KEYFACTOR

WHITE PAPER

Planning Ahead for Post-Quantum Cybersecurity

The time to protect enterprises and data from the future threat of quantum computing is now

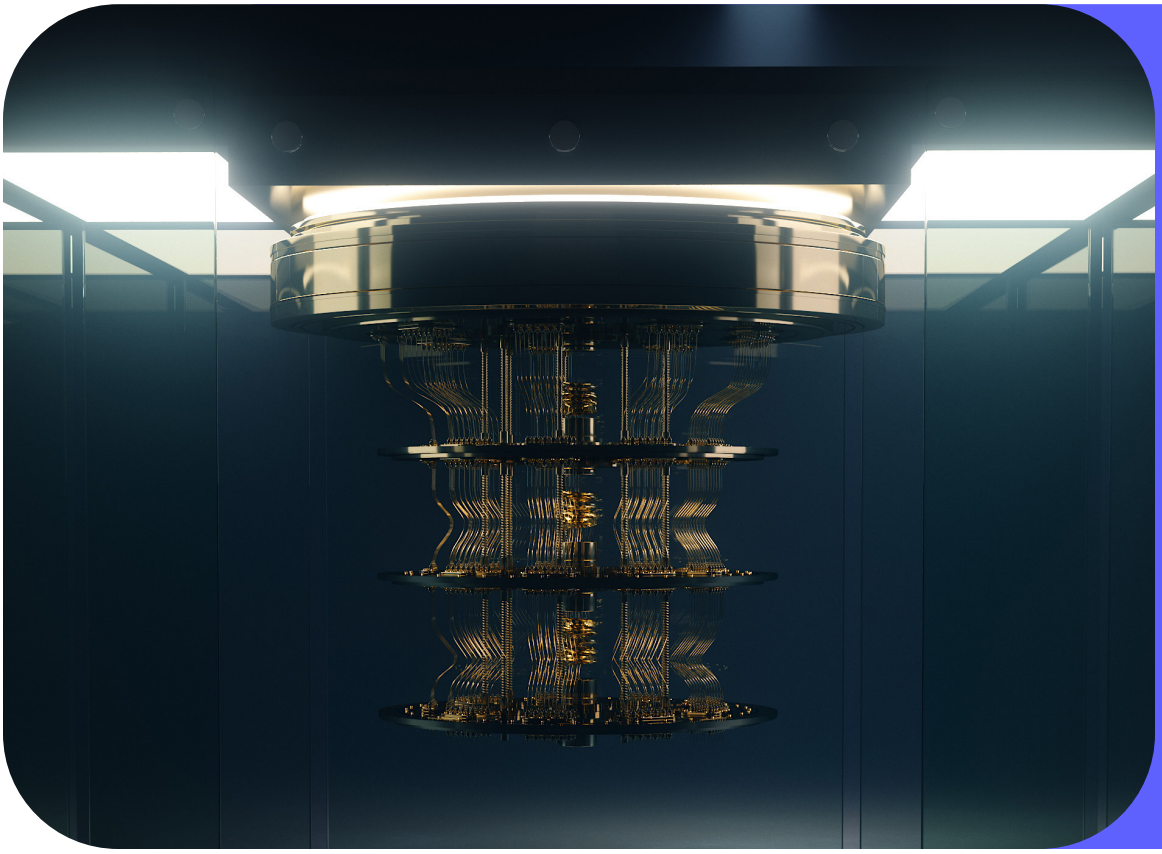


Table of contents

The promise of quantum computing is tantalizing. Once quantum machines become sufficiently powerful, tasks that would have taken hundreds or thousands of years using traditional binary computers might instead be completed in days or even hours.

According to a 2021 report by Deloitte, almost every industry and government agency stands to benefit from the exponential increase in computer power offered by quantum computing. From supply chain optimization to financial risk analysis, climate change simulation, and the discovery of new semiconductor materials, quantum technologies promise to be as revolutionary as the advent of personal computers.

