Protecting and Securing Data from the Quantum Threat

Dr. Georgianna Shea and Annie Fixler

Executive Summary

Over the next decade, quantum computing will unlock new technological advances and upend the current security landscape. Quantum computers of sufficient size and sophistication could "jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions," the White House cautioned in May.[1] "In short," warned a separate report from the National Counterintelligence and Security Center, "whoever wins the race for quantum computing supremacy could potentially compromise the communications of others."[2]

Once a quantum computer becomes sophisticated and large enough to be considered a threat to modern-day encryption, it is called a cryptanalytically relevant quantum computer, or CRQC.[3] Some experts expect quantum computing will become a risk to modern-day encryption within three years, although others put the number in the high twenties.[4]

There are two ways to provide security against the quantum threat. The National Institute of Standards and Technology (NIST) has been taking a "computational infeasibility" approach, which aims to develop encryption of such great complexity that no amount of computing power is realistically sufficient to breach it. To that end, NIST has been researching and testing new algorithms and developing post-quantum encryption standards that should be available by 2024.[5] Once they are available, NIST expects it will take another five to fifteen years for organizations to migrate to the new standards.[6] Yet if the migration takes that long, many users will become vulnerable to cyber breaches if CRQCs emerge in the next several years.

To help prepare for this risk of ineffective encryption, FDD's Transformative Cyber Innovation Lab (TCIL) explored an alternative approach that government agencies and private companies can implement more quickly so they are prepared to face the quantum threat.

The alternative TCIL tested is based on the principle of information-theoretic security, which remains effective even when unlimited time and computing power are available to the adversary.[7] Working with the data security experts at

1. The White House, Briefing Room, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," May 4, 2022. (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/)

2. National Counterintelligence and Security Center, Office of the Director of National Intelligence, "Protecting Critical and Emerging U.S. Technologies from Foreign Threats," October 2021, page 5. (https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_Emerging%20Technologies_Factsheet_10_22_2021.pdf)

3. The White House, Briefing Room, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," May 4, 2022. (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/)

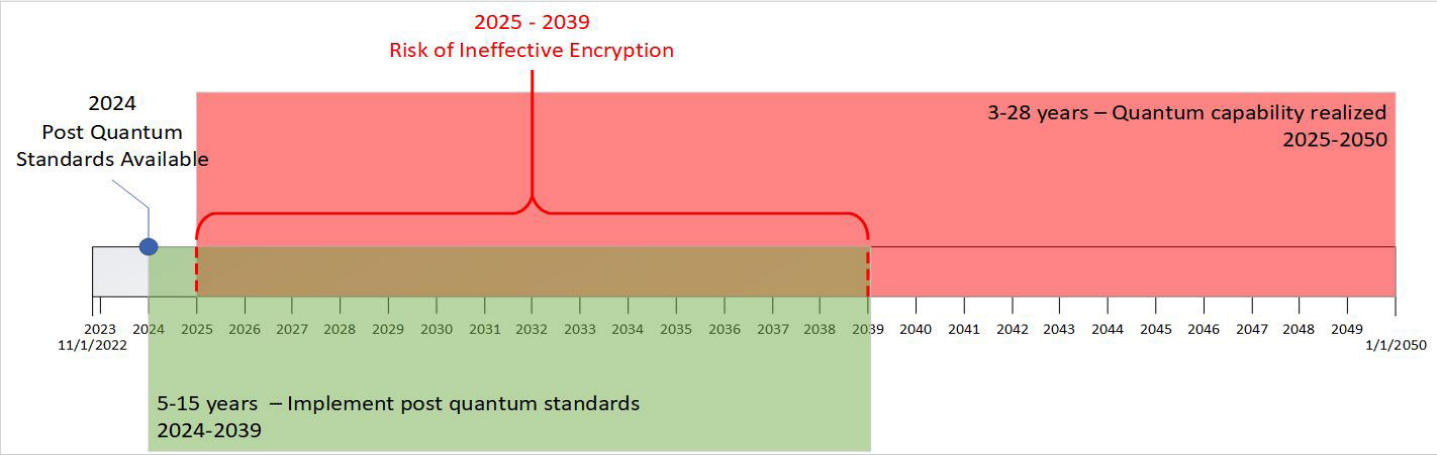
4. Michele Mosca and Marco Piani, "Quantum Threat Timeline Report 2020," *Global Risk Institute*, January 2021, page 30. (https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/)

