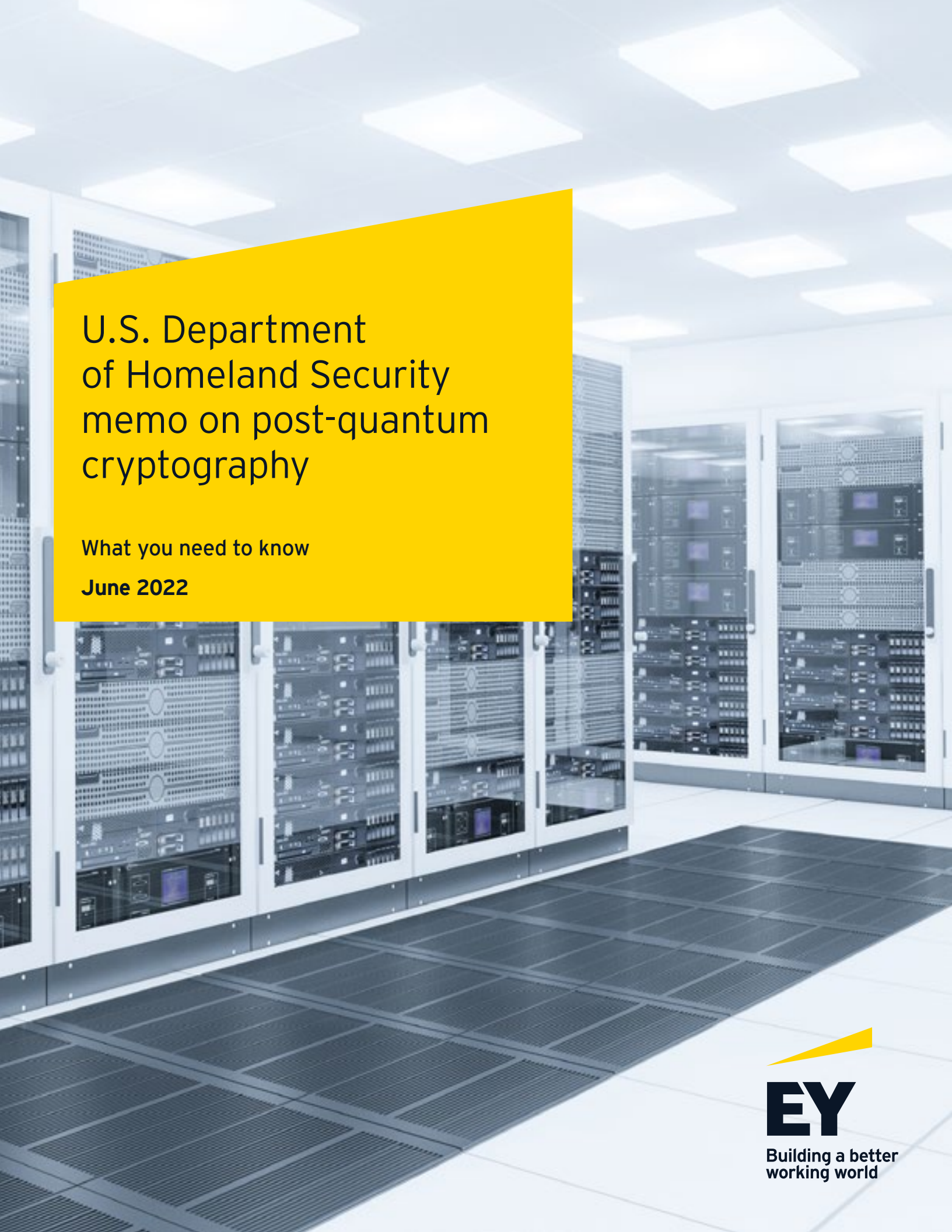


U.S. Department of Homeland Security memo on post-quantum cryptography

What you need to know

June 2022

EY

Building a better working world

1 Executive summary

Quantum computing has the promise of changing aspects of our world unlike anything that we have seen in history. Many fields of study stand to make monumental leaps in progress due to the significant increase in computing power afforded by the application of quantum physics to computing. Advancements in areas such as pharmaceutical development, disease etiology, material science, energy, aeronautics, weather forecasting, blockchain and financial modeling portend to be revolutionary when quantum computing reaches its maturity. All of these examples provide for a very positive impact. **The implications related to cryptography are equally as impressive; however, for concerning reasons.**

Data and communication transmissions today are protected by cryptographic algorithms developed over the past several years. The security of these algorithms is believed to be very strong and can withstand attempts of compromise, even by today's supercomputers. Quantum computing, however, is believed to possess the power that will enable current cryptographic algorithms to be compromised in mere minutes.

