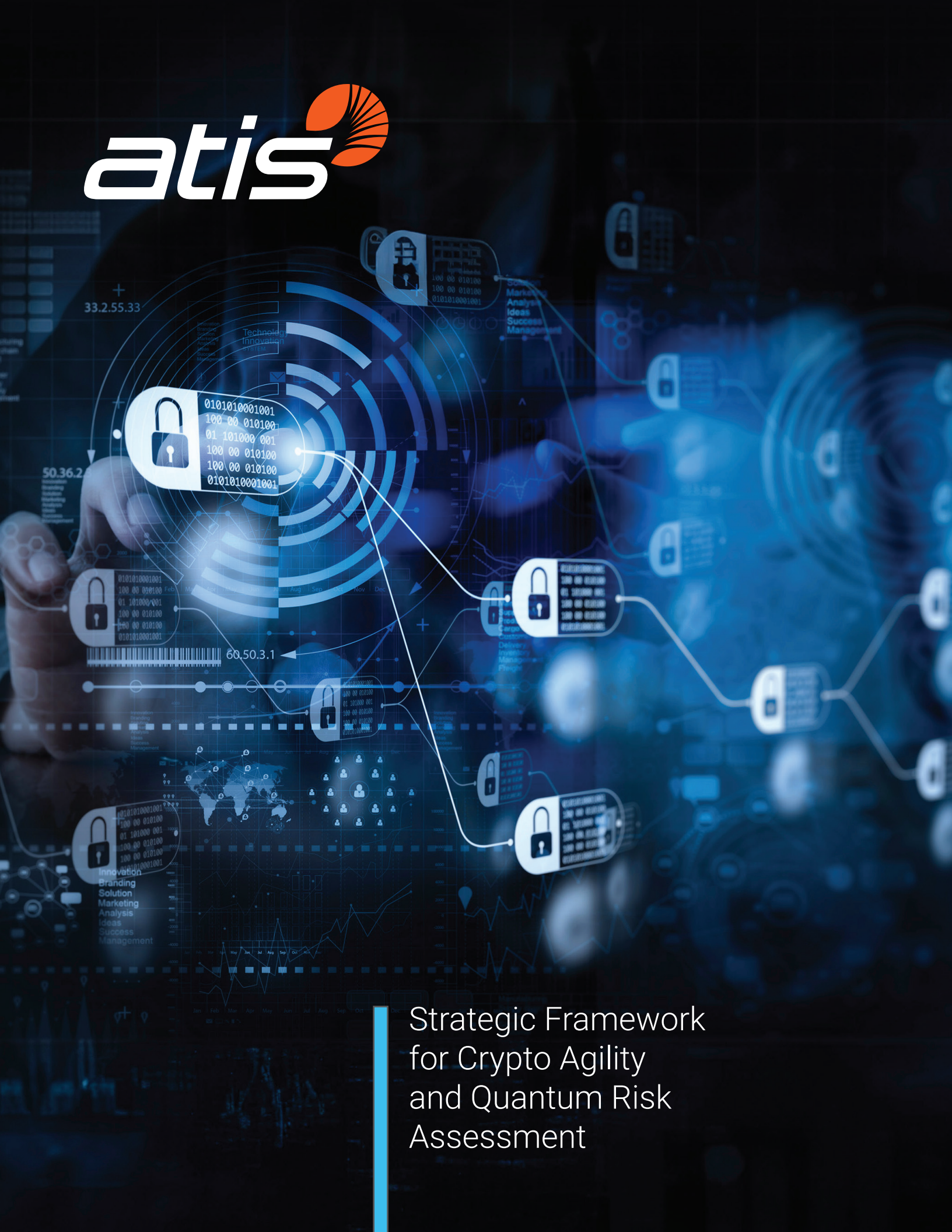


Strategic Framework for Crypto Agility and Quantum Risk Assessment

TABLE OF CONTENTS

EXECUTIVE OVERVIEW

In an era dominated by digital transactions, cryptographic algorithms underpin the security of our online interactions, safeguarding data confidentiality, integrity, and authentication. These robust mathematical constructs have diligently shielded our digital realm, impervious even to the mightiest supercomputers available today.