5. "Computer Security Resource Center: Post-Quantum Cryptography PQC," *National Institute of Standards and Technology*, accessed November 28, 2022. (https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline)

6. William Barker, William Polk, and Murugiah Souppaya, "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms," *National Institute of Standards and Technology, Computer Security Resource Center*, April 28, 2021, page 2. (https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932330)

7. Ueli Maurer, "Information-Theoretic Cryptography," *Department of Computer Science, Swiss Federal Institute of Technology*, August 1999. (https://crypto.ethz.ch/publications/files/Maurer99.pdf); For additional research on information-theoretic security, visit https://crypto.ethz.ch/~maurer/publications.html

Figure 1: Quantum timeline



Cyber Reliant — a company specializing in data security[8] — TCIL walked through onboarding an enterprise-wide security strategy we have dubbed augmented improbability of access (AIA), which applies the principles of information-theoretic security to defend against CRQCs.

AIA strategies also mitigate the risk that adversaries will steal encrypted data today and wait to decrypt it until CRQCs are available. AIA strategies prevent the adversary from collecting sufficient components to decrypt stolen data, even if victims are not using post-quantum encryption.

This pilot project's goal is to better inform organizations how to enhance security and mitigate the diminishing lifespan of current encryption algorithms without having to wait for NIST's new encryption standards. TCIL's research findings conclude that the U.S. government and private entities should pursue AIA solutions.

What is Quantum Computing?

Quantum computing exponentially increases computational power when addressing certain problems, reducing the time required to solve complex mathematical calculations. In classical computing, the smallest unit of data is a bit, expressed as either a one or a zero. In quantum computing, the smallest unit is called a qubit and can exist in multiple states at the same time. It is as if a light switch is not on or off but both on and off simultaneously. The result is that a CRQC can simultaneously test multiple solutions to the mathematical problem rather than one at a time.

The difference between classical computing and quantum computing is like the difference between a mouse running through a maze to find a piece of cheese and a cloud of smoke spreading through the same maze.[9] The mouse can only test one path at a time. If it hits a wall, it must go back and restart down a new path. On the other hand, when the smoke reaches an intersection, it will travel in both directions simultaneously until it reaches the end of the maze. Unless the mouse is very lucky and happens to choose the right path on the first try, the smoke will always reach the cheese before the mouse. Quantum computing technology allows the user to compute multiple calculation streams simultaneously to reach the answer more quickly.

8. "Cyber Reliant," *Cyber Reliant*, accessed November 28, 2022. (https://www.cyberreliant.com)

9. Ajay Narayanan, "Quantum Superposition and what that means to Quantum Computation," *Becoming Human: Artificial Intelligence Magazine*, October 23, 2019. (https://becominghuman.ai/quantum-superposition-and-what-that-means-to-quantum-computation-3fbb5a711b9a)

Calculations taking 10,000 years to complete with current systems could be finished in just one second using quantum technology, making it 100 million times faster than classical computers.[10] This kind of power could help attackers overcome some existing encryption algorithms that are based on the factorization of two very large prime numbers. It would take billions of years for a classical computer to test all the combinations of prime numbers to crack today's encryption, known as 2048-bit RSA encryption. Using quantum computing, it could take as little as eight hours.[11]

Conventional security processes involve storing data and applying access controls (like passwords) to the information and the systems that store it.[12] U.S. adversaries have demonstrated they can defeat those controls. Thus, defensive measures now include encrypting the data itself. Yet once adversaries have CRQCs, they will be able to break through this encryption rapidly.

The Current Approach to Post-Quantum Encryption

At present, 2048-bit RSA encryption protects national security secrets, financial data, personal communications, and many other forms of information. Recognizing the impending obsolescence of such encryption, Congress passed, and President Donald Trump signed, the National Quantum Initiative Act of 2018[13] to ensure continued U.S. leadership of quantum research and application.[14] One provision of the law calls for greater interagency coordination through the Subcommittee on Quantum Information Science (SCQIS) within the National Science and Technology Council.[15] The SCQIS conducted a strategic review of quantum technology within the United States, resulting in policy recommendations, including greater engagement with academic and research communities to advance quantum research.[16] While acknowledging the need for quantum-resistant encryption, the report provides no recommendations on meeting this need.

