DTCC

SEPTEMBER 2022

POST-QUANTUM SECURITY CONSIDERATIONS FOR THE FINANCIAL INDUSTRY

A WHITE PAPER TO THE INDUSTRY

POST-QUANTUM SECURITY CONSIDERATIONS FOR THE FINANCIAL INDUSTRY

Financial institutions are safekeepers of investments, public assets, pensions, and retirement accounts. They ensure that trades and asset transfers occur with complete, uncompromisable integrity. Those responsibilities call for maintaining the security and privacy of personal information, accounts, holdings, and financial transactions.

Over the past 25 years, financial institutions have used encryption to maintain the security and privacy of computer-based information. Conventional encryption uses mathematical techniques to encode digital data and requires keys to revert that data to human-readable information. Most of today's encryption methods use algorithms that might break only after thousands of years of nonstop processing by the world's largest conventional computers.

Now experts realize that quantum-based computers will have the power to break those codes in seconds. Some estimate that the majority of data protected with conventional encryption techniques could be vulnerable within the next decade.

DTCC has taken early steps to evaluate its exposure by beginning to educate itself on the risks, to inventory encryption methods in use, and to determine if and where the organization has post-quantum risk.

DTCC is publishing this paper to bring this near-term risk into focus for the financial industry, to identify initial steps financial institutions can take, and to provoke a more intentional dialogue about how the industry can act now to ward off post-quantum risk.

"As emerging technologies continue to reshape the global financial landscape, DTCC's new white paper represents a proactive approach. We endeavor to understand the potential disruptive implications quantum computing technology will have on the financial industry. As a critical industry infrastructure, we recognize our responsibility to anticipate – and mitigate – potential risk and increasing resilience."

- Rob Palatnick, DTCC Managing Director and Global Head of Technology Research and Innovation

BACKGROUND

Quantum computing leverages the phenomena of quantum physics to perform certain types of calculation many orders of magnitude faster than conventional binary computing. Its capabilities are simply unachievable for any number of traditional computers. Quantum computing will deliver new ways to analyze and solve complex problems, and therefore carries the potential to disrupt industries. Early adopters of quantum computing will be equipped to leap ahead of their competitors.

Quantum computing will grant greater capabilities to bad actors, too. This creates real risk for every organization because all organizations presently rely on encryption methods that will be vulnerable when quantum computers achieve greater levels of power. Quantum computing will pose a threat to today's cryptography within this decade.

Some readers will want to dig deeply into the science underpinning quantum computing's potential, but this paper focuses on how businesses can get ready for the new, quantum-related risks that are becoming evident today. Even though quantum computing may be several years away from broad commercial application (there are only about three dozen quantum computers on the cloud at present)[1], businesses are already facing new vulnerabilities in the form of bad actors who are even now planning quantum-based hacks.

Quantum Fundamentals

Quantum computers take advantage of quantum physics principles like superposition and entanglement. They use these quantum phenomena to perform calculations and encode data. Today's binary-based, classical computers store all information as bits — i.e., with values of zero or one. Quantum computers use quantum bits ("qubits") which can hold values of zero and one — and many combinations of those two values — simultaneously. Quantum computing achieves this through quantum's "superpositioning" phenomenon: being in more than one state at one time. Qubits are based on atoms to drive this capability.

Computer instructions (algorithms) that leverage quantum's capabilities will perform better — and use less energy — than today's classical computers.[2] While we'll see classical computing exist in parallel with quantum for the foreseeable future, within the decade quantum computers will outperform classical computers in certain contexts for governments and large institutions.

Cryptography 101

A better understanding of recent cryptology history helps clarify quantum risk.

Cryptography keeps information secret using various means. Documents, messages, and other data are written in human-readable language (**plaintext**), and an **encryption** scheme renders it unreadable (**ciphertext**) without the corresponding **decryption** key.[3] Cryptography lets parties exchange and store sensitive information in contexts like online banking, automatic teller machines, and the blockchain.