But there is an old saying that every solution carries the seeds of the next problem. This holds true for the post-quantum world. All the current encryption and credential tools used to protect data and identity will be rendered effectively useless, and easy prey to quantum hacking.

That doesn't have to happen. If governments, industries, and organizations start planning for a post-quantum environment right now, we can still benefit from all of the advantages of quantum computing while mitigating the dangers to cybersecurity.

The duality of quantum computing

In May 2022, the White House issued an Executive Order to strengthen the federal government's pursuit of the international leadership role in quantum computing. On the same day, it also issued a National Security Memorandum directing federal agencies to mitigate the risk of quantum computing.

The national security memo does a good job of outlining the dangers. It states, in part:

> **"Most notably, a quantum computer of sufficient size and sophistication — also known as a cryptanalytically relevant quantum computer (CRQC) — will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world. When it becomes available, a CRQC could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions."**

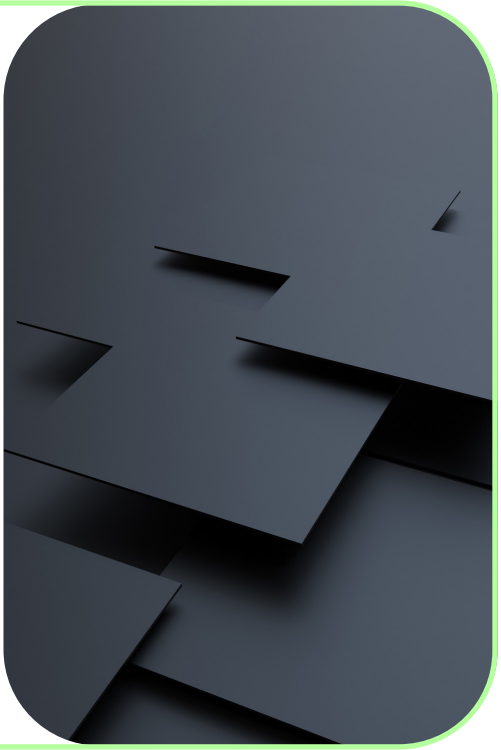
Think about that — on the one hand, the government is dedicated to developing quantum computing and setting its standards; on the other, it is warning agencies they have to take steps right now to protect against it, even though it doesn't yet exist.

The reason for this seeming contradiction is because the vast potential of quantum computing to address problems previously too big to solve also means it can be applied to hacking a critical element of today's computing environment — encryption.

For instance, RSA's encryption scheme for public key infrastructure (PKI) is based on multiplying very large prime numbers together; using one of today's computers, it would take around 300 trillion years to solve it — making it unsolvable, for all intents and purposes. But a quantum computer of sufficient power could unravel the same encryption code in just a few minutes, or possibly even faster.

This is why, for all the attention paid to requiring that data be encrypted whether at rest or in transit, federal agencies work so hard to prevent data exfiltration.

There is hacking going on in advance of quantum, attacks for "steal-to-decrypt" later. The hackers, often hostile nation-states, know that at some point in time, the encrypted information they steal now will be decryptable using quantum technology, and then they can figure out what part of their stolen data is most useful. As such, the data exfiltration attacks of today could become the national security breaches of tomorrow, just as soon as a quantum computer is able to break the encryption of that stolen data.



Another consequence of more powerful quantum computers could be any user's inability to browse the internet securely. The little padlock icon next to the URL signifies it uses the Transport Layer Security (TLS) protocol, which was developed by the Internet Engineering Task Force (IETF), an international standards organization. The first version of the protocol was published in 1999, and it was most recently updated in 2018. But it was designed to protect against the threats of today, not those posed by quantum machines.

TLS is intended to provide privacy and data security for communications via the internet. Quantum hacking would end its usefulness. IETF is already addressing ways to maintain TLS security in a post-quantum environment, but in the end, the only way to know if the new protections work is to use them in the world — which could be a very big gamble.