The Biden administration has continued efforts to advance quantum information science while beginning to prioritize post-quantum encryption. The January 2022 White House Memorandum on Improving the Cybersecurity of National Security[17] requires the Department of Defense and Intelligence Community Systems to develop a plan to transition all

10. Emily Reynolds, "Google's quantum computer is 100 million times faster than your PC," *Wired*, September 12, 2015. (https://www.wired.co.uk/article/google-quantum-computing-d-wave)

11. Emerging Technology from the arXiv, "How a quantum computer could break 2048-bit RSA encryption in 8 hours," *MIT Technology Review*, May 30, 2019. (https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/)

12. Federal systems and many critical infrastructure operators use NIST's Risk Management Framework as a process for implementing cybersecurity. This approach, however, focuses primarily on implementing and monitoring protections, not assessing a system's overall security and resilience. Entities can choose from over 1,000 different protections within the NIST catalog of controls. The more stringent the data classification, the more controls an entity should add. Next, an assessment team reviews the implementation of each control. The result is a security assessment based on compliance rather than the system's actual security. See: U.S. National Institute of Standards and Technology, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf)

13. National Quantum Initiative Act, Pub. L. 115-368, 132 Stat. 5092. (https://www.congress.gov/bill/115th-congress/house-bill/6227)

14. "National Quantum Initiative: The Federal Source and Gateway to Quantum R&D Across the U.S. Government," *National Quantum Coordination Office*, accessed November 28, 2022. (https://www.quantum.gov/)

15. "About the National Quantum Initiative," *National Quantum Coordination Office*, accessed November 28,2022. (https://www.quantum.gov/about/#SCQIS)

16. U.S. National Science & Technology Council, Subcommittee on Quantum Information Science, "National Strategic Overview For Quantum Information Science," September 2018. (https://www.quantum.gov/wp-content/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf)

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

national security systems to an NSA-approved quantum-resistant algorithm.[18] Then on May 4, the president issued an executive order and a national security memorandum promoting the advancement of U.S. quantum technology and addressing the risk of quantum computing to cyber, economic, and national security, respectively.[19] The executive order notes, "Any digital system that uses existing public [encryption] standards … or that is planning to transition to such cryptography, could be vulnerable to an attack" by a quantum computer of sufficient size and sophistication. The order calls for prioritizing a timely and equitable transition to quantum-resistant cryptography to mitigate as much of the quantum risk as is feasible by 2035.[20]

Meanwhile, NIST (a member of the SCQIS) and other organizations are doing vital work to develop standards for post-quantum encryption that can resist the code-breaking power of a CRQC.[21] NIST's approach focuses on increasing the computational infeasibility of algorithms. In July, NIST announced the successful testing and selection of the first four algorithms that will become part of NIST's post-quantum encryption standard.[22] However, once NIST publishes the standards and the guidance on transitioning to them, it will take another five to fifteen years for the government, companies, and other organizations to adopt this new standard.[23] While some of this delay is the result of how long it takes to update hundreds of thousands of devices and replace equipment that cannot be updated, it is also driven in part by government policy decisions on when agencies and regulated industries will be required to meet this new standard.

At this rate, however, CRQCs may be available before the broad implementation of post-quantum encryption. The U.S. government's current approach to developing quantum-resistant security is simply moving too slowly.

The Proposed Quantum Protection Solution

In the nineties, private companies and government agencies addressed the Y2K challenge with a sense of urgency because they knew precisely when it would materialize. In contrast, a lack of certainty contributes to complacency about the quantum threat. Depending on the expert asked, quantum computing will render today's encryption methods obsolete in anywhere from three to 28 years.[24] For decades, the finish line has been far off since quantum computing

18. U.S. National Security Agency, Central Security Service, "Commercial National Security Algorithm Suite," August 19, 2015. (https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm)

19. The White House, Briefing Room, "FACT SHEET: President Biden Announces Two Presidential Directives Advancing Quantum Technologies," May 4, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/); The White House, Briefing Room, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," May 4, 2022. (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/); The White House, Briefing Room, "Executive Order on Enhancing the National Quantum Initiative Advisory Committee," May 4, 2022. (https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/04/executive-order-on-enhancing-the-national-quantum-initiative-advisory-committee/)