However, the advent of quantum computers at scale threatens to disrupt this paradigm. These exceptionally powerful machines possess the potential to unravel much of our current encryption, potentially exposing private communications, sensitive company data, and even government and military secrets. A quantum computer that will be able to run these attacks is referred to as a cryptographically relevant quantum computer (CRQC).

The widely used Rivest-Shamir-Adleman (RSA) asymmetric encryption algorithm, which relies on factoring large primes, is particularly vulnerable. While classical computers would require centuries to crack a 2048-bit RSA key, a quantum computer could potentially do so in a mere day. Crucial technologies like public-key infrastructure (PKI) and blockchain are also at risk. Even symmetric key encryption may also be weakened.

To address this threat, the National Institute of Standards and Technology (NIST) is spearheading the development of quantum-resistant public-key cryptography. These quantum-resistant cryptographic algorithms, known as post-quantum cryptography (PQC), are crucial for protecting against quantum and traditional computers. However, the lack of maturity in these PQC candidates, along with the length of time it takes to migrate to a different algorithm, highlight the need for organizations to swiftly adapt to new cryptographic standards. We call this concept **cryptographic agility or crypto agility**. Preparing for quantum threats demands comprehensive assessments of existing cryptographic implementations and the development of a strategy to mitigate risks. Options include transitioning to quantum-secure cryptographic algorithms or phasing out vulnerable systems. Organizations must embrace a nimble approach to implementing new cryptographic security, known as crypto agility, enabling the swift replacement of potentially compromised algorithms with robust, quantum-secure alternatives.

The ATIS Quantum Safe Communications and Information Initiative (QSCII) convenes industry experts to develop a roadmap aligned with industry best practices to address regulatory, governance, and interoperability implications.

This paper provides a comprehensive approach to crypto agility and risk assessment across communication and information systems, fortifying them against quantum threats in the future. It furnishes illustrative examples to help organizations evaluate their risk exposure.

However, transitioning to quantum-resistant cryptography is not merely an option but an imperative for preparedness. Robust metrics are essential to assess internal processes, offering a true measure of crypto agility.

In preparation for the quantum era, organizations must commence quantum-focused risk assessments, as quantum-capable threat actors are expected to emerge before fully functional quantum computers. The threat of "store now, decrypt later" attacks necessitates immediate action to safeguard sensitive data.

Implementing crypto agility extends beyond product implementation, encompassing comprehensive organizational strategies. It entails cultivating executive awareness, appointing effective leadership, judicious allocation of resources, and organization-wide training initiatives.

The transition to quantum-resistant cryptography is not merely a technological shift, but a strategic imperative that demands coordinated efforts across industries and organizations worldwide. This proactive approach will ensure the continued security and integrity of digital transactions in the quantum age.

Recommendations and Call to Action

In light of the imminent quantum threat, it is imperative for organizations to fortify their systems against potential breaches. The store now, decrypt later scenario poses a tangible risk, emphasizing the urgency of action. Implementing crypto agility should be prioritized not only in product implementation but also through well-defined organizational strategies. This entails a structured approach, including creating executive awareness, designating responsible leaders, allocating resources judiciously, and providing comprehensive training. Furthermore, adopting a standardized risk assessment framework for crypto agility, coupled with a set of well-defined metrics, will be instrumental in ensuring quantum resilience. These metrics inform the organization and provide crucial insights to vendors and any third parties involved. They serve as informed measures of how crypto agile the organization is, offering a clear picture of its preparedness against emerging quantum threats. This proactive stance will protect sensitive data and safeguard the integrity of critical systems in the face of the quantum revolution.

INTRODUCTION

Almost everything we do online is made possible due to cryptographic algorithms. These complex mathematical structures are embedded in hardware and software systems throughout enterprise infrastructure, supporting and securing the storage and flow of data. These are the systems that encrypt data to protect our privacy, establish our identity, and secure our payments. Day in and day out, these cryptographic algorithms have worked relentlessly to secure the data transactions the world currently runs on. Even with the fastest supercomputers available today, breaking these cryptographic algorithms would be an impossible task.

