BCG

How Quantum Computing Will Upend Cybersecurity

By Jean-François Bobier, Clément Fouilloux, Vanessa Lyon, Gildas Bouteiller, David Panhans, and Pierre Roussel

ARTICLE OCTOBER 15, 2025 12 MIN READ

This article was written in collaboration with BCG's Center for Leadership in Cyber Strategy.

Imagine a world where every locked door has the same key and suddenly that key is stolen. That's what quantum decryption could mean: a world where nothing online—emails, e-commerce, banking—is secure.

That world is in sight. Sometime around 2035, quantum computers are expected to become sufficiently powerful to compromise current widely used cryptographic standards, the foundation for online security. The number of connected devices worldwide is expected to surpass 40 billion by 2030, and e-commerce will account for around 4% of global GDP by 2029. With so many systems dependent on these standards, quantum cryptanalysis could literally break the internet.

Fortunately, quantum-resistant cybersecurity solutions are within reach. The transition to post-quantum cryptography (PQC) won't be cheap—nothing involving IT ever is—and it will take time. For business leaders, this puts a premium on three actions:

- **Strategize.** Classify critical applications and systems and preemptively plan for system sunsets.
- **Start as soon as possible.** Mitigate immediate threats and avoid escalating costs.
- **Integrate crypto agility.** Develop modular cryptographic systems and quickly assess your organization's readiness for a post-quantum security environment.

As quantum threats approach and the cost of inaction rises, leaders can't afford to wait on PQC.

Quantum Trouble

Few of us ever see cryptography in action, but it is the mechanism that safeguards data privacy and integrity. There are two primary types of cryptography in widespread use today: symmetric, exemplified by such standards as the advanced encryption standard (AES), and asymmetric, which includes widely adopted methods such as RSA and elliptic curve cryptography (ECC).

Symmetric cryptography uses a single, shared secret key for both encryption and decryption and provides speed and efficiency, particularly in handling large data volumes. Asymmetric cryptography involves a pair of different, but related, keys—a public key for encryption that is widely accessible and a corresponding private key for decryption, which is securely held by the recipient.

Both symmetric and asymmetric cryptography are essential to secure digital communications, authenticate identities, and facilitate secure key exchanges. Many use cases, such as HTTPS connections on the web, employ a hybrid of the two. If the asymmetric part of such a hybrid scheme is broken by quantum computers, the whole scheme is broken.

> “At their current rate of development, quantum computers have a better than 50% likelihood of breaking widely used cryptographic algorithms by 2035.

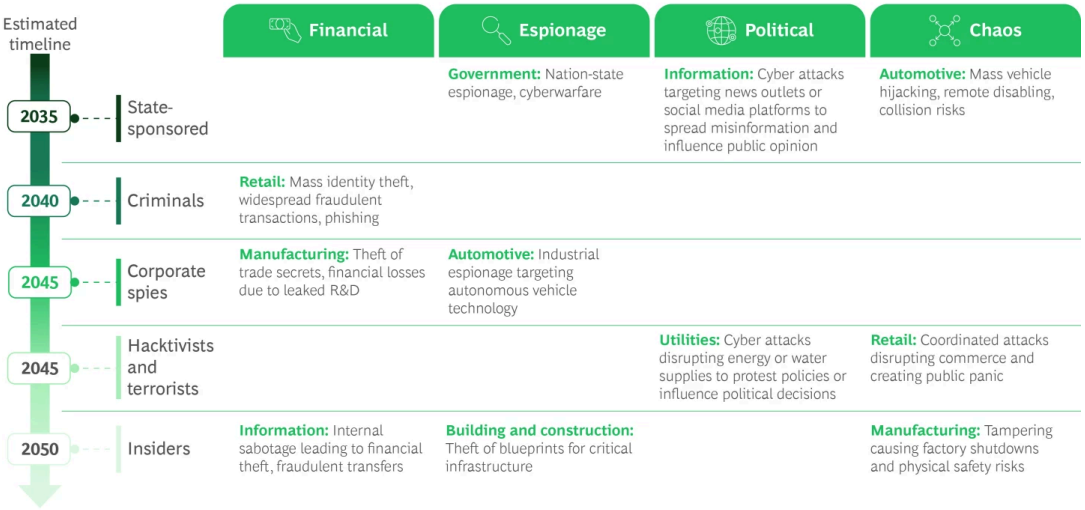
If parameters are chosen carefully, the mathematical problems that asymmetric cryptography relies on cannot be solved by classical computers. But quantum computers work differently, using quantum bits, or qubits, that can exist in multiple states simultaneously and are very proficient at solving certain types of mathematical problems, including the integer factorization problem and the discrete logarithm problem—the problems that the security of RSA and ECC relies on.