20. The White House, Briefing Room, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," May 4, 2022. (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/)

21. Georgianna Shea and Matthew Brockie, "U.S. Standards Body Reaches Critical Milestone for Mitigating the Quantum Threat, But More Work Is Needed," *The Foundation for Defense of Democracies*, July 19, 2022. (https://www.fdd.org/analysis/2022/07/19/us-standards-body-quantum-threat/)

22. National Institute of Standards and Technology, Press Release, "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," July 5, 2022. (https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms)

23. National Institute of Standards and Technology, Computer Security Resource Center, "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms," April 28, 2021, page 2. (https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932330)

24. Michele Mosca and Marco Piani, "Quantum Threat Timeline Report 2020," *Global Risk Institute*, January 2021, page 30. (https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/)

was only theoretical. However, advances in science and technology are narrowing the gap between theory and reality. Small-scale quantum computers already exist.

NIST's "computational infeasibility" approach focuses on increasing the complexity of encryption algorithms so they become harder to break, but that is not the only way to achieve security. An alternative, less-explored strategy, AIA, uses the principle of information-theoretic security.[25]

AIA is achieved by fragmenting the data, encrypting each fragment, encrypting the keys, then distributing all encrypted fragments amongst various platforms inside and outside the organization. The user stores the encrypted fragments on multiple platforms like mobile devices, outsourced cloud storage, and internal servers, to name a few. The varied platforms add layers of complexity, requiring more significant resources and skill from the hacker to penetrate all platforms to retrieve all fragments. If just one fragment is not obtainable, the data remains secure.

Regardless of the computational power available for cracking the encryption, it is a statistical improbability that an adversary could gain access to multiple platforms owned and managed by various entities where the fragmented data is stored. If adversaries cannot access a predetermined amount of the puzzle pieces, they cannot decrypt the data. With AIA, the customer defines the quorum of puzzle pieces required before decryption can take place to reveal any part of the data. As long as the adversary is missing the required quorum of pieces, regardless of the available computation power, the data remains secure.

In 2021, TCIL conducted a pilot project on the benefits of decentralized file storage to mitigate the risk and effects of ransomware attacks by fragmenting, encrypting, and distributing data to multiple storage locations.[26] That project demonstrated that decentralized storage creates the resilience necessary for ransomware victims to continue operating as usual, as compared to defenses based only on access control, which offer no such benefit. Moreover, employing decentralization and encryption prevents the hacker from reading any stolen files. This latest TCIL pilot built on that approach by exploring a new distribution and fragmentation model utilizing an AIA strategy. The principal advantage of this new model is that it expands fragment storage beyond the owner's assets as an additional layer of defense.

Traditional data security relies on one or two obstacles to prevent unauthorized access. Cyber Reliant's security model uses AIA by fragmenting both the data and the key that decrypts it, distributing those fragments randomly across multiple platforms. To defeat such encryption, the adversary must compromise multiple platforms owned and operated by multiple entities, making it a statistical improbability. Figure 2 compares traditional data security and an AIA solution.

The top row represents the traditional storage process. The user sends their files to a central repository that bulk encrypts all data in storage. If encryption is compromised, all data becomes available and readable.