Public-key cryptography (PKC) uses a private key that's kept secret by the user to generate a public key that's shared with others. Users sign data with their private key, and anyone with the corresponding public key can verify it. It's also known as "**asymmetric cryptography.**" The RSA algorithm (named for its developers Rivest, Shamir and

[1] https://www.protiviti.com/US-en/insights/podcast-preparing-quantum-threat-cryptography-and-cryptocurrency

[2] https://www.protiviti.com/US-en/insights/newsletter-bpro139-quantum-computing

[3] https://people.math.umass.edu/~gunnells/talks/crypt.pdf

Adleman) is one popular public-key algorithm.[4] PKC's vulnerability is that the public key can be broken by a quantum computer.

Many classic encryption schemes — including PKC — rely on **factoring** to protect sensitive information. Factoring renders an integer as the product of smaller integers (for example, 15 is a product of 3 and 5.) That's a simple example, but encryption schemes rely on factoring integers containing hundreds of digits. Even using hundreds of classical computers in parallel, some of these integers take years to factor (and some can never be factored with classical computers at all).

In 1994, Massachusetts Institute of Technology (MIT) Professor Peter Shor[5] developed an algorithm that could calculate prime factors of the large numbers that PKC and other cryptographic schemes use. To operate **Shor's algorithm** would require a computer with "a large number of quantum bits" to make it many times more efficient than classical computers. In 1994, no such machine was available, and this matter was merely theoretical.

In 2016 however, researchers reported that they'd built a small-scale quantum computer that could carry out Shor's algorithm "with a confidence level exceeding 99%."[6] In the words of Isaac Chuang, professor of physics and professor of electrical engineering and computer science at MIT, "we show that Shor's algorithm, the most complex quantum algorithm known to date, is realizable in a way where, yes, all you have to do is go in the lab, apply more technology, and you should be able to make a bigger quantum computer."

A Few Cryptography Terms

Cryptography is "the discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification."[7]

Cryptology is the "science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence."[8]

Post-quantum cryptography (PQC) is a discipline within the field of cryptography whose goal is to keep existing "public key" infrastructure protected once quantum computing is broadly available to good and bad actors both. PQC is intended to keep both traditional and quantum computers secure, without making disruptive changes to today's protocols and infrastructure.[9]

Where is Cryptography Used Today?

Encryption is everywhere. It's on your mobile phone, it's in your bank card, and it's in most enterprise applications to protect the organization's most important data.

Encryption has been used in networking since the 1970s to ensure the privacy of messages between sender and receiver. Today, organizations use encryption to protect information privacy and security for data in each of these categories:

[4] https://csrc.nist.gov/glossary. Terms: public-key cryptography, RSA

[5] https://news.mit.edu/2016/quantum-computer-end-encryption-schemes-0303

[6] https://www.science.org/doi/10.1126/science.aad9480

[7] https://csrc.nist.gov/glossary/term/cryptography

[8] https://csrc.nist.gov/glossary/term/cryptology

[9] https://www.nist.gov/programs-projects/post-quantum-cryptography

- Data in transit: information in messages and files that are sent between different parties in a communication network.
- Data at rest: information stored in devices, including computers and servers in physical data centers, the cloud, mobile devices, or portable drives.
- Data in use: information as it's being processed from the time of its retrieval from storage through the time of output.

Governments and military organizations as well as commercial enterprises use encryption to protect secrets. Governments throughout the world create laws and regulations to mandate specific levels of encryption based on data sensitivity.

Over the past 25 years, the variety of encryption standards — and varying support from vendors for various categories of data — has created a security challenge. Now, many organizations use a wide variety of encryption technologies across their system portfolios, which complicates efforts to migrate data when encryption methods are changed or upgraded.

The Current State of Post-Quantum Cryptography

The United States Department of Commerce houses a department called the National Institute of Standards and Technology (NIST), which since 2016[10] has worked to develop standard approaches for PQC. Even with broad adoption of quantum computing still quite far off, NIST has responded to an "unprecedented urgency"[11] to develop quantum-resistant cryptography standards. This effort is known as PQC standardization.

PQC Standardization

NIST's goal is to specify "one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers."[12]

NIST began with an open call for new algorithm proposals in 2016. Researchers from 82 design teams in 25 different countries submitted candidates. Over the past six years, NIST has led efforts to analyze and reduce the candidate pool by evaluating security, performance, and other characteristics.[13]

Since the PQC standardization process began, NIST has led three rounds to evaluate new post-quantum cryptosystems by analyzing proposed algorithms in collaboration with the global cryptographic community.

