Quantum Strategy Institute

QSI's Report on Cryptography:

Taking a Data-Driven Approach to the Quantum Computing Threat

Report Authored by Danika Hannon, Deputy Head and International Quantum Strategy Day Chair of the Quantum Strategy Institute (QSI).

In her role with QSI, Hannon writes thought leadership on quantum computing and business development, plus she leads International Quantum Strategy Day, which features a global strategy competition. In addition to her work with QSI, Hannon's earning a Cybersecurity Master's degree and will be graduating from the University of North Dakota in December 2024.

Hannon also focuses on giving back to the tech community as both a speaker and a mentor. In 2024, she'll be speaking at the Quantum Innovation Summit and South by Southwest. She's recently been nominated for a Femtum Leap Award in Quantum Leadership and in 2022, she was nominated for VentureBeat's Women in AI Awards in the Mentorship category. Added to that, she's served as a mentor with Girls in Quantum and Women in Quantum.

Afterword by Chuck Brooks, Chuck Brooks has been named the "Top Tech Person to Follow" by LinkedIn, Voted "Cybersecurity Person of the Year", Cited Top 10 Global Tech & Cyber Expert & Influencer, Georgetown University Professor, Two Time Presidential Appointee, FORBES writer, 113k LinkedIn Followers.

Brooks is the President of Brooks Consulting International and a Consultant with over 25 years of experience in cybersecurity, emerging technologies, marketing, business development, and government relations. He helps Fortune 1000 clients, organizations, small businesses, and start-ups achieve their strategic goals and grow their market share.

Brooks also serves as an Adjunct Professor at Georgetown University, where he teaches graduate courses on risk management, homeland security, and cybersecurity, and designed a certificate course on Blockchain technologies.

About QSI: QSI provides industry participants with ongoing insights into the progress in the field of quantum technologies through research, social media, and conference presentations. You can find more information about QSI on our website.

Quantum Strategy Institute

Contents

1. Introduction 4
2. What Types of Encryption are at Risk? 4
   - 2.1 What's Safe 5
   - 2.2 What's at Risk 5
   - 2.3 What This Means for You 5
3. Where Will the Attacks Come from and What Will the Targets Be? 6
4. What are the Timelines for this Threat Arriving? 6
   - 4.1 Pre-December 6, 2023 7
   - 4.2 Post-December 6, 2023 8
   - 4.3 Navigating the Different Expert Opinions 8
5. How Can My Business Prepare for This? 9
   - 5.1 Assess the Defensive Tools Available 9
   - 5.2 Migration Planning Guidance from DHS, NIST, CISA, and the NSA 10
   - 5.3 Talent Shortages and Legal Considerations 11
6. Looking Ahead 13
7. Afterword by Chuck Brooks 13
8. References 15

Quantum Strategy Institute

1. Introduction

Reactions to the idea of quantum computing breaking encryption range from uncertainty (at best) to fear (at worst). Given how harmful that is to businesses, this report breaks down the quantum computing threat from a US standpoint and explores these critical questions:

1. What types of encryption are at risk?
2. Where will the attacks come from and what will the targets be?
3. What are the timelines for this threat arriving?
4. How can my business prepare for this?

A data-driven approach will be used to explore each of those areas.

Because if you're going to face the changing landscape with confidence, then you'll need fact-based guidance.

2. What Types of Encryption are at Risk?

The confidentiality, integrity, and availability of information are the cornerstones of cybersecurity infrastructure.[1]

When it comes to keeping data confidential, cryptography is crucial to providing private and secure communications.[2] Although it's common to hear that quantum computing poses a threat to encryption, which seems to imply every type of encryption, the reality is more nuanced than that.