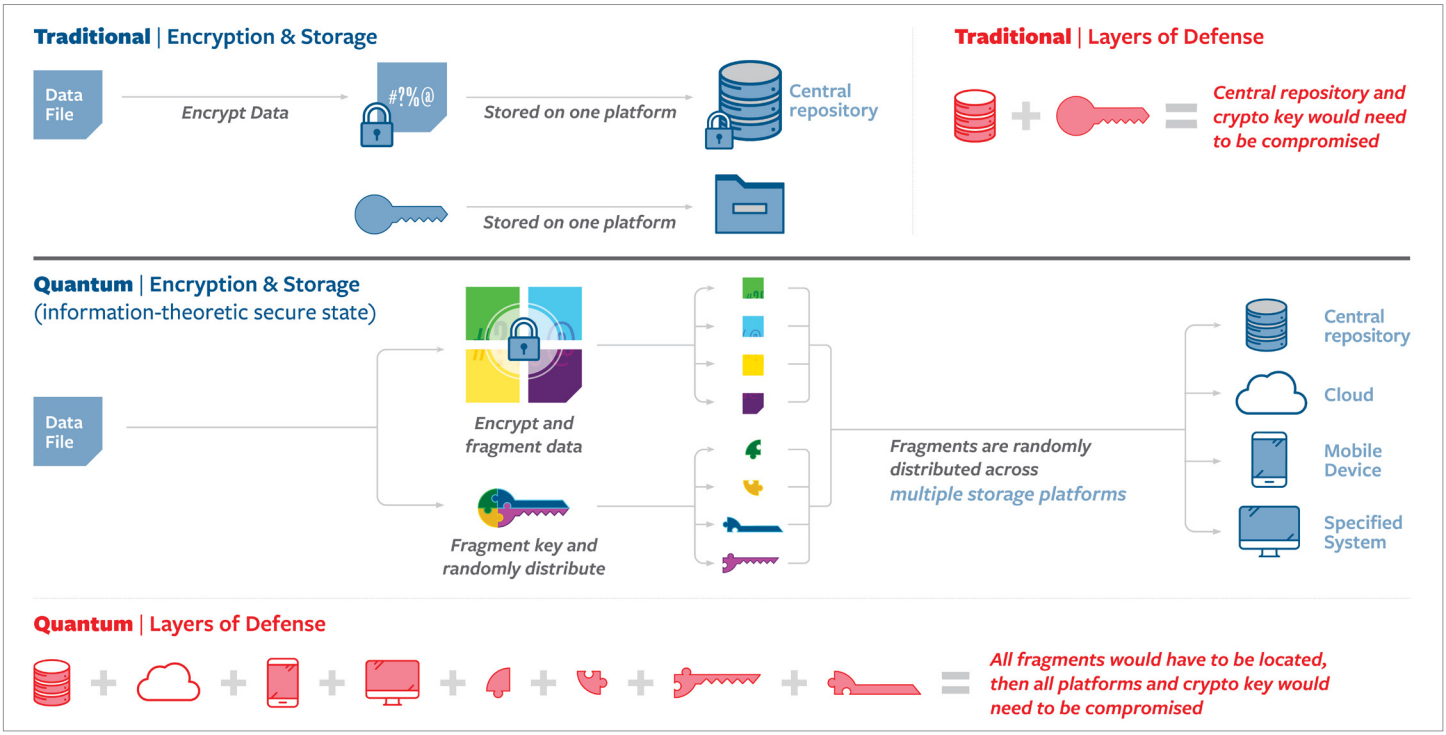
The bottom row represents an AIA system with a data-centric, as opposed to a device-centric, security strategy. When a user creates a file, it is immediately encrypted. The data and the key are then fragmented, distributed, and held across multiple storage platforms. There is no single location for an unauthorized user to access the required quorum of protected fragments. The adversary would have to compromise all storage platforms and encryption to access all data fragments.

25. True information-theoretic security is impractical even if feasible. For example, the sender and receiver of a message might use a one-time shared secret to encrypt and decrypt messages. This is known as "one-time pad." Each character of the message is encrypted, using a key as long as the message itself. However, given the size of the key, the one-time use, the large-scale entropy (randomness), and the requirement for infinite resources, this solution is largely impractical. AIA uses the principle of information-theoretic security in a more practical application.

26. Georgianna Shea, "Secure the Data, Not the Device," *The Foundation for Defense of Democracies*, November 8, 2021. (https://www.fdd.org/analysis/2021/11/08/secure-the-data-not-the-device/)

Protecting and Securing Data from the Quantum Threat

Figure 2: Comparison of traditional storage to AIA solution



The storage platforms used vary depending on the organization's infrastructure but could include cell phones, cloud environments, local storage devices, and remote storage containers. Each platform has its own security protocols, systems, and configurations protecting the data fragments. Therefore, compromising every platform is significantly more complex than gaining access to a central repository. Each platform would have its own protections to keep the data safe, requiring the attacker to use different vectors to penetrate each platform. In some cases, the attacker would have to be skilled in numerous operating systems, protocols, tools, and attack techniques. The more complex and varied the protections, the harder it is to find one group of hackers (even backed by nation states) capable of such a compromise.

Pilot Results

The pilot walked through the onboarding of Cyber Reliant's AIA data protection solution to better inform organizations what to expect when purchasing Cyber Reliant's product or other similar solutions from other companies.