- In December of 2018, President Trump signed into law the National Quantum Initiative Act (NQI Act) "to accelerate quantum research and development for the economic and national security of the United States." The NQI Act authorized NIST, the National Science Foundation, and the Department of Energy to strengthen quantum information science (QIS) programs, centers, and consortia. It also called for a coordinated approach to QIS research and development within the federal government.[14]

[10] https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms

[11] https://www.nccoe.nist.gov/news-insights/cornerstone-cybersecurity-cryptographic-standards-and-50-year-evolution

[12] https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms

[13] https://www.nccoe.nist.gov/news-insights/cornerstone-cybersecurity-cryptographic-standards-and-50-year-evolution

[14] https://www.quantum.gov/about/#OVERVIEW

- In July of 2020, NIST announced seven third-round finalists and eight alternate standardization candidates that are being considered for standardization.[15]
- In June of 2021, NIST held its third PQC Standardization Conference to discuss the fifteen candidates for standardization and get feedback for a final selection.[16]
- In July of 2022, NIST announced[17] the first four quantum-resistant cryptographic algorithms that "will become part of NIST's post-quantum cryptographic standard, expected to be finalized in about two years." Some experts were surprised at the speed with which NIST made these selections. They inferred that NIST shares the business and technology community's growing sense of urgency to act on the quantum security threat. At the same time, however, NIST cautioned against immediate application of the algorithms; an indication that these methods could still change. The announcement also mentioned that four additional algorithms remain under consideration for standardization. NIST hasn't set a date for completion of those assessments.

A release of draft standards is expected in 2023, and final publication of PQC standards is scheduled for 2024.[18]

Further PQC Developments

- In October 2021, NIST invited organizations to propose products and technical expertise — and demonstrate security platforms — for their Migration to Post-Quantum Cryptography project.[19] This step helped establish initial collaborations between technology companies and NIST's National Cybersecurity Center of Excellence (NCCoE) to tackle quantum-related cybersecurity challenges.
- In January 2022, the World Economic Forum published "Quantum Computing Governance Principles."[20] A global community of quantum experts, emerging technology ethics and law authorities, decision makers and policy makers, social scientists and academics co-designed the best-practice governance principles the report details to guide future design and adoption. "The critical opportunity at the dawn of this historic transformation is to address ethical, societal and legal concerns well before commercialization," said Kay Firth-Butterfield, Head of Artificial Intelligence and Machine Learning at the World Economic Forum. "This report represents an early intervention and the beginning of a multi-disciplinary, global conversation that will guide the development of quantum computing to the benefit of all society."[21]
- In May 2022, the White House released a "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems."[22] This document discusses mitigation of quantum risks "to the Nation's cyber, economic, and national security," and directs agency actions to migrate computer systems to quantum-resistant cryptography.

Given the status of PQC standardization and other developments, leaders are advised to watch for new information. While NIST has selected four algorithms to date, they've indicated those algorithms are not unchanging. In addition, NIST indicated they'll be selecting additional algorithms to include in their standard.

[15] https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement

[16] https://csrc.nist.gov/Events/2021/third-pqc-standardization-conference

[17] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[18] https://www.nist.gov/blogs/cybersecurity-insights/cornerstone-cybersecurity-cryptographic-standards-and-50-year-evolution

[19] https://www.federalregister.gov/documents/2021/10/13/2021-22223/national-cybersecurity-center-of-excellence-nccoe-migration-to-post-quantum-cryptography

[20] https://www3.weforum.org/docs/WEF_Quantum_Computing_2022.pdf

[21] https://www.weforum.org/press/2022/01/first-quantum-computing-guidelines-launched-as-investment-booms

[22] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems

We do not counsel waiting for announcement of PQC standard algorithms two years from now before taking action. There is ample work to be done now that will enable more rapid migrations and remediation once NIST announces the PQC standards in 2024.

WHY SYSTEMS ARE ALREADY AT RISK

Conventional cryptography relies on factoring that actually makes use of classical computing's limited power. Breaking today's cryptographic schemes would call for factoring large numbers in such a way that even all conventional computers, working together, couldn't complete the task in a million years.[23] Quantum computing will be able to take advantage of Shor's algorithm to obliterate classical computing's limits and render conventional computers and some of their current cryptography schemes useless.