When the National Institute of Standards and Technology (NIST) began publicly assessing post-quantum cryptography in 2016, they pointed out something important: by using longer keys, symmetric key encryption will largely be safe from quantum, and hash functions will be fine as long as they have a larger output, but asymmetric (or public key encryption) will no longer be secure.[3]

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Image Credit: NIST[3]

2.1 What's Safe

In the case of symmetric key encryption, the Advanced Encryption Standard (AES) is a widely used algorithm that largely relies on 128-bit keys. In NIST's 2016 assessment, they initially recommended using larger key sizes to defend against the quantum computing threat; however, in 2018, updated guidance stated that while a large-scale quantum computer could use Grover's algorithm to run a brute-force attack, AES with key sizes 128, 192, or 256-bits would be able to withstand that.[3, 4]

In looking at guidance on hash functions, functions with 256-bits are expected to be safe from large-scale quantum computers, even when taking Grover's algorithm into consideration.[5]

2.2 What's at Risk

Public key encryption, which uses Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography, and Finite Field Cryptography is vulnerable. Shor's Algorithm poses a risk to RSA because it could eventually be used to factor large prime numbers, which would undermine the security that RSA provides.[6]

For Elliptic Curve Cryptography and Finite Field Cryptography, both rely on the difficulty of solving the elliptic curve discrete logarithm problem to provide security. Shor's Algorithm is a potential threat there, too, because it could one day be used to solve the underlying mathematics of the elliptic curve discrete logarithm problem.[6]

2.3 What This Means for You

Broadly speaking, symmetric key encryption protects data at rest and public key encryption guards data in transit.[7] (Please note that data in use is out of scope for this report because encrypting that is an emerging practice.[8]) By clarifying what types of encryption will be impacted by large scale quantum computers, the threat's scope can be narrowed. And more thoughtful conversations can be had on how to approach this from a defensive standpoint, which starts with looking at where threats will come from.

3. Where Will the Attacks Come from and What Will the Targets Be?

In taking an innovative approach to threat intelligence, the Intelligence Advanced Research Projects Activity (IARPA) is using behavioral analysis to look at who threat actors are, what motivates them, and what their goals are.[9]

That same strategy will be used here.

Identifying the Threat Actors	Of the private companies, research institutions, and nation-states that are building quantum computers, quantum computing-based attacks will likely come from nation-states.[10, 11] This is for a couple of reasons: 1. Private entities and research institutions will have legal protections in place to restrict their customers from using a quantum computer to launch a decryption attack. 2. Buying time on a quantum computer is cost prohibitive, putting this tool out of reach for many.
Their Goals	The goal of nation-state actors will be to destabilize national critical functions. According to the Cybersecurity Infrastructure Agency (CISA), these functions are vital to the point where a major disruption in their operations would have a debilitating impact on national security, economics, public health, safety, or a combination of those areas.[10]
Their Targets	Attacks will focus on infrastructure that connects, distributes, manages, and supplies critical services.[10, 12] Altogether, that infrastructure includes 55 different functions, which range from the banking sector to electricity generation.[11] Further, in a National Security Memorandum from 2021, the White House stated that public and private sectors could be targeted, given that each supports public infrastructure.[13] As an added wrinkle, in the US the majority of infrastructure is privately owned. While it's difficult to find exact figures on this, in 2009 the Department of Homeland Security (DHS) estimated that private entities have 85% ownership.[14, 15]

4. What are the Timelines for this Threat Arriving?

There's not a clear-cut answer on when a large-scale quantum computer will be available, with the National Security Agency (NSA) acknowledging that expert estimates on this vary widely.[16]

From a US government standpoint, DHS and NIST released joint guidance on preparing for post-quantum cryptography and included a timeline showing that a large-scale quantum computer may exist by 2030.[17]

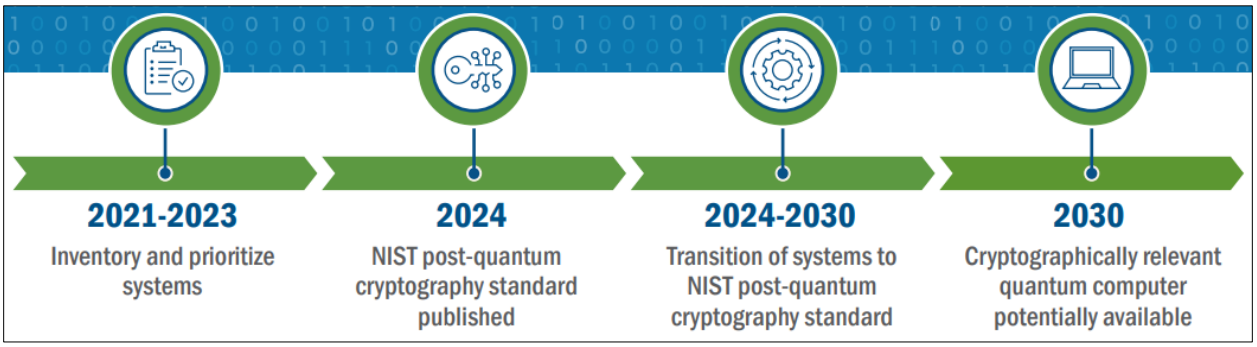


Image Credit: DHS and NIST[17]

