Hudson Institute

MARCH 2019

# The Executive's Guide to Quantum Computing and Quantum-secure Cybersecurity

BY ARTHUR HERMAN

We would like to acknowledge ISARA Corporation for their generous support.

For more information about obtaining additional copies of this or other Hudson Institute publications, please visit Hudson's website, **www.hudson.org.**

ABOUT HUDSON INSTITUTE

Hudson Institute is a research organization promoting American leadership and global engagement for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings and recommendations.

Visit **www.hudson.org** for more information.

**Hudson Institute**
1201 Pennsylvania Avenue, N.W.
Suite 400
Washington, D.C. 20004

P: 202.974.2400
info@hudson.org
www.hudson.org

Photo Credit: Getty Images

Hudson Institute

MARCH 2019

# The Executive's Guide to Quantum Computing and Quantum-secure Cybersecurity

BY ARTHUR HERMAN

# INTRODUCTION

CEOs and CIOs are accountable for protecting their company, their investors, their customers, and their employees from cyber-threats that endanger the company's private information and financial well-being.

Today the most serious of these is the threat to the integrity of data and information that are vital to a company's success. This comes not only from current cyber-attacks and hackers, which according to 2017 estimates by cyber-research firm Accenture, on average cost organizations around the world $11.7 million a year. It also includes the future threat posed by quantum computers and quantum technology, which will render public-encryption systems helpless and enable competitors and adversaries to steal a company's most precious information without leaving a trace behind.

In October 2018, global research and advisory firm Gartner elevated the quantum computer threat to the top of its list of digital disruptions for which CIOs may not be prepared. It noted that "quantum computers have the potential to run massive amounts of calculations in parallel in seconds,"[1] including cracking the complicated math problems on which today's encryption systems depend.

At the same time, considerable confusion exists, even among experts, about the true potential of the quantum threat, the timeline for its advent, and the steps needed to protect a company's future.

This guidebook aims to provide some common-sense answers to these and other questions about quantum computers and the quantum threat. It also intends to offer solutions for CEOs, CIOs, and their fellow executives so that addressing the quantum threat is not disruptive, but merely part of their company's normal cybersecurity plan.

In addition, it provides guidance for the future, answers other questions regarding quantum technology, and includes links for keeping up to date on the subject.

Business management guru Peter Drucker once posed the question,

[1] Panetta, Kasey. *The CIO's Guide to Quantum Computing.* November 29, 2017 https://www.gartner.com/smarterwithgartner/the-cios-guide-to-quantum-computing/

“Will the corporation survive?”
One thing is certain: no corporation, agency, or enterprise can survive if its most important data and information are constantly and systematically vulnerable to attack and/or theft. Employees, shareholders and investors, and the general public need to trust that company executives have made every effort to secure that data and information, now and in the future.

It is to help senior executives fulfill that trust and ensure peace of mind that this guidebook was written.

# I. WHAT IS QUANTUM COMPUTING?

Quantum computers use the principles of quantum mechanics to manipulate data. In many cases, this leads to exponential increases in processing efficiency over traditional computers—in ways that will far surpass the capabilities of even today's fastest supercomputers. One of the quantum computer's unique properties is that it can be in multiple states at once, as opposed to traditional computers, which can only be in one state at a time.

As an example of how this makes it different, a quantum computer with 300 quantum bits ("qubits") could be in as many states as there are atoms in the universe. This is not the full story of the power of quantum computers, but is simply meant to show how different quantum is from classical computing.

Make no mistake: there will be no fully functional and programmable quantum computer on anyone's desk anytime soon, but it might be accessible sooner rather than later. The benefits of this accelerated calculating power will include improvements in machine learning, better approaches to design of pharmaceuticals, process optimizations, and many more.

Unfortunately, such a computer would also render today's public-encryption systems obsolete, creating widespread vulnerabilities. In addition, it would pose a serious threat to national security because it could open the encrypted secrets of countries, enterprises, and individuals and could be used to cripple critical infrastructure and financial systems.

# II. HOW BIG A THREAT DOES IT POSE TO MY COMPANY?

The global research firm Gartner has elevated the quantum threat to number 1 in its list of digital disruptions today's CIOs and CEOs will have to face.

Why?