Enter the quantum computers of the future. These advanced computing machines will possess the capability to break many of today's encryption methods, potentially exposing private communications, corporate data, government and military secrets.

One of today's commonly used asymmetric public key encryption algorithms, RSA, relies on factoring the product of two very large primes. Classical computers may require hundreds of years to crack a 2048-bit RSA key, but a future quantum computer may be able to do so in a day [1, 2]. Asymmetric encryption is not the only algorithm at risk. Future quantum computers may also have the potential to weaken symmetric key encryption [3].

To address these challenges, NIST has been investigating new quantum-resistant public-key cryptography, known under the umbrella term PQC, that can be adopted by organizations to secure against both quantum and traditional computers. After a multiyear process of soliciting, evaluating, and standardizing, NIST recently announced several PQC candidates have been selected. However, the lack of maturity in these PQC candidates, along with the length of time it takes to migrate to a different algorithm, demonstrates that systems and devices need to be able to adapt quickly to new cryptographic algorithms to remain secure.

To ensure that current systems are secure from the potential threat of quantum commuters in the future, organizations will need to assess all implementations of existing cryptography and establish a roadmap to determine the most appropriate approach to addressing the risks. Strategies such as transitioning to these new quantum secure cryptographic algorithms or completely phasing out impacted system are just two of the possible mitigation strategies addressed in this paper.

The ATIS QSCII brings together industry experts on this topic and is developing a roadmap of work items to advance operators' and users' needs in this area, aligned with industry best practices and other quantum standards initiatives.

Ensuring key regulatory, governance, and interoperability implications to enable quantum-safe security are also being addressed.

Implementing crypto agility is a strategic imperative that demands a systematic approach, including the use of well-defined key performance indicators (KPIs) and metrics to measure progress and effectiveness. This paper provides a comprehensive framework for crypto agility and quantum risk assessment, complete with illustrative examples and scorecards based on KPIs and metrics. It aims to help organizations evaluate their risk exposure and take appropriate actions to strengthen their security posture against the emerging quantum threats.

Impacts to Current Cryptography

Cryptography involves the use of mathematical functions called ciphers or cryptographic algorithms, which are combined with keys such as phrases, digits, or words to encrypt text. The strength of the cryptographic algorithm and the secrecy level of the key determine the effectiveness of the encryption. Cryptography is essential for ensuring secure network communications and e-commerce transactions, and provides four foundational security services:

1. ***Confidentiality***, which ensures that only authorized parties can view the content of a message.

2. ***Integrity***, which ensures that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.

3. ***Non-repudiation***, which ensures that the originator of an action cannot deny performing the operation later on.

4. ***Authentication***, which verifies the identity of a person or system.

To implement these critical functions, three types of algorithmic techniques are used: hash functions, symmetric-key algorithms, and asymmetric key/public-key algorithms.

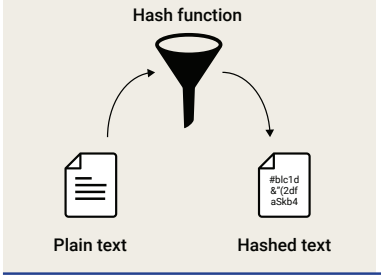
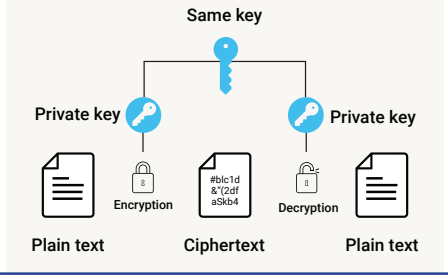
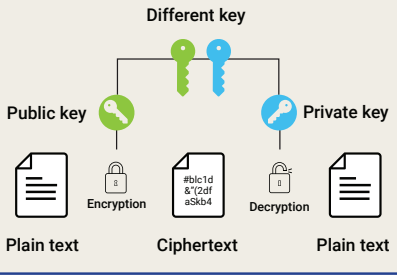
	Hashing	Symmetric cryptography	Public-Key cryptography
			