For the purposes of the pilot, TCIL played the role of a company that had assessed its current security posture to be insufficient based on the threat landscape. The company determined its current data, encrypted using today's standards, to be at risk of theft by an adversary willing to store the data until it acquired quantum computing capabilities. Once CRQCs are available, the company feared all of its data would be at risk and thus decided to implement an AIA solution.

The supplier (Cyber Reliant) and the customer integrator (TCIL) first simulated a thorough analysis of the existing architecture to identify the best way to augment it with a vendor or service provider-agnostic, distributed, multiplatform storage capability. AIA solutions can be flexible and highly customizable because fragments can be stored on any device inside and outside the organization. Thus, the next step is developing a customized architecture solution based on the customer's needs. Cyber Reliant's AIA strategy to secure data is much more complex than traditional storage solutions.

As a result, each customer requires a custom implementation to upscale their existing architectures and security practices with a process that obfuscates storage location and data readability.

Depending on the requirements, implementation of the architecture takes between two weeks and several months. Tailored solutions using storage platforms and external infrastructure will require coordination with various owners and stakeholders and may take longer.

After the supplier and customer developed and agreed upon a plan of action, Cyber Reliant simulated the development and delivery of the tailored solution.[27] Then, TCIL (playing the role of the customer's administrator) simulated downloading the contents with licensing information and applying the organizational policy-based configuration settings, including settings related to how often and under what conditions users log into the architecture. Once the solution was "deployed" to the organization and tailored to its internal operations, TCIL (playing role of the administrator) simulated sending a link to the end-users (FDD employees) to access and download the application to begin using it.

While beyond the scope of the pilot, an important final step when implementing new technologies and services is to ensure that all inherited security controls are implemented and effective. For example, even with AIA solutions, organizations should use access controls like multifactor authentication to prevent simple social engineering attacks that would compromise access to the data.

Overall, TCIL assessed the onboarding process as straightforward and comparable to adding new software, hardware, or services to any existing architecture.

Recommendations

The onboarding of this type of security solution is not instantaneous or automatic. It requires investments of money, time, and personnel. That said, the product successfully mitigates threats of today and tomorrow. TCIL recommends adopting AIA strategies.

That said, the approach may not be appropriate for all enterprises. Before adopting post-quantum mitigations (or any security strategy), organizations should identify their most critical data, longevity requirements for encryption, and overall risk posture.[28] If an organization's five-year-old data is irrelevant, for example, applying an AIA strategy to protect historical data may be unnecessary. In addition, if the potential damage is low if the adversary were to steal encrypted data today and decrypt it once they have a CRQC, an AIA strategy might not be necessary. Waiting until post-quantum encryption is available may be appropriate, but it does not come without risk.

Beyond developing solutions to post-quantum threats, ensuring national security and prosperity for the long term requires investment in cryptological and security research, workforce development, secure by design standards, and other challenges by the U.S. government, academic and research institutions, and private industry. The following recommendations are the most important steps the U.S. government and private sector can begin doing today.

27. Cyber Reliant uses open standards to prevent vendor lock.

28. When reviewing data, entities should also consider the metadata and network data created when searching the internet, downloading content, or communicating through various venues.

The U.S. government should accelerate the adoption of post-quantum algorithms, promote more holistic security strategies, and hinder the ability of adversaries to develop CRQCs:

Reduce the gap of ineffective encryption. Federal Civilian Executive Branch agencies are prohibited from purchasing "any commercial quantum-resistant cryptographic solutions for use in IT systems supporting enterprise and mission operations" until the NIST standards are released.[29] NIST is conducting valuable work on computational infeasibility for the post-quantum reality by testing algorithms and developing new standards. NIST anticipates completing this phase within the next two years. The gap of ineffective encryption will occur, however, because after the standards are released, NIST projects another five to 15 years for widespread adoption of these standards. This estimate appears to be based on how long it took for today's encryption to become widely adopted. This is not necessarily an applicable model because convincing organizations of the necessity of encryption is likely much harder than convincing them to upgrade their encryption. The U.S. government should therefore reduce the timeline to enforce the adoption of NIST post-quantum cryptography standards by requiring federal agencies to implement the standard faster. The requirement on federal agencies will catalyze broader adoption by government contractors and critical infrastructure owners and operators that often apply U.S. government requirements voluntarily or in response to regulations.