The challenge with that analysis is it didn't include guidance on how DHS and NIST reached that conclusion and it left out data that can provide more insight into that, like the number of qubits needed to pose a threat.

From an industry perspective, a few quantum computing companies, including Classiq, Fujitsu, and Microsoft, have given resource estimates for how many logical qubits are needed to break RSA 2,048-bit encryption.

Additionally, in a recent development on December 6, 2023, a Defense Advanced Research Projects Agency (DARPA)-funded study came out that found a way to significantly decrease the number of physical qubits needed to create a logical qubit; so, resource estimates will be looked at in the context of pre-December 6, 2023 and post-December 6, 2023.

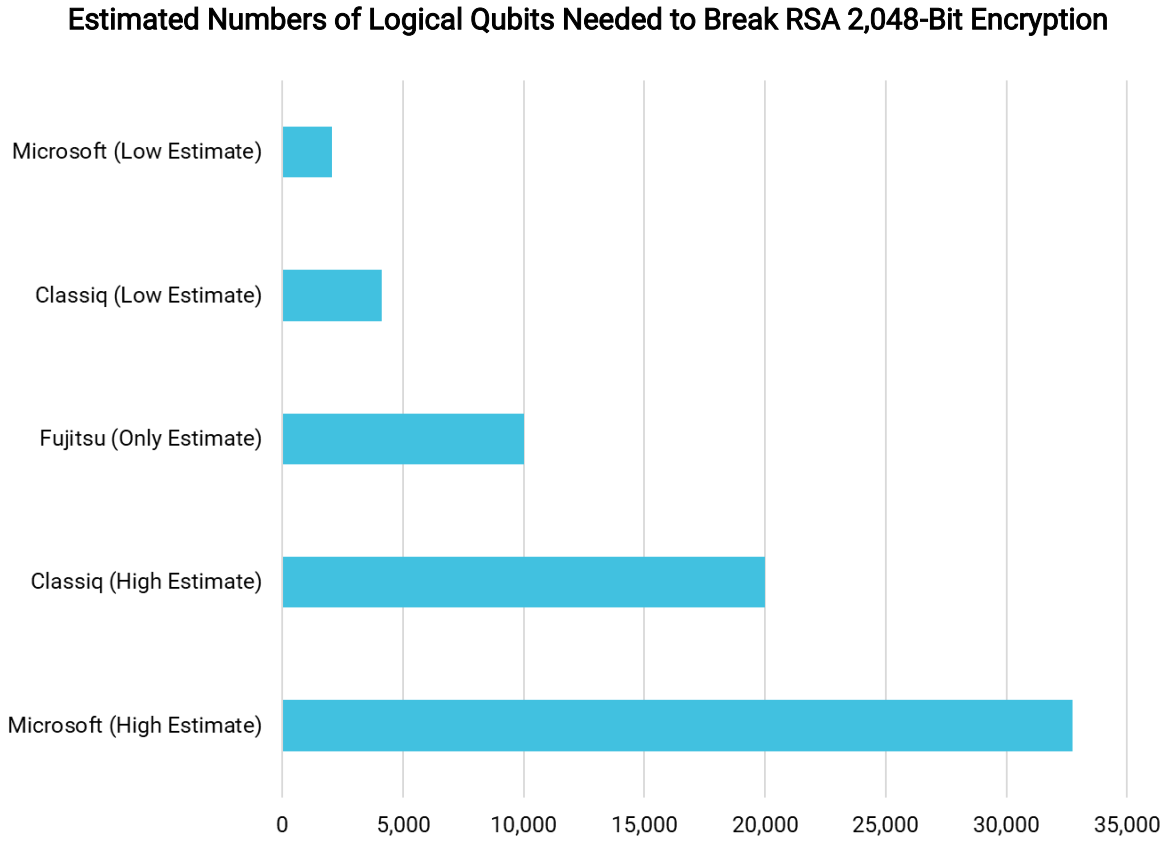
4.1 Pre-December 6, 2023

Both Classiq and Microsoft looked at independent research to gauge how many logical qubits would be needed to pose a threat to RSA, 2,048-bit encryption.