Cryptographic Application	Storing and verifying passwords and checking data integrity	Bulk encryption of large amounts of data	Basis of internet communication and e-commerce encryption protocols such as SSL, TLS, and HTTPS breaks all currently used public-key algorithms
Quantum Impact	Reduces security; more secure hash functions exist and can be used	Reduces security; the minimal key size should be doubled for most algorithms (e.g., AES)	Breaks all currently used public-key algorithms

Figure 1: Cryptographic operations and their function [4]

Asymmetric Key cryptography and Identity information: Asymmetric key cryptography is widely used for identity information, such as PKI and login credentials. If a quantum computer were able to decrypt this, it could lead to identity theft and other types of fraud.

PKI: PKI infrastructure is used for authentication and encryption of identity proofs or credentials such as digital certificates in a variety of applications, including web browsers, VPNs, and other secure communications. If a quantum computer were able to break the encryption used in PKI, it could lead to unauthorized access to sensitive information.

Blockchains are used for secure and transparent record-keeping in many industries, including finance, healthcare, and logistics. If a quantum computer were able to break the encryption used to protect blockchains, it could lead to a compromise of data integrity and potentially significant financial losses.

Symmetric key cryptography is used in a wide range of applications, including encryption of data at rest and in transit. If a quantum computer were able to break the encryption used in symmetric key cryptography, it could lead to unauthorized access to sensitive information.

Internet of Things (IoT) devices often communicate sensitive information over the internet and may be protected by encryption. If a quantum computer were able to decrypt this, it could lead to unauthorized access to the devices or to the data they transmit.

Assets using Transport Layer Security (TLS), which is a widely used encryption protocol for securing communications over the internet. If a quantum computer were able to break the encryption used in TLS, it could lead to unauthorized access to sensitive information transmitted over the internet.

Threat Timeline

The Global Risk Institute's Quantum Threat Timeline report 2022 surveyed 40 thought leaders in key relevant areas of quantum science and technology [5]. This report sheds light on the quantum threat timeline by analyzing the opinions of international leaders from academia and industry working on several aspects of quantum computing. They answered questions designed to elicit useful insights for managing cyber-risk associated with quantum cryptanalysis. These experts were asked to provide estimates about the development timeline for quantum computers, specifically for quantum computers powerful enough to pose a threat to cybersecurity.

Figure 2 illustrates the summary of their opinions about the likelihood of a significant quantum threat to public-key cybersecurity as a function of time. More than half of the respondents indicated the threat would be likely or more likely within the next 15 to 20 years. This time frame appears as a tipping point, as the number of respondents estimating a likelihood of "about 50%" or larger becomes the majority.