Develop enterprise-wide security standards. Shortening the timeline for implementing post-quantum encryption standards does not address the problem of the adversary stealing data today to be decrypted later. Even with a reduced implementation timeline, critical information is still at risk. Likewise, the implementation of post-quantum encryption standards will not address other kinds of cyberattacks that cause business interruption through deleting data or locking up systems. Addressing these problems requires an upgraded approach to what it means to be "cyber secure."

Today, federal systems and many critical infrastructure operators use NIST's Risk Management Framework (RMF) to implement cybersecurity. The approach focuses on adopting and monitoring protections (controls). For example, the more stringent the data classification, the more controls an entity should add. However, the system's overall security is not usually tested, just the compliance of individual controls.[30] This needs to change. Organizations need to adopt enterprise-wide solutions (like AIA solutions) that secure critical information and provide resilience against cyberattacks. Having conditioned organizations to treat cybersecurity as a checklist with RMF, the U.S. government must now develop standards that organizations can use to determine if they are secure and resilient. That is the goal behind a separate initiative (to which TCIL contributes) led by two industry groups — the Global Resilience Federation and the Business Resilience Council — to develop an Operational Resilience Framework of steps and rules for practitioners.[31] U.S. standards on security and resilience should include requirements for testing and exercises that address the security of the whole rather than the compliance of a part.

Use economic sanctions to limit the ability of adversaries to advance in quantum capabilities. The U.S. government has many tools to thwart the ability of its adversaries to innovate and advance technological capabilities for nefarious purposes. Similar to the sanctioning of Chinese companies that support China's development of quantum computing technologies for military applications, the U.S. Treasury and Commerce departments should block technology exports

29. The White House, Briefing Room, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," May 4, 2022. (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/)

30. National Institute of Standards and Technology, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf); U.S. National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," September 2020. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf)

31. "Operational Resilience Framework," *Global Resilience Federation*, accessed November 29, 2022. (https://www.grf.org/orf)

to and impose financial sanctions on companies supporting quantum computing development by U.S. adversaries.[32] The goal of these programs — in addition to restricting the activities of the targets — is to dissuade others from contributing to efforts that advance adversarial quantum capabilities.

Industry should create market incentives to encourage adoption of stronger cybersecurity including, but not limited to, AIA solutions:

Create market incentives for the adoption of data protection strategies. Private companies have trade secrets, intellectual property, and national security-sensitive data. They should assess the cybersecurity of their systems holistically and implement file-level protections. Companies should view cybersecurity as smart business. Unfortunately, that is not always the case today. So, market forces should incentivize good cybersecurity practices. For example, industries that provide loans, insurance, or other risk transfer-based services can provide more favorable terms to organizations that take proactive steps to secure data by implementing enterprise-wide security strategies like AIA. For the service provider, this makes sense. Data security solutions that can withstand the effects of ransomware and can mitigate quantum computing threats reduce the overall risk of data compromise — and thus the risk to the investment itself or the risk that an insurance customer will file a claim. For example, Lloyds of London, one of the first companies to provide cyber insurance,[33] offers higher coverage to customers who have implemented a secure data solution by applying an AIA secure state. In effect, Lloyds has embraced the idea that cyber insurance can no longer follow the risk transfer model absolving customers from security responsibility. Instead, cyber insurance must follow a risk reduction model, assisting clients in minimizing the chance of business interruption caused by a cyber breach. Banks, insurance providers, financial service providers, and others should deploy similar programs to incentivize the adoption of technologies that reduce the probability of an incident.

Conclusion

The Biden administration issued a directive this year to mitigate the threat of U.S. adversaries developing quantum computing capabilities by requiring a transition to quantum-resistant encryption. Unless the U.S. government acts now, developing relevant standards and implementing this encryption will require at least a decade. America does not have that kind of time; quantum computing may be in use in only three years. Therefore, the government must shorten the timeline for post-quantum cryptography implementation. The private sector should also prepare for an impending gap of insufficient cryptography by exploring and assessing data security strategies that offset the increased computer power of CRQCs. Technology is advancing, and if the data that is secure today must remain secure tomorrow, organizations need to plan with tomorrow's threats in mind.