Failures to upgrade to post-quantum encryption approaches will compromise the security of all electronic devices and systems that rely on soon-to-be outmoded encryption schemes, including mobile phones, enterprise and personal computing applications, communication networks, and cloud environments. Private information, bank accounts, health records, and cryptocurrency transactions will be vulnerable to quantum computer-powered hacking.

Over the past decade, multiple, widely publicized security breaches[24] have taken hundreds of millions of records. Organizations that suffer such attacks reassure stakeholders by stating that the data stolen from them was encrypted. The data in its encrypted state, however, could be retained by bad actors. These criminals are awaiting the availability of quantum-enabled decryption methods to unlock the data's secrets.

With quantum-enabled decryption likely to become possible in the next few years, much of the data stolen in the recent past will still have relevance and value.

Data stored in systems today is already at risk of post-quantum decryption. Why? Because bad actors — including criminals, terrorists, and rogue governments — may already be harvesting encrypted data today for quantum-driven decryption tomorrow. "The threat to information protected by asymmetric cryptography exists now because an adversary can collect currently encrypted data and break it when quantum computation becomes available."[25]

Knowing When to Worry

Quantum computing will compromise much of the cryptography that protects today's digital information. When bad actors gain access to quantum computers of sufficient power, today's cryptography will become vulnerable. Planning now for replacements of hardware, software, and processes that use today's public-key cryptography will help protect businesses from future attacks.[26]

[23] https://cs.stanford.edu/people/eroberts/courses/soco/projects/2004-05/cryptography/quantum.html

[24] How the FBI Got Colonial Pipeline's Ransom Money Back - WSJ

[25] https://www.dhs.gov/quantum

[26] https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

"Here at DTCC, we are well aware of the quantum threat. We wanted to be ready for that day, as well as for the day PQC standards became available. We knew if we made every preparatory step that's possible now, we might avoid an urgent scenario that recalled the rush of Y2K, where teams had to rush to prepare. We set out to improve our awareness, to understand our current risks, and give ourselves more time. We knew that enhancing our crypto-agility now – even as we await more guidance from experts and authorities – could only reduce disruption and potential vulnerability later." *- Ajoy Kumar, DTCC Managing Director and Chief Information Security Officer*

Security leaders may wonder how soon their organizations might experience the effects of post-quantum risk. The answer will vary by organization and by the data in question. Some data has a short lifespan. For instance, the details of an executed trade in an equity are highly valuable at the moment of trade execution and for a period of time thereafter, but that value diminishes as time goes on. Other data — like dates of birth or social security numbers — have value that will last beyond a lifetime.

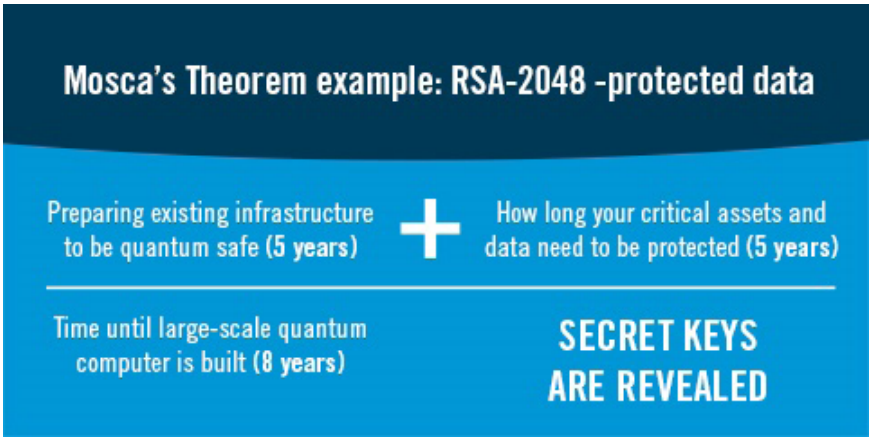
How Much Time Is Needed to Prepare for Post-Quantum Risk?