For Classiq, their lowest estimate was 4,099 logical qubits and their highest was 20,000.[18] Likewise, Microsoft took a similar approach and found the lowest number of logical qubits needed would be 2,050, with the highest being 32,755.[19]

Fujitsu took a different approach and they used their own quantum simulator to create a resource estimation of 10,000 qubits.[20] A hiccup with that figure is that Fujitsu didn't specify if they meant physical or logical qubits.

Given that it's estimated that 1,000 physical qubits are needed to make a single logical qubit, it'd be valuable to get clear guidance on if Fujitsu was referring to physical or logical qubits. But in looking at their figure alongside Classiq's and Microsoft's, Fujitsu likely meant logical qubits.[18, 19, 20, 21, 22]



4.2 Post-December 6, 2023

In challenging the industry understanding that 1,000 physical qubits are needed to make one logical qubit, new research (that was funded in part by a DARPA grant and led by researchers from Harvard, MIT, QuEra Computing, Caltech, and Princeton) used 280 physical qubits to create 48 logical qubits.[23] As a ratio, roughly six physical qubits were needed to make one logical qubit.

The researchers' paper didn't touch on the implications for cybersecurity, but if their work can be scaled up and adopted by industry players, then it will reduce the amount of time needed to create a large-scale quantum computer.[24]

4.3 Navigating the Different Expert Opinions

Even with guidance from DHS and NIST, the figures from pre-December 6th, and the recent breakthrough, it's still uncertain when a large-scale quantum computer will be available.

One way to approach that is by looking at the publicly available roadmaps that quantum computing companies release on their hardware projections. While the forecasts are just that, forecasts, and companies may fall short of their goals or exceed them, they're valuable for gauging the rate at which quantum computers are scaling.

If you're new to looking at this type of forecast, IBM's roadmap is a good place to start because it has projected qubit counts through 2030.[25]

5. How Can My Business Prepare for This?

Every company will need to take a unique approach that takes their factors into consideration.

In creating your strategy, here are things to consider:

1. Assess the defensive tools available.
2. Migration planning guidance from DHS, NIST, CISA, and the NSA.
3. Talent shortages and legal considerations.

5.1 Assess the Defensive Tools Available

Currently, quantum key distribution (QKD), quantum random number generators (QRNGs) / classical random number generators (RNGs), and the NIST candidate algorithms are the most widely known defensive tools.

The NSA doesn't recommend QKD for use in national security systems because they've identified inherent security vulnerabilities in that approach, which range from increased implementation costs and exposure to insider threats, to the difficultly of upgrading and maintaining QKD equipment. Further, they've stated that until those concerns are remedied, they won't recommend this tool.[26]

When it comes to QRNGs / classical RNGs, the NSA has taken a more neutral approach. Ultimately, their position is that the use of random number generators is a complex decision and many factors must be taken into account when making that assessment.[16]

In looking at the third option, the NSA has strongly endorsed candidates that NIST is reviewing, even though the final recommendations won't be ready until sometime in 2024.[16]

NIST, which put out a call for post-quantum cryptography algorithms in 2016, has narrowed down the initial pool of 69 candidates to four.[27]

This includes:

- CRYSTALS-Kyber, which is meant for general encryption purposes, like creating secure websites.
- CRYSTALS-Dilithium, for protecting digital signatures when signing documents remotely.
- SPHINCS+, for digital signatures.
- FALCON, which is also for digital signatures.

Of those candidates, the NSA has already added CRYSTALS-Kyber and CRYSTALS-Dilithium to its Commercial National Security Algorithm Suite 2.0 (CNSA 2.0).[16]

5.2 Migration Planning Guidance from DHS, NIST, CISA, and the NSA

In an effort to support the private sector, DHS, NIST, CISA, and the NSA have put together guidance on how to prepare for large-scale quantum computers.