To understand how grave the threat will be, imagine the security systems that protect a company's information as a pyramid, going from the least to the most securely protected (Figure 1):

At the top are the most common challenges to system security: **user errors** like poor passwords, opening phishing emails, and similar mistakes and mishaps.

Next come **administrator errors**, such as failing to patch vulnerabilities in existing systems or to update systems.

Then there are **platform issues**, which include implementation flaws and glitches flowing from poor installation of security systems.

**Architecture flaws**, the result of poorly designed systems, generate other vulnerabilities that an agile hacker can leverage into a major security breach.

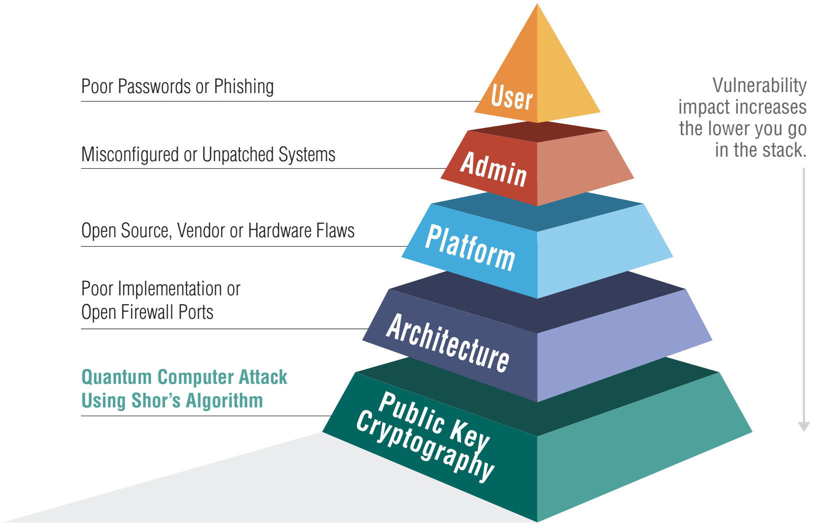
Finally, at the bottom stands **cryptography**, the most important means by which companies and agencies normally protect and authenticate data and transactions.

What every CEO and CIO must realize is that as we move down the security-impact pyramid, the vulnerabilities get harder to exploit (public-key encryption systems, for example, are extraordinarily difficult even for experienced hackers to crack), but the potential impact on critical elements grows. In fact, the last element in the pyramid—cryptography, and more specifically, public-key cryptography—is where the quantum computer threat is greatest.

The fact is, quantum computing has the potential to catastrophically disrupt a company's IT norms, impose huge new workloads on its IT staff, and even threaten the existence of the company.

Today, the advent of a quantum computer able to factorize the huge sub-prime numbers that underlie current public-encryption systems is not a question of if, but when.

## Figure 1. Potential Security Vulnerability Causes


Poor Passwords or Phishing
User
Misconfigured or Unpatched Systems
Admin
Open Source, Vendor or Hardware Flaws
Platform
Poor Implementation or Open Firewall Ports
Architecture
Quantum Computer Attack Using Shor's Algorithm
Public Key Cryptography
Vulnerability impact increases the lower you go in the stack.

Source: ISARA (December 2018)

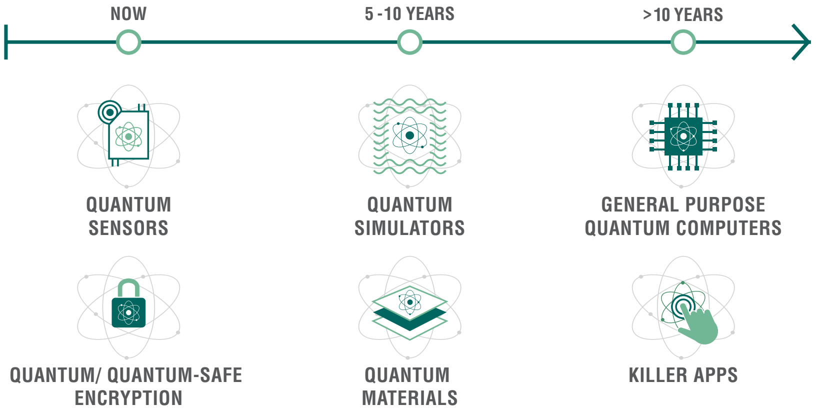
# III. WHEN WILL A QUANTUM COMPUTER CAPABLE OF BREAKING PUBLIC-ENCRYPTION SYSTEMS BE READY FOR USE?