32. Georgianna Shea and Cara Cancelmo, "Washington Seeks to Counter China's Quantum Computing Drive," *The Foundation for Defense of Democracies*, December 6, 2021. (https://www.fdd.org/analysis/2021/12/06/chinas-quantum-computing-drive/)

33. Mingyan Liu, *Embracing Risk: Cyber Insurance as an Incentive Mechanism for Cybersecurity,* (Michigan: Morgan & Claypool Publishers, 2021). (https://www.morganclaypool.com/doi/abs/10.2200/S01093ED1V01Y202104LNA026)

Appendix A: Encryption Functions of the NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) is a flexible tool that addresses and manages cybersecurity risk through a repeatable and performance-based approach.[34] E.O. 13636 of 2013 promoted the CSF's adoption of critical infrastructure.[35] E.O. 13800 of 2017 required all agency heads to use the framework.[36]

The CSF consists of five functions: Identify, Protect, Detect, Respond, and Recover. Encryption falls under protection. Securing data using quantum secure data protection aligns with the protect functions; the data security category and subcategories "data-at-rest is protected," "data-in-transit is protected," and "protections against data leaks are implemented."

Function	Category	Subcategory	Enabling Technology
PROTECT (P.R.)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**P.R.DS-1:** Data-at-rest is protected	**Augmented improbability of access**
		P.R.DS-2: Data-in-transit is protected	**Augmented improbability of access**
		P.R.DS-3: Assets are formally managed throughout removal, transfers, and disposition	
		P.R.DS-4: Adequate capacity to ensure availability is maintained	
		P.R.DS-5: Protections against data leaks are implemented	**Augmented improbability of access**
		P.R.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	
		P.R.DS-7: The development and testing environment(s) are separate from the production environment	
		P.R.DS-8: Integrity checking mechanisms are used to verify hardware integrity	

34. U.S. Department of Commerce, National Institute of Standards and Technology, "Cybersecurity Framework," accessed August 20, 2021. (https://www.nist.gov/cyberframework)

35. Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013. (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity)

36. Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017. (https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure); The White House, National Security Council, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," June 1, 2018. (https://trumpwhitehouse.archives.gov/articles/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure)

Acknowledgments

FDD's TCIL is a nonprofit organization that relies on volunteers passionate about advancing cybersecurity practices.

Thank you, Stephen Campbell, Adam Firestone, Andrew Hildick-Smith, Andrew Jones, Clayton Jones, Mark Prys, Brad Rhodes, and Charles Robinson for reviewing the paper and providing feedback.

Cyber Reliant Partner

Daniel Kay
Vice President, National Security & Justice

Thank you, Danno, for taking the time to explain and re-explain the complex topic of quantum computing and its threat to modern-day encryption. It was a pleasure working with and learning from you!

Protecting and Securing Data from the Quantum Threat

About the Authors

Dr. Georgianna "George" Shea serves as chief technologist for FDD's Center on Cyber and Technology Innovation and TCIL. In that role, she identifies cyber vulnerabilities in the U.S. government and private sector, devising pilot projects to demonstrate feasible technology and non-tech solutions that, if scaled, could move the needle in defending U.S. prosperity, security, and innovation.

Annie Fixler is the director of FDD's Center on Cyber and Technology Innovation, contributing to the cyber-enabled economic warfare project and the Transformative Cyber Innovation Lab, and a research fellow at FDD. She works on issues related to the national security implications of cyberattacks on economic targets, adversarial strategies and capabilities, and U.S. cyber resilience. She also contributes to the work of FDD's Center on Economic and Financial Power on offensive and defensive tools of economic coercion.

About the Foundation for Defense of Democracies

FDD is a Washington, DC-based, nonpartisan 501(c)(3) research institute focusing on national security and foreign policy.

About FDD's Transformative Cyber Innovation Lab

TCIL finds and nurtures technologically feasible, testable pilot projects which begin to solve some of the hardest cyber problems afflicting the national security industrial base and the United States. TCIL's mission is to help shorten the lag between idea and piloting and between piloting and the adoption of potential solutions to the thorniest of cyber problems. TCIL seeks to drive revolutionary, society-wide improvement in cyber resilience through the innovative synthesis of technology, policy, and governance.

For more information, visit: https://www.fdd.org/projects/transformative-cyber-innovation-lab