First, DHS and NIST released a seven step process that any organization can use to start preparations early.[28]

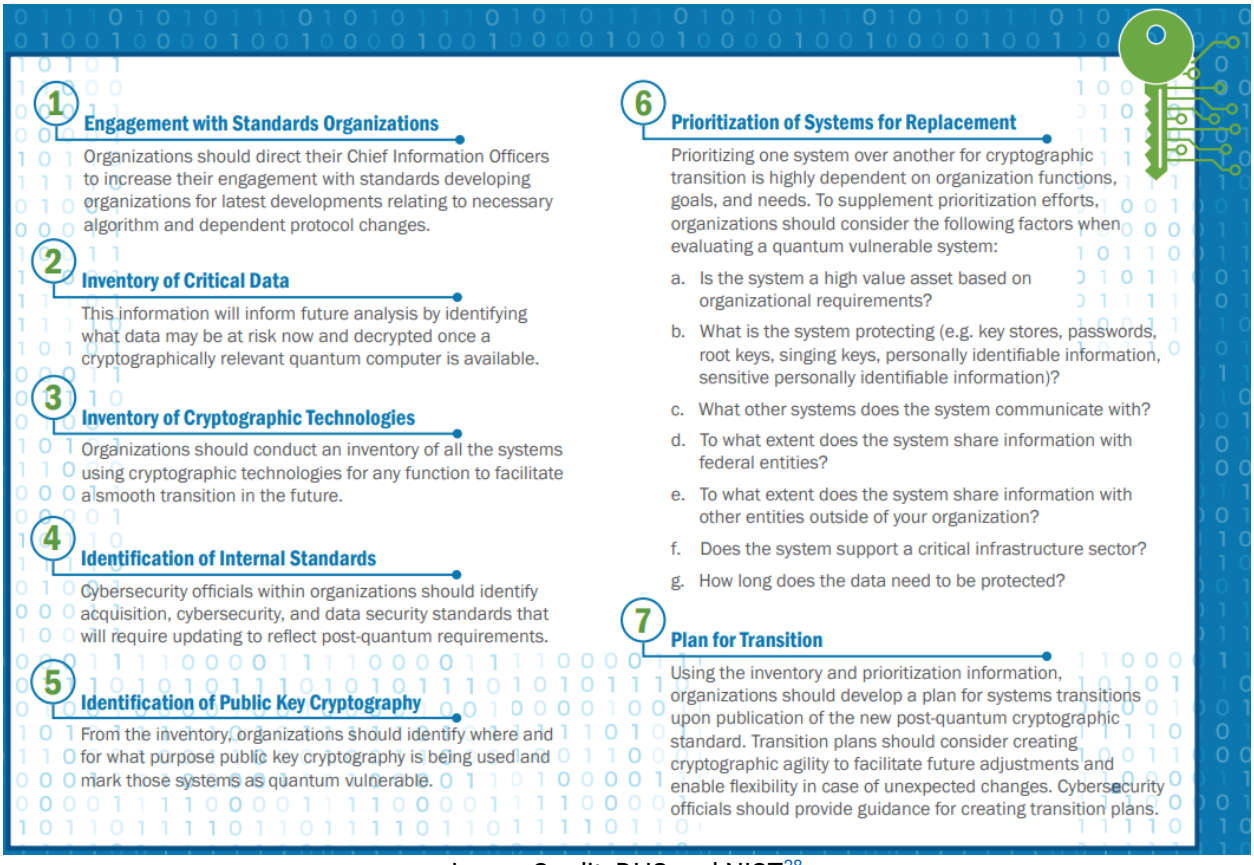


Image Credit: DHS and NIST[28]

In supporting leaders who are proactively thinking about the impacts of a large-scale quantum computer, CISA's National Risk Management Center created a strategy game called, "Alternative Futures: Quantum Technologies." It's designed to get teams to look at the changing threat landscape and use long-range thinking to build their own response plan.[29]

Then, in what could create a ripple effect, CISA, the NSA, and NIST made a joint recommendation for companies to talk with their vendors about their post-quantum roadmaps. Their guidance is broadly applicable and applies to on premises, off-the-shelf products and cloud based products.[30]