In September 2021, the U.S. Department of Homeland Security (DHS) issued a memorandum titled, "Preparing for Post-Quantum Cryptography." In this memorandum, DHS highlighted the threat to the current cryptographic standards and to organizations in all sectors, including the government. We believe this will be the first of many memorandums and regulations that get published and approved around this topic.

The memorandum also provides guidance for a transition from the current cryptographic standards and technologies to post-quantum encryption standards. Currently, however, a US post-quantum cryptographic standard does not exist. The National Institute of Standards and Testing (NIST) is currently considering many algorithmic solutions to become finalists for the NIST standard. DHS's goal is to provide a roadmap that will reduce the time needed to transition to these standards when they are made available through the NIST process.

"

Quantum computing, however, is believed to possess the power that will enable current cryptographic algorithms to be compromised in mere minutes.

This white paper discusses the threat to information security posed by quantum computing, specifically with encryption. We will explore what quantum computing is, how quantum computing impacts current cryptography, the current state of quantum computing advancement, what the government is suggesting to make cryptography quantum resistant, and what EY professionals believe is currently available to organizations for both planning and action.

2 Cryptography fundamentals

To understand the impact of breaking commonly used cryptographic systems with quantum cryptography, let us first understand cryptography's primary objectives to securely identify sources and protect the confidentiality and integrity of data. They are:

- **Confidentiality:** protects information from unauthorized disclosure by transforming the data into an unintelligible form called ciphertext
- **Integrity:** provides assurance that data has not been altered and the data is from the authorized source
- **Authentication:** provides assurance of the identity of the system (or user) being communicated with

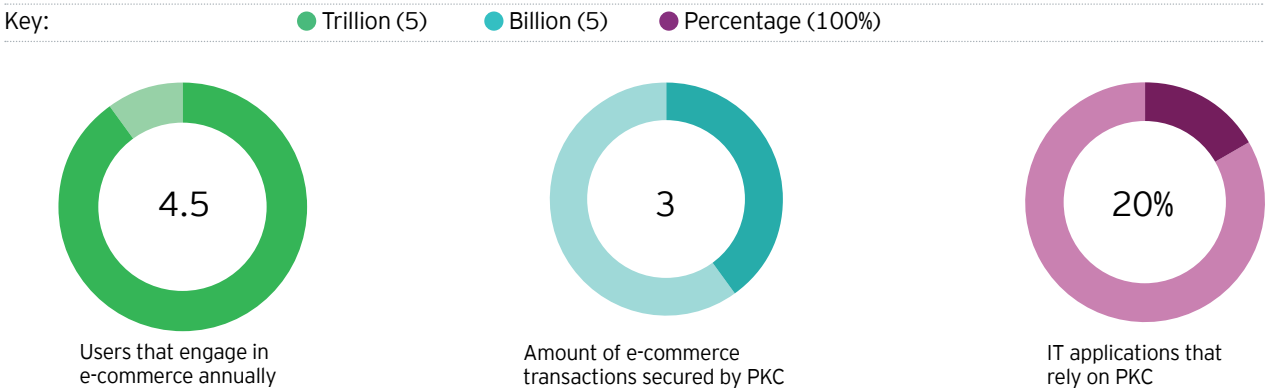
By examining real-world analogs, the scope of cryptography's importance is easily established. Encryption ensures adversaries cannot view data in an accessible data store or capture communication over networks by converting intelligible data, called plaintext, into unintelligible data, called ciphertext. The reverse process, from ciphertext to plaintext, is known as decryption. Without the confidentiality and integrity achieved by encryption, an adversary could inject, modify, or view data in a database or while it is being transmitted over a network, thereby compromising that data. Lastly, without authentication, an adversary computer can masquerade as a legitimate system to access a network or an application.