The timeline for advances in quantum computing is moving fast. In March 2018, Google announced its researchers were on the brink of a 72-qubit quantum processor. Late in the year, IBM announced it had passed the 50-quibit threshold, while Intel is holding steady at 49 qubits. Rigetti Computing, a mid-sized company and rising star in the quantum field, aims to achieve a 128-qubit computer by the end of 2019.

That said, experts agree it would take a 2,000-qubit, fully fault-tolerant system to be at least theoretically capable of breaking some public-key cryptography algorithms, such as 1,024-bit RSA or 256-bit ECC. That may seem a long way off, but many researchers believe 2019 could see some major progression toward more powerful quantum systems. As Figure 2 shows, some believe a universal 2,000-qubit system could be as little as seven-fifteen years away.

## Figure 2. Quantum Technologies Timeline

ESTIMATE AS TO WHEN NEW QUANTUM TECHNOLOGIES WILL START TO BECOME COMMERCIALLY AVAILABLE



Source: Quantum Valley Investments (October 2018)

# IV. HOW LONG DO I HAVE TO PROTECT MY DATA AND NETWORKS?

Since information is a critical asset for today's businesses, protecting it is as important as protecting classified information is for defense agencies.

In most companies or agencies, information technology depends on multiple independent systems—such as Linux or Android—each with its own discrete encryption tools and security safeguards.

Unfortunately, the popular cryptographic algorithms that play a central role today in protecting proprietary information and data—including the Rivest-Shamir-Adleman algorithm (RSA), Diffie-Hellman, and digital signature algorithm (DSA)—will not be secure from attacks by quantum computers. Nor will blockchain, since it depends on elliptical curve cryptography (ECC), which also suffers from the same quantum vulnerability.

In fact, any encryption system that relies on RSA or ECC will be vulnerable to quantum intrusion—which will be virtually undetectable. Nor does the threat end there. While the advent of Q-Day (when quantum computers are powerful enough to disrupt classic encryption) may be a decade off or more, data harvesting will enable competitors to store purloined data until then, in what is often called a "harvest and decrypt" attack. If an otherwise secure communication or transaction is stored, the data will be available for future decryption once a quantum computer of sufficient size is available.

# V. WHAT IS QUANTUM-SAFE CRYPTOGRAPHY (QSC)?

Just as quantum technology offers ways to penetrate existing classical encryption, so it will enable IT professionals to build essentially unhackable networks. Systems such as quantum-key distribution (QKD) and quantum-safe cryptography (QSC), which use quantum random-number generators (QRNGs), will provide virtually hack-proof data and networks.

QKD is a secure communication method whose cryptographic protocol involves components of quantum mechanics. It enables two parties to produce a shared random secret key, which can then be used to encrypt and decrypt messages.

A QRNG is a device that provides a stream of random bits generated with a method based on the laws of quantum physics. Such QRNGs provide the random secret keys that QKD requires, and will be the basis of hack-proof quantum communication networks in the future.

Currently, it is possible to obtain random data generated through methods based on quantum physics. Unfortunately, growing this technology into systems for genuine data protection and for information-sharing over networks is perhaps decades away.

A much more practical approach is to introduce new algorithms into existing systems to replace RSA and ECC. Government agencies and some private companies are hard at work optimizing these algorithms, which are digitally based and use hard math problems that are resistant to intrusion, even by general-purpose quantum computers. This form of security is known as quantum-safe cryptography or post-quantum cryptography.

# VI. WHAT IS THE CURRENT STATE OF QSC?

The National Institute of Standards and Technology (NIST), an agency of the Department of Commerce, has begun work on defining new global standards for the era of post-quantum cryptography. In April 2018 NIST held a major standardization conference, and it expects to release its new draft standards by 2024.

While awaiting NIST's leadership, security professionals can still identify the information that may be at risk in the quantum computing era and devise some interim solutions to safeguard information and data critical to their company's performance.

Therefore, instead of scrapping existing cryptography systems like RSA and ECC, companies will need to embed quantum-safe algorithms in order to continue using those systems. These "hybrid" solutions will allow for companies to keep their product certifications while also future-proofing existing systems seamlessly.