If the current expectations for quantum progress prove to be true, it is already time to be concerned about post-quantum risk. Mosca's Theorem calculates the time needed to prepare for post-quantum risk: consider the shelf life of a secret, add the time to upgrade to PQC, and get a deadline. Dustin Moody, a mathematician at NIST, described Mosca's Theorem in a presentation at NIST's 2015 Cybersecurity Innovation Forum.[27]

For each data asset:

- Determine how long the data encryption must remain secure.
- Estimate how long it could take to put a quantum-safe solution into place (e.g., replace the existing encryption).
- Forecast how many years it'll take until a large-scale quantum computer is built.
- If the length of time encryption must remain secure — together with the time it will take to put a quantum-safe solution in place — exceeds the time large-scale quantum computers are built, then secret keys related to the data asset will become easy for bad actors to expose.

[27] https://csrc.nist.gov/Presentations/2015/A-Quantum-World-and-how-NIST-is-preparing-for-fut



Mosca's theorem is used to calculate when RSA-2048-generated keys[28] will be compromised]

"You have to consider the amount of shelf life a secret has, plus the amount of time you expect to take to implement a new solution in the future. When you add those two together, you end up with several years that most likely passes the marker of when quantum computing becomes powerful enough to reverse encryption," Konstantinos Karagiannis, Director of Quantum Computing Services at Protivit said. "The time to start looking at this was yesterday."[29]

WHAT ORGANIZATIONS CAN DO TODAY

Moving toward Crypto-Agility

Organizations just starting to consider post-quantum readiness can make a good start by understanding their current state. The following classifications will help enterprises assess their status and provide a basis for articulating a strategy to prepare for post-quantum risk.

- Many or most organizations are **quantum-unaware** today. However diligent their senior leaders and security experts may be about current and conventional threats; they've not yet expanded their attention to more distant threats like post-quantum attacks.
- **Quantum-aware** organizations are already taking steps to build familiarity with quantum computing developments and forecasts among individuals and throughout teams. Their leaders are aware that there might be gaps in their computing environments which could inhibit the organization's crypto-agility if left unaddressed.
- **Crypto-advancing** organizations have begun establishing robust inventories of their critical data and cryptography in use as a basis for identifying gaps, if any. Leaders understand and monitor for imminent PQC risks, and they're working to articulate a strategy to protect critical data. They're developing processes to facilitate the migration from existing cryptography to quantum-safe encryption once standards emerge. They've already started assessing post-quantum approaches like messaging solutions that use hybrid (classical and post-quantum) ciphers, or point-to-point solutions like quantum key distribution.

[28] https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf

[29] https://www.protiviti.com/US-en/insights/podcast-preparing-quantum-threat-cryptography-and-cryptocurrency

- **Crypto-agile organizations** have change processes and appropriate resources ready to replace their existing cryptography algorithms and protocols without disrupting business operations or incurring undue costs. Their — and their third parties' — cryptography is well-documented and regularly maintained. A dedicated team is in place to monitor and oversee coming migrations to standardized PQC algorithms as they emerge.

The arrival of viable quantum computers will threaten today's encryption standards. **Crypto-agility** is the ability to deploy quantum-safe encryption mechanisms — once available — in a timely manner.

Becoming crypto-agile entails developing a new kind of literacy related to developments in the quantum computing world. Monitoring quantum computing concepts and trends now will equip organizations to understand the evolving PQC landscape, and clarify what to expect.

What to Do While Awaiting PQC Standards

Even as organizations await PQC standardization, there's plenty of work to be done now. It starts with prioritizing organizational change and post-quantum risk identification and management.

- **Size up the migration to come** by identifying systems and encryption mechanisms in scope for remediation. Organizations can inventory systems to identify those containing sensitive data as well as to understand encryption mechanisms used by the systems that contain sensitive data.
- **Strengthen cryptography practices** by centralizing management of keys and certificates, instilling standards for encryption mechanisms, and implementing change management for encryption solutions. Deploy encryption mechanisms based on data sensitivity. Upgrade today's information technology so it can support secure encryption practices (like key rotation and distribution). Automate processing to remove risks from manual interactions. Deprecate insecure protocols and security mechanisms throughout the system landscape.
- **Develop a playbook** to detail the steps needed to replace an encryption platform. Exercise the playbook through a pilot or prototype to ensure the steps can be successfully executed and to understand the time required.
- **Modify systems** to facilitate work to come. Separate data based on its sensitivity to help set priorities for remediation of encryption risks.
- **Start organizational change management (OCM) efforts** to build a strong risk culture and risk-based mindset throughout the organization. Objectives can include raising awareness among personnel and starting the conversation with customers and vendors about quantum risk. Establish a team to focus on post-quantum readiness, educate staff and trading partners, and drive the work described here. Provide quantum risk reporting to leaders.