Cryptographic algorithms and protocols come in two forms: symmetric and asymmetric cryptosystems.

- With symmetric cryptosystems, the same secret key is used for all of its operations (e.g., confidentiality encrypting and decrypting use the same key). Widely used symmetric cryptosystems include AES and HMAC.
- On the other hand, an asymmetric cryptosystem has two types of keys: a public key that can be shared and a private key that must remain secret (e.g., for confidentiality encrypting with a public key and decrypting, often referred to as public key cryptography (PKC)). The popular algorithms to enable asymmetric encryption (aka PKC) include RSA, DSA, ECDSA, Diffie-Hellman (DH) and EC-DH.

Asymmetric cryptosystems require significantly more computing power than their symmetric encryption counterparts. However, asymmetric cryptosystems reduce the complexity of managing cryptographic keys. In practice, asymmetric and symmetric cryptosystems are deployed together. Hybrid solutions leverage the advantages of symmetric cryptography's computational efficiency, while benefiting from the pragmatic key management offered by asymmetric cryptography.

Figure 1. Users at risk for breach of data



Reference for this information: Comandar, Lucian, Bobier, Jean-Fraqncois, et al., "Ensuring Online Security in a Quantum Future," *Boston Consulting Group website,* https://www.bcg.com/publications/2021/quantum-computing-encryption-security, accessed May 2022.

3 Quantum's impact on cryptography

A conventional computer's fundamental unit of computation is a bit, which is limited in its ability to exist in a state of either a zero or a one value. In the quantum world, the fundamental unit of computation is a quantum bit, or qubit, which has the ability to hold multiple states at one time and can exist in the state of both a zero and a one at the same time. An abstract illustration of how qubits work is the analogy of a coin that is both heads up and tails up simultaneously. It is this multiplicity that allows computing power to grow exponentially as the number of qubits expands, allowing for more and more computations to be performed simultaneously, and which also enables a quantum computer to solve certain types of problems more efficiently than a conventional computer.

Examples of the types of problems a quantum computer is able to solve, in which a conventional computer is not, include Grover's algorithm and Shor's algorithm. Each of these algorithms was developed by the mathematician from which they derived their names, Lov Grover and Peter Shor. Grover's algorithm leverages the processing power of quantum computing to speed up the attack on those symmetric encryption schemes using smaller key sizes. **The solution to this is to simply increase the key length (e.g., AES 128 to AES 256),** whereas **the solution to Shor's algorithm requires an entirely new quantum-proof algorithm.** The algorithm has the ability to take a key pair's public key, and relying heavily on the ability of a quantum computer to be in many states simultaneously, to derive the private key through a process of prime factorization. Through this method, Shor's algorithm effectively breaks the most commonly used asymmetric cryptosystems, including RSA, DSA, ECDSA, DH and EC-DH.

Implication: When quantum computing has sufficient size and reach, asymmetric encryption key algorithms will be susceptible to their private keys being compromised, resulting in insecure data and communications

A conventional computer needs **300 trillion years** to crack RSA 2048 prime number factor encryption.

A 4,099-qubit quantum computer would need just **10 seconds** to crack the same RSA key.

Source: Baumhof, Andreas, "Breaking RSA Encryption – an Update on the State-of-the-Art," QuintessenceLabs website, https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art/,accessed May 2022.

4 Quantum computing advancements

Today, the vulnerabilities introduced by quantum computing through Shor's algorithm are still mostly theoretical, as quantum computers exist, but have not yet achieved a high enough number of qubits to significantly reduce the amount of time it takes to compromise a private key. However, the rapid pace of advancements in quantum computing technologies across the globe is bringing the reality of Shor's algorithm ever closer.