Plenty of technical challenges remain, but quantum technology is progressing quickly. IBM’s quantum computing roadmap predicts quantum processors scaling rapidly—from today’s 433-qubit Osprey chip towards systems surpassing 1,000 qubits within the next few years and potentially exceeding several thousand qubits by 2035. At that scale, quantum computers have a better than 50% likelihood of breaking widely used cryptographic algorithms such as RSA-2048.

The threat comes in several forms, from various types of malicious actors. (See Exhibit 1.) State-sponsored attackers are likely to be the first movers, sometime around 2035, exploiting quantum capabilities for espionage purposes. (Intelligence agencies have already demonstrated interest in quantum computing for surveillance. A $80 million initiative called "Penetrating Hard Targets," specifically aimed at developing quantum capabilities to break encryption, was referenced in Edward Snowden's 2013 disclosures.)

EXHIBIT 1

Tomorrow's Quantum Attacks Are Already on the Calendar



Source: BCG analysis.

By 2040 or so, organized criminal groups could leverage quantum computing to disrupt financial systems, execute massive identity theft, and compromise sensitive health care records. Hacktivists and terrorist groups may soon follow, potentially targeting critical infrastructure such as power grids and water supplies, or sabotaging manufacturing systems.

It's the Law—or Soon Will Be

The good news is that government authorities have recognized the looming problem and moved swiftly to develop solutions. In 2016, the US National Institute of Standards and Technology (NIST) initiated a global competition to develop and standardize quantum-resistant cryptographic algorithms. After extensive evaluation and testing involving the international cryptographic community, NIST in 2022 selected four PQC algorithms to replace existing standards vulnerable to quantum attacks. (See "Securing the Post-Quantum Future.") All derive their security from mathematical problems considered computationally infeasible for both quantum and classical computers, ensuring resilience against future quantum threats.

— Securing the Post-Quantum Future

The PQC algorithms selected by NIST include CRYSTALS-Kyber, a lattice-based algorithm designed specifically for secure key exchanges, and three digital signature algorithms:

- CRYSTALS-Dilithium, also lattice-based and optimized for efficiency.
- FALCON, known for its compact signatures.
- SPHINCS+, a hash-based algorithm serving as a conservative, fallback option in case other mathematical assumptions are compromised.

A growing number of websites, including those of leading tech firms, already operate on these standards, but adoption is still only about 9% for the majority of websites. (See the exhibit.) Although the transition requires significant organizational planning, early adoption of NIST-recommended PQC algorithms will be critical for maintaining security and regulatory compliance in the quantum era.

Regulatory bodies, especially within the EU, have already laid the groundwork for future cybersecurity requirements. Once quantum-resistant standards are finalized, compliance will swiftly become mandatory. The EU's Digital Operational Resilience Act (DORA) and the updated Network and Information Security Directive (NIS2) have introduced stringent guidelines around encryption and secure key management for critical sectors such as finance, energy, and health care.