EDUCATING THE ORGANIZATION

NIST's PQC Standardization Project and NIST Papers

NIST's PQC Standardization Project is an important resource to monitor to understand PQC developments. Readers can check for updates on NIST's PQC Standardization Project website30 or subscribe to NIST's general updates (which cover all NIST efforts).[31]

- "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms" [32] is a paper NIST has published to describe how quantum computing impacts classical cryptography — especially PKC. The paper also discusses PQC adoption challenges likely to come after PQC standardization is announced, as well as PQC migration planning requirements. NIST discussed its own next steps for "helping with the migration to post-quantum cryptography" in this paper.
- "Migration to Post-Quantum Cryptography," [33] describes NIST's National Cybersecurity Center of Excellence (NCCoE) initiative to facilitate migration from classical cryptography to PQC algorithms. The NCCoE plans a set of practices that "will take the form of white papers, playbooks, and demonstrable implementations for organizations." The intended audience includes not only providers of cryptographic standards and protocols, but also "enterprises that develop, acquire, implement, and service cryptographic products."

World Economic Forum

As part of its Centre for Cybersecurity Platform, the World Economic Forum (WEF) has embarked on The Quantum Security project, a "global multi-stakeholder initiative aiming to help build a secure quantum economy."[34] The effort will focus on identifying risks, raising awareness, and determining "emerging focus areas for future research, investment and governance."

Experts to Follow

- The Post-Quantum World Podcast[35] hosts quantum experts and business leaders to discuss and share insights and actions all organizations should be considering today to prepare for mass adoption of quantum computing.
- Protiviti's Technology Insights blog[36] features commentary, insights, and points of view from Protiviti's subject-matter experts on key technology challenges companies are facing, including quantum computing.

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

[31] Subscribe to updates on NIST activities at https://public.govdelivery.com/accounts/USNIST/subscriber/new [updates include all NIST activity; not just PQC]

[32] https://csrc.nist.rip/publications/detail/white-paper/2021/04/28/getting-ready-for-post-quantum-cryptography/final

[33] https://csrc.nist.rip/publications/detail/white-paper/2021/08/04/migration-to-post-quantum-cryptography/final

[34] https://www.weforum.org/global_future_councils/gfc-on-quantum-computing/projects/quantum-security

[35] https://blog.protiviti.com/2021/05/05/the-post-quantum-world-a-new-protiviti-podcast-series-explores-the-exciting-new-world-of-quantum-computing

[36] https://tcblog.protiviti.com/?s=quantum

CONCLUSION

The financial industry expects DTCC to take the long view and engage in strategic forward thinking about where technology is going. This is how DTCC sustains its mission "to deliver the world's most resilient, secure and efficient post-trade platform for our clients"[37] — into the post-quantum age.

Quantum computing will present more opportunities than today's experts have predicted, but it also brings new risk by invalidating some existing data-protection methods. DTCC is taking proactive steps today to ensure that all of its data — the financial industry's critical data — remains protected by the right PQC solutions, long into the future.

This paper is a call to action for financial industry leaders to begin the dialogue and to prepare for the emergence of PQC standards to ensure that the security, privacy, and integrity of the financial industry is sustained.

Preparing for post-quantum computing risk requires a multi-disciplinary approach that will benefit from insights from the widest array of subject matter experts and will be built on close coordination between all stakeholders – in line with DTCC's focus on "Advancing Financial Markets. Together." In that spirit, we encourage you to share your comments and feedback with us at pqc-info@dtcc.com.

[37] https://www.dtcc.com/about/our-corporate-strategy

For more information on our products and services, visit DTCC.com

For information on careers at DTCC, visit careers.dtcc.com

FOLLOW US ON

DTCC

ADVANCING FINANCIAL MARKETS. TOGETHER.™