amounts of data, devices, and systems in their networks and protocols will experience this limitation most acutely.

Second, because PQC solutions are still nascent and because it is impossible to test them against quantum computers that do not yet exist, they haven't been conclusively proven to provide protection from quantum—or even conventional—threats. As a result, organizations will need to acquire both conventional and PQC solutions to ensure the highest possible level of security if they take action today. Organizations also risk having to switch to higher-performance PQC solutions that come to market in the future, particularly if a currently available solution is excluded from future regulations. Consider that some protective algorithms have already been eliminated by a major US agency, with a few candidates remaining in the final round of reviews.[7]

Third, currently available PQC solutions require significant additional computing power and higher latency times compared with existing standards. While both measures are expected to improve, today's solutions are impractical for organizations that require low-latency performance over public channels. This includes any organization that runs high-value edge- and cloud-computing applications that require large volumes of data to flow quickly between local nodes and decentralized sources of computing power. However, today's PQC solutions may be sufficient for applications with lower latency requirements, such as nonurgent, simple bank transfers or the transfer of insurance contracts.

Given the risks and costs outlined here, most organizations should take a wait-and-see approach to PQC solutions. The exceptions are organizations and uses for which the stakes for security are particularly high, such as in the defense industry, where even provisional PQC protection for some high-value systems or for data with long lifetimes outweighs trade-offs in cost or performance. Another exceptional circumstance is when it would be more costly or impractical—or impossible—to access and retrofit high-value systems in the future compared with installing some protection today.

[7] For more information, see "Post-quantum cryptography (PQC): Post-quantum cryptography standardization," NIST, March 10, 2022.

Option 2: Retrofit systems with post-quantum cryptography solutions later

Companies that choose to wait to adopt PQC for financial, technical, or other reasons still have some work to do today.

First, they should ensure that their hardware and software architectures can be retrofitted as easily as possible. Measures such as reserving computational resources for future cryptography updates or making the architecture sufficiently modular can simplify adding and exchanging cryptography modules in the future. In line with traditional security measures, hardware and software should be separate so that systems can remain flexible to emerging PQC algorithms.

Second, organizations should prepare, both operationally and financially, for retrofitting. Systems will need to be accessible and updated with PQC solutions, possibly while in use or while highly distributed. Some of these changes can be made remotely with software updates, but PQC solutions with high performance requirements will likely rely on specialized hardware, meaning that affected devices will need to be accessed physically in order to retrofit them. Companies responsible for a large number of devices or systems, such as consumer-electronics or auto manufacturers, risk facing operational complexities and high costs when choosing this option, so it's important to begin planning accordingly today.

Finally, organizations should begin building long-term relationships with relevant suppliers, regulators, and peers within and outside of their industries as soon as possible. These relationships will be critical for staying up to date on emerging standards and solutions for PQC. In particular, recent supply chain challenges for hardware components have illustrated the importance of relationships with suppliers. Investing in relationships with suppliers that are already working on PQC-specific hardware can provide a significant advantage when the time comes to procure equipment to retrofit systems. Plus, collaborating with peers is likely to create more benefits than hoarding expertise and capabilities; collectively developing solutions, for example, could cost less than if an organization devised solutions on its own.

Option 3: Focus only on enhancing traditional encryption protocols

Organizations with the most time to act and little value at risk to quantum threats may choose not to make the switch to PQC for the foreseeable future.

Nevertheless, these organizations should consider traditional mitigation actions, particularly extending asymmetric key lengths and using symmetric cryptography where possible. Longer keys would keep companies ahead of early versions of error-corrected quantum computers because those keys require many more qubits (or "quantum bits," the basic building blocks of

Organizations should begin building long-term relationships with relevant suppliers, regulators, and peers within and outside of their industries as soon as possible.

quantum computers) to break. Concretely, moving from RSA-1024 to RSA-2048 encryption may extend security lifetimes by one to three years.

For more protection, organizations should consider scaling up other security measures, such as symmetric key lengths, for particularly sensitive data. Decision makers should also begin planning for future updates to long-lasting systems by, for instance, evaluating the modularity of their technological architecture.

To be sure, forgoing PQC-specific measures creates some risk for companies and their customers. After all, without PQC investments, any application requiring asymmetric encryption will be vulnerable to a fully error-corrected quantum system sooner or later. However, as with any risk, organizations must weigh the costs of increasing protection against the costs of a breach.

Post-quantum cryptography is approaching. The right way to prepare for this new era varies by company, as do the considerations around balancing near-term costs with possible risks further in the future. Leaders and decision makers in security and risk should evaluate their options—and get moving.

Lennart Baumgärtner is a consultant in McKinsey's Munich office, where **Anika Pflanzer** is a partner; **Benjamin Klein** is an associate partner in the Berlin office; **Niko Mohr** is a partner in the Düsseldorf office; and **Henning Soller** is a partner in the Frankfurt office.