Using quantum computing as a hacking tool is sort of like a "brute force" attack, but that comparison only goes so far. The CTO of one company working on post-quantum solutions, himself an expert in encryption, said there are ways to program a Cryptographically Relevant Quantum Computer (CRQC) so that it doesn't use brute force, and instead relies on the oddities of quantum computing itself. "Set up a simulation of the number [to be hacked], assign rules for the CRQC to follow, instill those properties into the thousand or two thousand qubits, then push a button and say 'Go,'" he said. "The quantum system will settle into the state that solves the problem, in an insignificant amount of time. You might find a couple of hundred plausible solutions, but that makes it easy to then use a conventional computer to find out which one is right."

That example is just one that demonstrates the oddity of how quantum computing works. The word "settle" in that example is like having a ball on a spinning roulette wheel, bouncing around until it settles into a single slot. In quantum, all the qubits bounce around and settle into their 1 or 0 states, producing hundreds of possible solutions. And quantum computers, if programmed correctly, can achieve that without resorting to traditional brute force tactics used by binary computers. In other words, it can achieve its goal without having to try every single combination of numbers or solutions along the way.

Planning for short- and long-term solutions to quantum hacking

Addressing the risk side of the quantum computing equation clearly is critical to both the security of nations and their economic wellbeing.

National security solutions

The White House national security memo assigns responsibility for finding long-term solutions. Specifically, it states that:

> **Currently, the Director of the National Institute of Standards and Technology (NIST) and the Director of the National Security Agency (NSA), in their capacity as the National Manager for National Security Systems (National Manager), are each developing technical standards for quantum-resistant cryptography for their respective jurisdictions."**

To comply with the memo, NIST selected four "quantum-resistant" (QR) cryptographic algorithms in July 2022 to begin testing. By the middle of August, one of them had already fallen, in just four minutes, to a 10-year-old regular desktop computer.

In September, NSA issued its own advisory, which supports NIST's initial algorithmic selections, in order to "provide future [National Security Systems] requirements so vendors may begin building toward these requirements, and so acquisition officials and NSS owners and operators will know what the requirements are." The advisory noted that the transition to QR algorithms should be completed by 2035. In other words, companies that serve the intelligence community should start incorporating one of NIST's prospective QR cryptographic algorithms beginning immediately.

This is a gamble, as the almost immediate failure of one of the algorithms demonstrates, but given the stakes, it makes sense in the national security world. It is a combination of short-term tactics (use one of these algorithms) and long-term strategy (so that when quantum hacking shows up, the systems are already prepared to defend against it).

Economic security solutions

The challenge for agencies and companies not in the intelligence community, but which still rely upon encrypted communications, is how to prepare for this dangerous future without necessarily betting the farm on one of NIST's algorithms before it has been proven.

For organizations, quantum computing will require a significant amount of work to keep the organization safe. The problem is, many organizations don't know where encryption is used, and on which data. In a perfect world, there would be a big red button that says, "Don't push until Quantum Day — or until RSA is abrogated." Organizations want that, but there is no easy way to get there.

Steps to Take Moving Forward

If organizations wait until a quantum computer is invented that can shred encryption, it will be far too late to begin trying to protect against it. To avoid that fate, there are a couple of key steps that should be taken now to get their post-quantum security at their agency, company or organization moving in a positive direction.

Step 01

Make a commitment to strategic planning

Any organization that uses encryption today needs to prepare for the post-quantum future. But it doesn't stop there. Any industry that produces products with a lifespan longer than five years — like automotive, medical devices, appliances, and anything that falls within the Internet of Things (IoT) — is going to be affected.

The financial sector, for instance, already is preparing. Wells Fargo has an entire division just to prepare for post-quantum, and other banks are following suit, but there are still a ton of other fields where they don't know what post-quantum means, even though the impact of not being ready is so dangerous.

In other words, corporations have to find a way to break out of their short-term, next-quarter-results mindset, and adopt a much longer term view of security when it comes to preparing for a post-quantum environment.