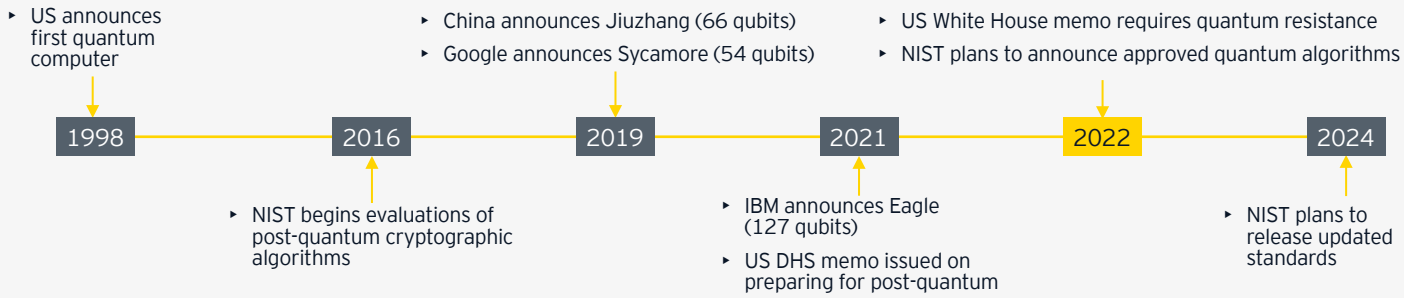
In the last five years, China, Israel[1] and Russia[2] have all developed quantum computers, with China's efforts on its Jiuzhang quantum computer claiming quantum supremacy[3] in 2019.

The US private sector emerged as an early leader in quantum computing capabilities, having developed the first quantum computer as early as 1998, and most recently Google claims to have taken the lead with the introduction of its quantum computer Sycamore in 2019.[4] Additionally, IBM has assisted Germany and Japan in entering the quantum race by partnering with both countries to build quantum computers. Like IBM, many other multinational companies have expanded the quantum computing landscape to a more global setting. Intel, Toshiba, Google and Alibaba Group all hold multinational patents in quantum technology. Google and Alibaba Group each hold patents in 12 countries.[5]

Investments in quantum computing also continue to grow. To date, Canada has invested $2.2 billion in quantum computing, Germany $2.4 billion[6] and China dedicated $10.0 billion to its National Quantum Lab.[7] In the US, the National Quantum Initiative Act was signed to invest $1.2 billion in the field of quantum information science and technology during a 10-year period.[8] That said, there are numerous private companies spending billions of dollars on researching the use of quantum computing for uses such as protein folding for medical treatments and pharmaceuticals, energy, financial optimization planning and, of course, cryptography.

Figure 2. Quantum computing continues to advance at a rapid pace

Quantum advancements 1998-2024



5 The push for quantum-resistant cryptography

As the reality of quantum computing draws nearer, the US government is working to prepare for the quantum vulnerabilities that will inevitably materialize.
The NIST began the work to identify quantum-resistant algorithms in 2016. The institute warned that many common encryption algorithms used widely by both the private and federal sectors to protect sensitive data could be rendered ineffective within the next decade as the race toward quantum computing accelerates globally. As a solution, they announced the creation of a Post-Quantum Cryptographic Evaluation process meant
to replace the algorithms that would not withstand the expected shift toward quantum computing.

It is expected that the NIST will release its first set of approved algorithms in 2022 and publish standards for those algorithms by 2024. Since most cryptography implementations use one or more NIST standard, businesses should prepare for implementing the new standards.

The White House and DHS each released requirements related to the growing risks of quantum computing capabilities abroad — namely the need for identification and replacement of encryption algorithms that would not be resistant to quantum computing's increased power and speed. The DHS memo listed specific algorithms that are likely to be vulnerable and informed component heads to expect detailed requirements related to reporting requirements for the transition of such algorithms in alignment with the timeline for the updated NIST standards.[9]

> "The quicker global quantum computing capabilities advance, the less time current keys will be considered 'safe.'

Additionally, the White House's January and May 2022 memos built upon an earlier executive order mandating cybersecurity standards for federal information systems to include additional requirements to identify and replace vulnerable encryption practices with quantum-resistant algorithms on an aggressive timeline.[10]

6 Threats posed by quantum computing

It is clear from the information above that the pace at which quantum technology is advancing is much faster than the pace previously set by traditional computer technology advancements. The DHS states in its memo, "While the exact timeline of a quantum computer capable of executing advanced algorithms putting DHS cryptographic equipment inventory at risk is uncertain, the significance of the risk is not."[11] Threat actors are also aware of the rapid pace of quantum computing and are looking ahead at the opportunities to exploit future vulnerabilities. These threat actors are currently exercising crypto harvesting techniques, where they are applying a "harvest now, decrypt later" approach to data theft. For many years, encryption has been the answer to the data loss challenge, but the application of Shor's algorithm with a quantum computer is causing traditional encryption techniques to soon become obsolete and is driving an aggressive response.