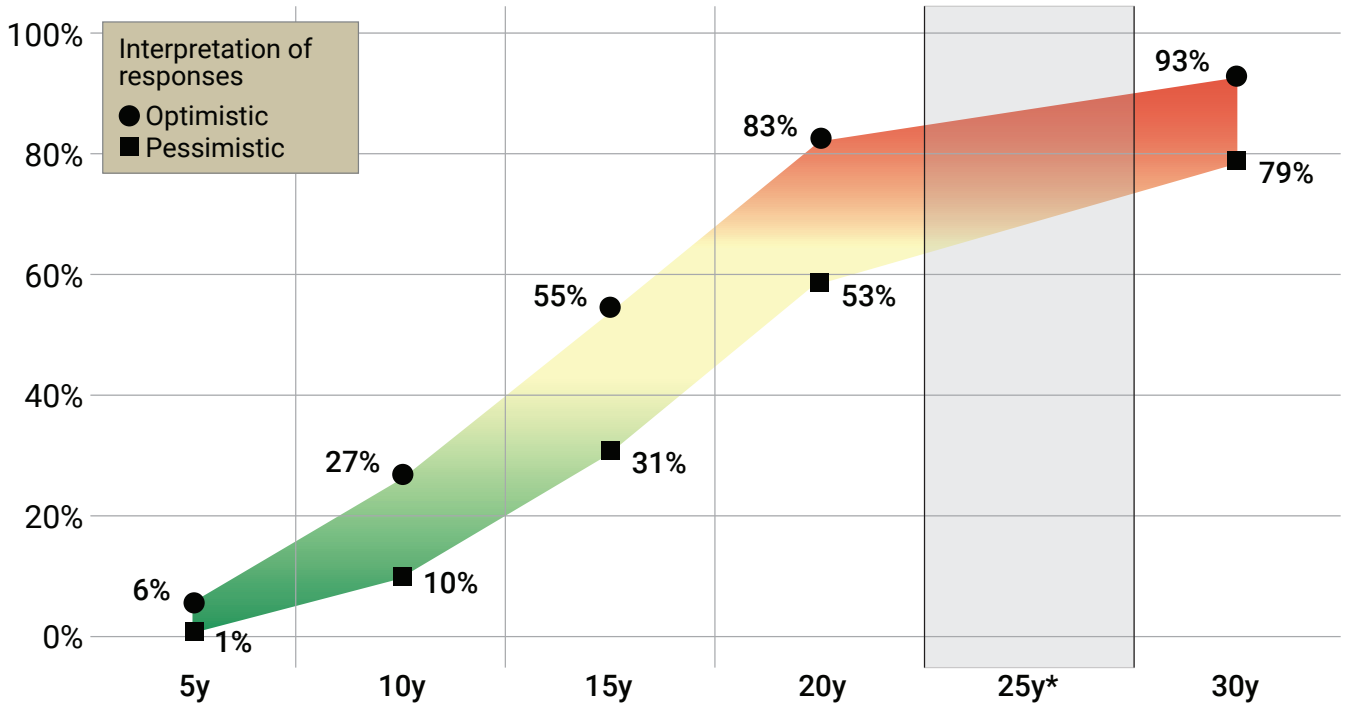


Figure 2: Expert opinions on the likelihood of quantum computer breaking RSA 2048 in 24 hours [5]

Despite the current lack of maturity of functional quantum computers and unknown timeline, attacks known as "store now, decrypt later" are still very relevant to businesses today. This attack occurs when an adversary hacks into a company network and steals sensitive, high-value, long-shelf-life data (e.g., Social Security numbers, medical records, government information, etc.). When a CRQC becomes available in the future, the adversary can compromise the encryption algorithms protecting the stored data to read the information.

Taking into consideration everything discussed above and regardless of the timeline for when a CRQC becomes viable for adversarial purposes, it is imperative that organizations understand that quantum-capable threat actors (QCTA) will pose a very real threat and to start on the journey of performing quantum focused risk assessments of their systems now.

What is Crypto Agility?

Crypto agility refers to the ability of a system or organization to adapt and switch to different cryptographic primitives, algorithms, or protocols easily and efficiently with limited impact on operations and with low overhead. Crypto agility can be a solution for a product or service to maintain flexibility of encryption used to accommodate a cryptographic breakthrough or updated standards. Crypto agility can also be a measurement of the time, effort, and cost it takes for an organization or product to switch cryptographic primitives. The concept of crypto agility is crucial in the context of cybersecurity and data protection because cryptographic algorithms can become weak or compromised over time due to advancements in technology or the discovery of vulnerabilities.

It is important for infrastructure and security systems to be crypto agile to accommodate PQC in the future because quantum computing is still under development and any security measures against it are still being tested. These cryptography algorithms are constantly being broken or revised, so the update to the cryptographic infrastructure and system will be an iterative process.

Incorporating crypto agility by design into a system allows it to stay resilient against emerging threats and to comply with evolving security standards and regulations. By supporting multiple cryptographic algorithms, a system can switch to stronger algorithms or replace compromised ones without disrupting its operations or requiring major changes in the overall infrastructure.