For the NSA's part, in a 2022 report they laid out their timelines for adopting quantum-resistant algorithms in national security systems.[16]

Given their unique position, the NSA's moving quickly and started updating their national security systems in 2022. While page six of their FAQs sheet on post-quantum cryptography says their goal is to have CNSA 2.0 in place by 2035, page seven indicates they're aiming to update all their systems by 2033, which creates a two-year grace period.[16]

National Security Systems to be Protected	Transition Start Date	CNSA 2.0 to be Supported and Preferred by:	CNSA 2.0 is Exclusively in Use by:
Software- and Firmware-Signing	2022	2025	2030
Web Browsers / Servers and Cloud Services	Not publicly known	2025	2033
Traditional Networking Equipment (e.g., Virtual Private Networks, Routers)	Not publicly known	2026	2030
Operating Systems	Not publicly known	2027	2033
Niche Equipment (e.g., Constrained Devices, Large Public-Key Infrastructure Systems)	Not publicly known	2030	2033
Custom Applications and Legacy Equipment	Not publicly known	Not publicly known	2033

5.3 Talent Shortages and Legal Considerations

As the cybersecurity industry matures, two notable things have happened. The first is that talent shortages have proven to be a chronic issue. The second is that US regulators have recently introduced new legislation around cybersecurity.

Both of those things may impact how your business prepares for large-scale quantum computers.

Talent Shortages in the US

The cybersecurity industry has been facing an ongoing talent shortage for years. $(ISC)^2$, which creates an annual report on the global cybersecurity workforce, found that 67% of the companies they surveyed have staffing shortages. Further, those gaps made it more difficult for businesses to prevent and troubleshoot cybersecurity issues.[31]

In looking at the US, $(ISC)^2$ estimated that the cybersecurity workforce grew 11% from 2022 to 2023. In spite of that, there's still a shortfall of nearly half a million professionals and the need for more cybersecurity talent increased by 18% during that same time period.

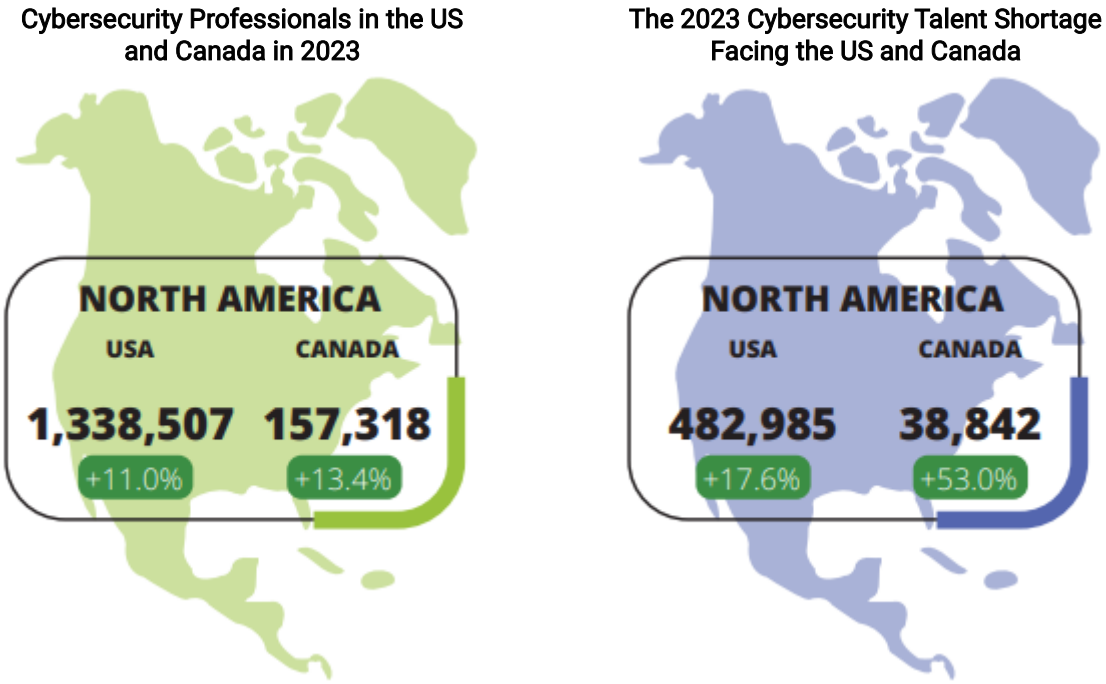


Image Credit: (ISC)[231]