The federal government is taking this risk very seriously and is advocating for a swift, proactive approach to mitigating the risk. The DHS is expecting federal agencies to complete their preparations for post-quantum protections prior to the NIST's updated cryptographic guidelines, which are expected to be released in 2024. Additionally, President Biden issued a national security memorandum in January 2022 giving only 180 days for government agencies to "identify any instances of encryption not in compliance with NSA-approved Quantum Resistant Algorithms."[12] And for those instances, they must create both an exception and a timeline for their remediation. The aggressive timelines set forth by the government are dramatically different from any timing we have seen in past migrations (e.g., SHA1 to SHA2). The DHS memo specifically states, "A slow transition could prove costly in terms of security."[13]

EY point of view

While there is still uncertainty about when "Q day" — the day when quantum computers can crack PKC — will actually occur, transitioning to a post-quantum-resistant environment will likely take a lot of time and money. In an effort to shorten the migration to post-quantum cryptography, following are several practical steps that should be closely scrutinized and promptly put in place as you develop a strategy to mitigate future quantum risks.

Develop an inventory of high-value information assets: Develop an inventory of critical data by understanding the data held by the organization and its value (e.g., the data that needs to be protected the most), and then classify that data as it is created. Having an inventory of your organization's most sensitive data types and repositories gives you a starting point to look for vulnerable crypto algorithms.

Identify and inventory cryptographic objects: Leverage existing infrastructure and tools to identify the crypto objects (e.g., keys, certificates) being used by your high-value information assets.

EY point of view

Understanding the algorithms and key metadata will allow you to identify weak algorithms that are not quantum ready. Systems with quantum vulnerabilities should be flagged for future remediation.

System prioritization: Perform data flow mapping to understand upstream and downstream impacts from a cryptographic algorithm migration. System migration should be prioritized based on the length of time data must be protected and the sensitivity of that data. Look at our approach to minimizing risk through data disposition[14]

Identify updates needed for internal standards and third-party contracts: Earmark internal standards and policies that will require updates to reflect post-quantum guidance provided by the NIST. Additionally, identify third-party contracts where post-quantum encryption may need to be mandated.

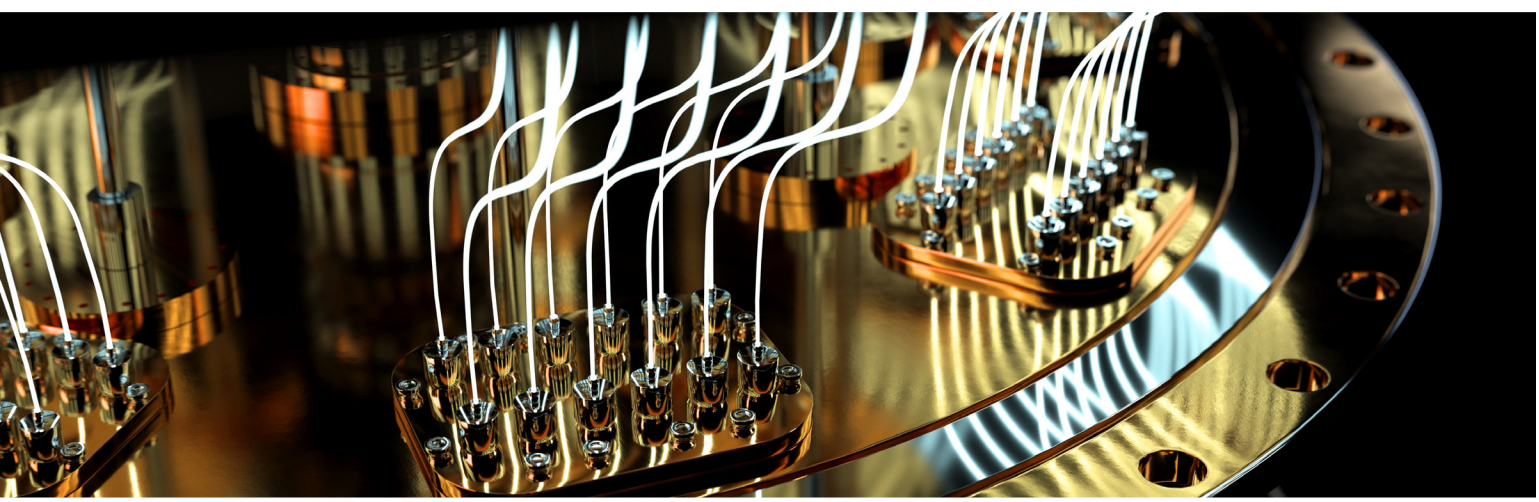
Plan for a migration: Develop a strategy to apply post-quantum technologies and solutions to support the migration to post-quantum requirements.