Of course, knowing which companies offer the best implementations of QSC and hybrid, agile solutions requires careful preparation and research and the ability to ask the right questions.

# VII. WHAT STEPS DO I NEED TO TAKE TO PROTECT MY COMPANY, AND WHO NEEDS TO BE INVOLVED?

From a quantum-safe perspective, it is best to take a holistic approach to the company's cybersecurity needs, running all the way from the back office (IT and digital services) to the front office and even the corporate board.

The first step is running a basic post-quantum data-risk assessment, which should include:

- generating an inventory of all systems and applications using cryptography;
- classifying data and mapping data flows;
- developing and/or updating existing cryptographic policies;
- creating a timeline for installing quantum-safe cryptography;
- developing a post-quantum implementation strategy.

The next step is deciding what company or agency data to protect and determining how it is protected now. This means extensive conversations with the chief information security officer, the chief technology officer, and the head of HR, since personnel records are often one of the most high-value—and least-protected—targets for hackers.

The other key area needing post-quantum protection will be proprietary information, including intellectual property (IP). IP has been among the most attractive targets for conventional hackers in the past two decades, especially those from Russia and China. This is because harvesting foreign IP has been an important part of those countries' national economic and security strategies.

Those same actors, particularly China, will also be the first to build and utilize large-scale quantum computers for the same purpose. Securing proprietary information and patents will be fundamental to every company's business strategy in the post-quantum era.

From that perspective, one of the most overlooked but also perhaps most valuable pieces of data and information a company possesses is its business strategy. Gaining access to the business strategy of a highly successful company, or the leader in a specific industry, will become an attractive goal for an unscrupulous competitor—or an equally unscrupulous state actor.

A conversation with the company's CFO should also be high on the list, since implementing a plan to protect vital information should be seen as an investment like any other business investment, which will enable a company to survive as well as grow.

For example, the latest Ponemon Institute study on data breach costs found that on average, such a breach will cost a company $3.86million. The study also revealed that the average cost of a lost or stolen record is $148, the likelihood of a recurring breach is 27.9 percent, and the average time to identify a breach is 196 days.[2]

At the same time, the study found that extensive use of encryption leads to average savings of $13 per record—a substantial saving compared to the cost of losing those records. The report underlines the point that investing in security, and encryption in particular, pays off in the long term, while delays in addressing cybersecurity issues—or even ignoring them—can be devastating in the short term, as companies like Sony have recently found out.

This rule is even more important for dealing with the coming quantum threat. The sooner a company invests in quantum-proof solutions, the sooner it will see a return on its investment, i.e., the robust protection it will need to defend against the most serious cyber-threat anyone can imagine.

[2] Ponemon, Larry. *Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT.* July 11, 2018 https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

# VIII. WHAT QUESTIONS SHOULD I ASK?

***What assets am I protecting currently?***

As noted earlier, for today's businesses, information is a critical asset, and they must protect proprietary information as zealously as defense agencies protect classified information. Therefore, understanding the state of current cyber and other IT security protections is fundamental to understanding where that protection needs to go in future, and how.

***Which are the most important assets, and how are they protected today?***

Every CEO and CIO needs to remember: data breaches occur because someone has deemed the targeted information to be critical. If these executives do not know what information is critical in their company or agency, it is important to find out.

***How is data and other information stored, and who has access to the most critical information?***

The answers to both these questions will provide important guidance as to how many information-management systems within a company are interconnected and whether that connectivity is a source of security or an additional vulnerability.

***How long will current cyber-protections last?***

Even if current protections have a long shelf life, none will be safe unless steps are taken to render them quantum-secure. On the other hand, if protections of important platforms have expired or are about to expire, this offers an opportunity to implement a security reset by incorporating hybrid tools and other solutions that can be progressively upgraded and made future-proof.

***Are the vendors and/or suppliers with whom I share data and information equipped with quantum-safe encryption, and if not, when do they expect to begin quantum-proofing their critical systems?***

No company is an island, and no amount of quantum-proofing will help if data and information are shared with companies or entities that have left themselves vulnerable to quantum attack. It is important to open a conversation with vendors and suppliers to make sure they are on the same path. The sooner the vendors begin testing through proof-of-concept projects, the sooner they will be able to provide the latest quantum-safe technologies to protect their customers' critical assets.