Viewing this through a quantum computing lens, the talent shortages are also severe – to the point where they've been identified as a national security vulnerability for the US and Canada.[32, 33, 34]

From a leadership standpoint, as you consider the migration recommendations from DHS and NIST, you'll need to consider what talent you have available and how you'll factor that into your own plans.

The Changing Regulatory Landscape

On July 26, 2023, the Securities and Exchange Commission's (SEC) Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure rule went into effect. In an effort to provide more visibility into security incidents, the SEC's new requirement states:

- "… we are adopting amendments to require current disclosure about material cybersecurity incidents. We are also adopting rules requiring periodic disclosures about a registrant's processes to asses, identify, and manage material cybersecurity risks, management's role in assessing material cybersecurity risks, and the board of directors' oversight of cybersecurity risks."[35]

In a statement about the rule, the SEC said that their goal isn't to make recommendations on how businesses approach cybersecurity. Instead, their aim is to help investors understand how public companies are managing their cybersecurity risks by requiring that businesses make annual disclosures about material incidents.[36]

As leaders evaluate the tools, migration plans, and resources available to them, the SEC's new rules are an added complexity to keep in mind.

6. Looking Ahead

The promise of large-scale quantum computers isn't going away, even as the timing of their arrival remains unclear.

While quantum computers hold potential to solve some of the world's most pressing problems, they'll bring new challenges to cryptography.

As you look at what's next for you and your teams, you can walk away with data-driven guidance on the emerging threat landscape and how to face this. And when you're ready to act, you can do so with confidence.

7. Afterword by Chuck Brooks

Without a doubt, quantum technology—particularly quantum computing—has enormous promise to transform a wide range of industries, including communications, real-time data analytics, biotechnology, genetic sequencing, and materials research.

By affecting the field of artificial intelligence and the metaverse, quantum computing will also hasten the future. However, in addition to the good, we also need to prepare ahead and stop the bad—most importantly, data, which is essential to economies and trade.

It is crucial to take a quantum-proof cybersecurity path from the beginning. Large-scale quantum computers will be able to utilize Shor's method to break all public key systems that use integer factorization-based (and other) cryptography on what quantum researchers have dubbed "Q-Day."

I spoke on the urgency of a Q-Day or quantum apocalypse in my talk, "A look into Commercialising Quantum 2022 in London," at an Economist conference. My talk centered on the fact that if Quantum computers, if placed in the wrong hands, it would have the potential to constitute geopolitical threats due to their superior speed and accuracy over classical computers.

Additionally, I noted that the same computational power that makes it possible to tackle complicated problems can also be used to compromise cybersecurity. This is due to the fact that current cybersecurity protocols usually encrypt sensitive data, like passwords and personal information, using pseudo-random numbers.

However, quantum computers will be able to break the techniques used by traditional computers to generate random numbers, which poses a serious risk to any organization that uses standard encryption tools. We have to begin getting prepared for these quantum challenges, as the threats are arriving sooner rather than later.

- Chuck Brooks, "Top Tech Person to Follow" by LinkedIn, Voted "Cybersecurity Person of the Year", Cited Top 10 Global Tech & Cyber Expert & Influencer, Georgetown University Professor, Two Time Presidential Appointee, FORBES writer, 113k LinkedIn Followers.