Although the roadmap above is applicable to all organizations, some industries will be targeted by quantum threat actors sooner than others. Our experience globally across sectors leads us to believe the industries most likely to be impacted by quantum threats include finance, energy, health care and government. These industries should be expected to take immediate action by initiating conversations around quantum risks at the highest levels and allocating resources to take the necessary steps as outlined above. Reach out to our Cybersecurity practice leaders below to take advantage of our experience and knowledge as you apply these steps.

Dave Burg
Principal
Ernst & Young LLP
dave.burg@ey.com

Chris Hall
Principal
Ernst & Young LLP
chris.hall3@ey.com

Varun Sharma
Principal
Ernst & Young LLP
varun.sharma7@ey.com



Sources

[1] Ben-David, Ricky, "A huge leap: Israeli researchers build country's first quantum computer," *The Times of Israel website,* https://www.timesofisrael.com/a-huge-leap-israeli-researchers-build-countrys-first-quantum-computer/, March 22, 2022.

[2] "By 2030, Rosatom will launch a quantum Internet," *TAdviser website,* https://tadviser.com/index.php/Project:Rosatom_quantum_computer, May 2022.

[3] Conover, Emily, "The new light-based quantum computer Jiuzhang has achieved quantum supremacy," *ScienceNews website,* https://www.sciencenews.org/article/new-light-based-quantum-computer-jiuzhang-supremacy, May 2022.

[4] Rincon, Paul, "Google claims 'quantum supremacy' for computer," *BBC website,* https://www.bbc.com/news/science-environment-50154993, October 23, 2019.

[5] "Quantum Computer and Quantum Communication," *TAdviser website,* https://tadviser.com/index.php/Article:Quantum_Computer_and_Quantum_Communication, April 13, 2022.

[6] Dr. Yildiz, Mehmet, "Why Six Countries Heavily Invest in Quantum Computing for Artificial Super Intelligence," *Medium website,* https://medium.com/technology-hits/why-six-countries-heavily-invest-in-quantum-computing-for-artificial-super-intelligence-8be766596e13#:~:text=According%20to%20Global%20Tech%20Outlook,United%20States%20(%241.2%20billion), November 16, 2021.

[7] Lin, Jeffrey and Singer, P.W., "China is opening a new quantum research supercenter," *United States Air Force website,* https://www.airuniversity.af.edu/CASI/Display/Article/1604330/china-is-opening-a-new-quantum-research-supercenter/, October 10, 2017.

[8] National Quantum Initiative Act, United States Congress, 2018 (accessed via https://www.congress.gov/115/plaws/publ368/PLAW-115publ368.pdf, 2018).

[9] "Preparing for Post-Quantum Cryptography," *U.S. Department of Homeland Security website,* https://www.dhs.gov/sites/default/files/publications/usm_quantum_memo_0.pdf, September 17, 2021.

[10] "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," *The White House website,* https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/, January 19, 2022.

[11,13] "Preparing for Post-Quantum Cryptography," *U.S. Department of Homeland Security website,* https://www.dhs.gov/sites/default/files/publications/usm_quantum_memo_0.pdf, September 17, 2021.

[12] "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," *The White House website,* https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/, January 19, 2022.

[14] "How to minimize risk through data disposition," *EY website,* https://www.ey.com/en_us/consulting/how-to-minimize-risk-through-data-disposition/, August 5, 2020.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2022 Ernst & Young LLP.
All Rights Reserved.

2205-4043111
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com