# IX. HOW WILL QSC PROTECT MY COMPANY'S MOST CRITICAL ASSETS?

Some post-quantum cryptographers use the term “migration” to describe the process by which a company or agency’s information assets become quantum-secure. The term recognizes the fact that quantum security is a long-term journey, a deliberate phased upgrade, and not a one-off rush job.

Why?

Classical encryption systems like RSA and ECC rest on a universal algorithm, meaning that the same algorithm is used for encryption and digital signing. With QSC, however, five different areas of math are available for these tasks, each with its own strengths and weaknesses. This means that instead of asking which algorithm is best for protecting all of a company’s data and networks, companies should ask which algorithm will protect particular memory, bandwidth, and processor requirements and other constraints. (This is one reason why the NIST standardization process is so complicated and is taking so long).

The more methodical the process, the less risk there is of errors. And getting started earlier means making the process cheaper and leaving more time for due diligence and testing.

For any company, customizing the QSC migration path means focusing on three key areas of vulnerability:

- **Harvest and decrypt**: Looking for ways to protect information stored today from quantum decryption tomorrow.

- **Roots of trust**: Enabling hardware and devices to securely communicate and authenticate software and firmware updates on a reliable basis, with processes or plans for regular upgrades.

- **Public-key infrastructure (PKI)**: This is where post-quantum “crypto-agility” is especially important. PKI refers to the rules, policies, and procedures needed to create and manage public-key encryption. Because PKI and other dependent systems are time-consuming and cumbersome to update, it is important that users be able to choose appropriate algorithms for their present and future needs while using the same certificate chain—i.e. preserving the chain of trust from root certificate to end user.

All this means that it is best to rely on a post-quantum cybersecurity company with an experienced, professional staff, ideally one that can offer agile, hybrid approaches as well as multiple options for digital signature, key agreement, and key encapsulation algorithms—in short, an all-in-one approach that allows for incremental upgrades as the technology advances and as Q-Day approaches.

# X. CONCLUSION

No one can say exactly when progress in quantum computing and quantum technology will reach the threshold allowing a quantum-based computer to decrypt current public-encryption systems. In addition, no one should be misled by the hype from certain members of the tech media and certain companies involved in the quantum race. As a recent report on quantum computing from the National Academy of Sciences put it, "Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm based public key cryptosystems will be built within the next decade."

At the same time, the report also noted, "Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, *the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster* (emphasis added)."[3]

In other words, while the timeline for quantum computers may be lengthy, the timeline for preparing for their arrival is much shorter. Getting prepared must be one of the growing priorities of responsible executives, and while resources for securing data and networks from quantum intrusion are still evolving, much already exists to justify taking action today.

As the saying goes, the most important step in any journey is the first step. The same is true with quantum-secure cryptography. The decision is yours: the future of your company or agency may depend on your taking that first step.

[3] National Academy of Sciences report. *Quantum Computing: Progress and Prospects.* 2018 https://doi.org/10.17226/25196

# XI. WHAT RESOURCES WILL HELP ME AND MY COMPANY STAY UP TO DATE ON DEVELOPMENTS IN QUANTUM AND QSC?

No area of technology is moving faster today than quantum information technology, in terms of quantum computing and post-quantum cryptography. CEOs and CIOs can follow the most recent developments by checking the **Quantum Alliance Initiative** homepage and the following websites for additional information:

https://www.hudson.org/policycenters/36-quantum-alliance-initiative

https://csrc.nist.gov/projects/post-quantum-cryptography

https://www.etsi.org/technologies-clusters/technologies/quantum-safe-cryptography

https://quantumcomputingreport.com/

https://www.gartner.com/doc/3772121/plan-quantum-computing-postquantum-cryptography

https://www.abiresearch.com/market-research/product/1028952-cryptography-in-the-quantum-computing-era/

www.isara.com

**About the Quantum Alliance Initiative:**
The mission of the Quantum Alliance Initiative (QAI) is to develop policies which guide the creation of a robust quantum ecosystem in which the United States and her allies become global leaders in quantum technology.

*QAI would like to thank Thomas Keelan for his assistance researching and editing this project.*

**Hudson Institute**
1201 Pennsylvania Avenue, N.W. Suite 400, Washington D.C. 20004
202.974.2400 www.hudson.org