8. References

1. NIST – National Cybersecurity Center of Excellence. NIST Special Publication 1800-26A, Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events. https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html
2. International Information System Security Certification Consortium. Certified Information Systems Security Professional Official Study Guide.
3. NIST. NISTIR 8105, Report on Post-Quantum Cryptography. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf
4. NIST. Post-Quantum Cryptography FAQs. https://csrc.nist.gov/projects/post-quantum-cryptography/faqs
5. National Academies Press. Quantum Computing: Progress and Prospects. https://nap.nationalacademies.org/read/25196/chapter/6
6. Arxiv. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. https://arxiv.org/pdf/quant-ph/9508027.pdf
7. Google Cloud. Encryption in Transit. https://cloud.google.com/docs/security/encryption-in-transit
8. VentureBeat. Why Data-in-Use Encryption is Essential to Data Security, Vaultree Raises $12.8M. https://venturebeat.com/security/data-in-use-data-security/
9. The Wall Street Journal. U.S. Intelligence Wants to Use Psychology to Avert Cyberattacks. January 25, 2023. https://www.wsj.com/articles/u-s-intelligence-wants-to-use-psychology-to-avert-cyberattacks-11674670443?st=8939icyazfhz6mr&reflink=desktopwebshare_permalink
10. CISA. CISA Insights: Preparing Critical Infrastructure for Post-Quantum Cryptography. August, 2022. https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf
11. Congressional Research Service. Preparing Secrets for a Post-Quantum World – National Security Memorandum 10. May 9, 2022. https://crsreports.congress.gov/product/pdf/IN/IN11921
12. CISA. National Critical Functions Set. https://www.cisa.gov/national-critical-functions-set
13. The White House. National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. July 28, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/
14. United States Government Accountability Office. Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector. November, 2021. https://www.gao.gov/assets/gao-22-104462.pdf
15. United States Government Accountability Office. The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report. June 26, 2009. https://www.gao.gov/assets/gao-09-654r.pdf
16. NSA. Cybersecurity Information Sheet: The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF
17. DHS. Preparing for Post-Quantum Cryptography Infographic. https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf
18. Classiq. Quantum Cryptography – Shor's Algorithm Explained. https://www.classiq.io/insights/shors-algorithm-explained
19. IEEE Explore. Quantum Computing: Codebreaking and Beyond. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8490171

20. Fujitsu Limited. Fujitsu Quantum Simulator Assesses Vulnerability of RSA Cryptosystem to Potential Quantum Computer Cryptography Threat. https://www.fujitsu.com/global/about/resources/news/press-releases/2023/0123-01.html
21. NewScientist. Google Demonstrates Vital Step Towards Large-Scale Quantum Computers. https://www.newscientist.com/article/2283945-google-demonstrates-vital-step-towards-large-scale-quantum-computers/
22. QuEra. Logical Qubit. https://www.quera.com/glossary/logical-qubit#:~:text=The%20ratio%20that%20is%20commonly,physical%20qubit%20per%20logical%20qubit.
23. DARPA. DARPA-Funded Research Leads to Quantum Computing Breakthrough. https://www.darpa.mil/news-events/2023-12-06
24. Nature. Logical Quantum Processor Based on Reconfigurable Atom Arrays. https://www.nature.com/articles/s41586-023-06927-3
25. IBM Technology Atlas. Quantum Roadmap. https://www.ibm.com/roadmaps/quantum.pdf
26. NSA. Quantum Key Distribution (QKD) and Quantum Cryptography (QC). https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
27. NIST. NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers. https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers
28. DHS. Preparing for Post-Quantum Cryptography Infographic. https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf
29. CISA. Matrix Game: Quantum Technologies. https://www.cisa.gov/resources-tools/resources/matrix-game-quantum-technologies
30. CISA, NSA, and NIST. Quantum Readiness: Migration to Post-Quantum Cryptography. https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf
31. $(ISC)^2$. $(ISC)^2$ 2023 Cybersecurity Workforce Study: How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e
32. Center for a New American Security. The United States' Quantum Talent Shortage Is a National Security Vulnerability. https://www.cnas.org/publications/commentary/the-united-states-quantum-talent-shortage-is-a-national-security-vulnerability
33. Government of Canada. Canada's National Quantum Strategy. https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy
34. Canadian Global Affairs Institute. The Quantum Revolution: Opportunities and Challenges for Canada. https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/4835/attachments/original/1634751916/The_Quantum_Revolution_Opportunities_and_Challenges_for_Canada.pdf?1634751916
35. SEC. Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. https://www.sec.gov/files/rules/final/2023/33-11216.pdf
36. SEC. Statement: Cybersecurity Disclosure. https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214#:~:text=In%20July%20of%20this%20year,rules%20will%20provide%20investors%20with