It's comparable to the way organizations should prepare for a natural (or manmade) disaster — not because it is imminent, but because by the time it's imminent, it's too late to prepare. Organizations will have to do the work and mature their cybersecurity standards. For instance, if they are updating their infrastructure to implement a zero-trust architecture, they should be investing in products that have built-in preparations for a post-quantum environment.

Step 02

Commit to good data and device inventories, plus security hygiene

Many organizations, especially in the private sector, do not have a good handle on all the devices connected to their systems, which security measures they employ, or where in their vast networks encryption is used. Nor do they know which data are most vulnerable, compared to which data are most valuable.

Interestingly, federal agencies are in a better position to identify and keep track of their use of encryption because of the regulatory framework within which they operate. This is because the government takes an ecosystem approach. Things like BYOD, working from home, and multifactor authentication, for example, are areas where agencies are likely to be in better control. Only now are we beginning to see the industry starting to stringently focus on the issue.

So, the first actual IT step after gaining leadership commitment to long-term preparation is developing that inventory and committing to keeping it updated.

This applies to industries using IoT, as well. Companies that design and build IoT devices, whether medical, residential, or commercial, need to include updated capabilities and build lifecycle management of the crypto piece into those devices.

For organizations making the transition to a zero-trust architecture — whether in the public or private sector — the transition itself is an opportunity to identify where encryption is being used and what devices are attached. That takes the fire-fighting behavior out of how to respond. They will already have fully defined inventories and prioritizations.

It also creates the opportunity to leverage automation, such as replacing zero-trust certificates with those that support quantum-resistant algorithms in many places all at once.

This is an important premise, because the labor shortage in cybersecurity is already a huge bottleneck, especially finding people who have specialized skills in areas like encryption and PKI. Being able to automate tasks will make it possible to keep up-to-date inventories and switch to post-quantum quickly.

Plant your quantum protection tree 20 years ago, or right now

There is an old adage that the best time to plant a tree is 20 years ago. And the second best time to plant a tree is today. That's a clever saying because it takes many years for a tree to grow to the point where people can get some benefit from it — nuts or other fruit, shade in the summertime, the environmental benefits, or even harvesting it for wood. And the second-best time is today because delay only puts off when the benefits can be realized.

The same can be said for investing in quantum-resistant security. It can't happen overnight, and by the time you really need it, it's already too late to begin to address the problem. You need to set the groundwork for that right now if you want to be ready for a post-quantum future.

A good example of successfully addressing a problem early is with the so-called Year 2000, or Y2K, bug, a problem that could have plagued computers at the end of the last century. It was discovered that computers without long enough date fields might fail when the clock struck midnight in the year 2000, because their operating systems and apps might think it was the year 1900, or maybe zero, instead. Thankfully, the problem was discovered years in advance of the deadline. The Y2K disaster never happened because people took it seriously. Post-quantum security needs the same level of focus because if it is not addressed early, the consequences will be very serious.

Conclusion

Quantum computing will open up an entirely new world of possibilities, and there is little doubt that it will help to advance our society in untold ways.

But it will also fundamentally change algorithms used for PKI. Ultimately whether or not quantum will become of the size and scope needed to effectively break existing algorithms is mute. The reality is that organizations are going to have to adopt new algorithms because the threat exists and will always exist. There is no going back once the new suite of quantum-resistant algorithms are approved and standardized. The new risks that we will face are considerable, but also manageable if we begin to lay the groundwork for our defenses today, long before we are overwhelmed by a bright (but challenging) post-quantum future.

Additional reading

EBOOK

Why It's Time to Re-think Your PKI

Migrating to the cloud?

Discover 5 reasons to modernize your PKI.

Download now ↗

EBOOK

Three Strategies to Navigate the Cybersecurity Labor Shortage

Demand for cybersecurity talent continues to surpass the resources available.

Download now ↗

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed. For more, visit keyfactor.com or follow @keyfactor.

Contact us

- www.keyfactor.com
- +1.216.785.2946