European cybersecurity agencies—including France's ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), Germany's BSI (Bundesamt für Sicherheit in der Informationstechnik), and the EU's Agency for Cybersecurity (ENISA)—are actively working on updated cryptographic guidelines. Japan's Cyber Research Consortium, a public-private group, is working to develop and standardize PQC technologies. China has launched an initiative to develop its own PQC algorithms.

Organizations that fail to comply with new regulations may not only be subject to fines; they could be held legally liable for breaches enabled by continued adherence to outdated standards. They

could also suffer operational setbacks, such as the inability to sell goods online or to orchestrate supply chains with vendors.

Pay Now, or Pay More Later

PQC transition costs will hit two budget lines: IT backbone upgrades and Internet of Things (IoT) infrastructure updates.

Companies typically spend about 3% of revenue on IT. The backbone must be safeguarded so data can be encrypted and secured and transactions can be authenticated. Based on early PQC efforts and lessons learned from the Y2K transition, we project PQC transition costs at 2.5% to 5% of the annual IT budget. Preemptive planning can significantly reduce this impact: for example, we estimate that a company with an annual IT budget of $1 billion would spend approximately $25 million if it starts the transition early. Delay not only increases the risk of a breach—it could double the cost to about $50 million by 2035.

> Delaying the transition to post-quantum cryptography not only increases the risk of a breach—it could double the cost of the transition.

Both the number and type of devices on the IoT have proliferated in recent years. At least 20 billion IoT devices, including consumer, wearable, smart home, medical, industrial, and smart infrastructure devices, are now estimated to be online, and this number is growing by 10% to 15% a year. Because of factors such as cost, power consumption, constrained networking, and long shelf duration, many of these devices rely on hardware and software that are either difficult to upgrade or fail to meet minimum requirements to run PQC algorithms (which may require more computing power and bandwidth than traditional schemes such as RSA).

IoT upgrades therefore present a more substantial financial challenge, especially in industries that rely heavily on connected devices. Global automotive companies, for instance, could face costs ranging from $400 million to $750 million because of the complexity and scale of updating vehicle hardware and software. Other sectors, such as manufacturing, utilities, transportation, and information and media, will likely experience smaller but still substantial expenses in the range of $10 million to $20 million. We have based these estimates on the premise that action is taken today; considering that IoT devices can stay online 10 years or more, inaction would be lead to much higher costs since physical devices would need to be decommissioned.

In addition to the financial costs, there's the potentially catastrophic risk for society at large if attackers gain access to critical systems. Financial services, automotive, and government are particularly exposed. (See Exhibit 2.)

Here's a roadmap for keeping costs down and achieving PQC security.

Strategize. Organizations should first classify their applications and data based on sensitivity and expected lifespan. Typically, only about 10% of applications are truly critical and require immediate quantum-resistant upgrades. Online banking platforms, patient records, and customer-facing portals are a few examples. The remaining 90%, including vendor-managed external systems (such as Salesforce, Workday, and Microsoft Teams) and internal noncritical systems (such as HR dashboards and expense tools) can be addressed later, enabling efficient prioritization. (See Exhibit 3.)

In addition, organizations can optimize resources by planning for product sunsets—such as the end of a typical automobile's 10-year lifespan—and exclude them from costly PQC upgrades. Such planning can avoid significant unnecessary cost and effort.

Start as soon as possible. Organizations have both operational-security and financial reasons to move quickly. Experience has shown that major cryptographic transitions typically require 10 years or more. For instance, in symmetric encryption, migrating from the data encryption standard (DES) to AES took most organizations about 16 years from the initial identification of the DES weaknesses through phaseout. Similarly, moving from older cryptographic hash functions (known as the message digest, or MD, family) to the newer secure-hash algorithms (SHA family) required approximately 10 years between standardizing the new algorithms and fully retiring the outdated ones. (See Exhibit 4.)

Moreover, even though quantum computers are not likely to break well-configured traditional cryptography before 2035 (or even later), the threat that malicious actors harvest "secure" data now for eventual decryption later brings the PQC imperative forward significantly. The harvest now/decrypt later scenario is especially concerning for highly sensitive data with long-term criticality, such as military plans, governmental records, and medical and financial information. For example, contracts digitally signed now, or in the next few years, could face authenticity issues down the road if compromised. Undermining digital signatures could threaten everything from interbank payments to credit card purchases to certification authorities.

Attackers often face practical challenges, such as precisely selecting sensitive data, which ironically leads them to steal and store large volumes of encrypted information. While the attackers incur storage costs, data owners are more substantially compromised. Companies should combat harvest now/decrypt later with "prepare now, save cost later" approaches.

Some organizations will face scenarios in which immediate upgrades to legacy or less-critical applications are not technically or financially feasible. Workarounds such as reverse proxies could preserve business continuity for legacy systems, enabling a smoother transition as long-term upgrades are planned and implemented. But they also introduce extra complexity and costs.

Integrate crypto agility. To implement PQC, organizations need modular, automated, and standardized cryptographic architectures that enable rapid and seamless updates as quantum-resistant standards evolve. In a March 2025 memo, NIST outlined the key principles for effective crypto agility. These include modular cryptographic design, automated update mechanisms, interoperability, comprehensive cryptographic asset inventory, risk management, clear governance structures, and staff training. History shows that maintaining crypto agility is crucial: between 1989 and 2001 alone, organizations experienced five different hash-algorithm standards. (See Exhibit 5.)

Rigid implementations that do not allow for quick adjustment can carry severe risks, which was illustrated by the Heartbleed vulnerability in 2014. Heartbleed was a critical flaw in OpenSSL, a widely used cryptographic library securing internet communications (including HTTPS, virtual private networks, and email). Although the mathematical foundations of the algorithm were sound, an implementation error allowed attackers to trigger a "heartbeat" request, causing servers to leak sensitive information, such as private keys and user credentials.

Because of limited crypto agility, it took many organizations weeks or even months to fully patch affected systems, leaving more than 300,000 servers vulnerable two months after disclosure and compromising over 4.5 million medical-patient records. The estimated global cost was $500 million, and there are still systems running with the bug today.

The Countdown Has Begun

Quantum risk isn't a distant storm on the horizon; the clock is already ticking. Every encrypted contract, medical file, or transaction created today could be harvested and unlocked once quantum machines reach scale.

With history showing cryptographic transitions take ten years or more, starting in 2030 will already be too late. The organizations that act now will not only secure their systems but also earn the trust that will define the next digital economy. Those that wait will be left explaining why their systems were breached.

As digital transformation accelerates, it opens new frontiers for innovation, growth, and competitive advantage—but also heightened vulnerabilities. Cyber is no longer just a technical concern; it's a strategic imperative. Organizations must evolve their cyber posture in tandem with digital progress to safeguard trust and enable resilience.

BCG's Center for Leadership in Cyber Strategy applies bold, business-first thinking to reframe cybersecurity as integral to business strategy—not an afterthought. We embed "security by design" into how leaders shape, evaluate, and execute priorities from the outset. Drawing on BCG's global network of cybersecurity, risk, and strategy experts, we help executives cut through technical complexity and fear-driven narratives. By reframing digital risk in business and economic terms, we empower confident decision making that turns resilience into a

source of lasting competitive edge—enabling organizations to innovate, adapt, and emerge stronger through disruption.

Authors

Jean-François Bobier

Partner and Vice President, Deep Tech
Paris

Clément Fouilloux

Senior Manager, Cybersecurity & Digital Risk
Paris

Vanessa Lyon

Managing Director & Senior Partner
New York

Gildas Bouteiller

Managing Director & Partner
Paris

David Panhans

Managing Director & Senior Partner
Dubai

Pierre Roussel

Managing Director & Senior Partner
Paris

ABOUT BOSTON CONSULTING GROUP

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.