A crypto agile design would allow for replacement of algorithms with minimal impact to implementation and performance such as adoption rate and backward compatibility. One of the ways to combine all the factors into a broader crypto agility strategy is to use a Crypto Agility Risk Assessment Framework (CARAF) such as the one proposed in the *CARAF: Crypto Agility Risk Assessment Framework* [6].

Why Should We Implement Now?

Commercial National Security Algorithm Suite (CNSA) 2.0 has a timeline that shows the migration to quantum resistance complete by 2033 [7]. The National Cybersecurity Strategy Implementation Plan states it will prioritize the transition of vulnerable public networks and systems to PQC with a complete date of the third quarter of 2025 [8]. NIST's proposed PQC algorithms, at the time this is written, are yet to be standardized. With projections for the first three PQC algorithms to be standardized in 2024, the CNSA 2.0 timeline also shows that PQC may start being tested or requested in 2024. Simultaneously, swapping out obsolete algorithms with new quantum-resistance ones is not as simple as previous migrations. PQC algorithms are drastically different, with much larger key sizes.

Designing products to be crypto agile will enable them to swap to quantum-resistant algorithms easily. Designing processes in place to enable crypto agility across all product lines will ensure the organization is quantum resistant.

Crypto agility is more than just a solution. It's also a marker for preparedness. Having solid metrics can help access your internal process to determine a TRUE level of crypto agility.

Typically, transition times for encryption algorithms have taken years to decades. In 2005, NIST withdrew (FIPS) 46–3, 74, and 81–all Data Encryption Standard (DES) standards and guidance [9]. NIST then released a DES transition plan, to move from DES to AES, which was approved for federal government use in 2001. NIST's transition plan was two years, but it would take over 20 years to migrate from DES or 3DES to AES [10]. These transitions, compared to the transition to post-quantum cryptography, were far less complex. Without enabling our systems and organizations to become more cryptographically agile, we can expect transition times to be even longer. The threat of CRQCs is likely to arrive before all systems have been fully migrated.

IMPLEMENTING CRYPTO AGILITY

Crypto agility goes beyond product implementation and also relies on organizational strategies. From a business perspective, implementing crypto agility requires a structured approach that encompasses executive awareness, leadership assignment, judicious allocation of resources, and providing training across the organization.

Executive Awareness and Commitment

The cornerstone of a successful crypto agility implementation lies in the commitment and understanding of the organization's leadership. Executives need to be acutely aware of the pivotal role that crypto agility plays in fortifying the organization's security posture against emerging threats. This awareness translates into a commitment to allocate the necessary resources and support for the initiative.

Establishing Leadership and Ownership

Central to this process is the appointment of a dedicated leader responsible for driving the crypto agility initiative. This individual, ideally possessing expertise in cryptography, assumes a pivotal role in formulating a comprehensive plan, delineating a strategic roadmap, and overseeing the seamless execution of the initiative. Their responsibilities encompass communication of the implementation plan, collaboration with cross-functional teams, supervision of testing and integration efforts, and periodic reporting of progress to the executive team. Leaders must define the scope of each implementation area to properly take inventory and prioritize. Scope can be defined by IT systems, product lines, by customer, high impact areas, business area (software vs. hardware), or geographic area. This will be needed to properly allocate budget and resources.

Allocating Budget and Resources

An essential aspect of implementing crypto agility is the allocation of budgets and resources tailored to the unique needs of the organization. This necessitates the establishment of distinct budgets: One is dedicated to the organizational transition toward crypto agility, covering expenses related to training, recruitment, and the implementation of new cryptographic solutions. Another is reserved for the establishment of specialized labs and rigorous integration testing, ensuring the seamless incorporation of cryptographic innovations into the existing infrastructure.

BUDGET VS. RESOURCES:
STRIKING THE RIGHT BALANCE

In the pursuit of establishing crypto agility, the allocation of budget plays a pivotal role in determining the initiative's scope, depth, and ultimately, its effectiveness. This financial commitment must be strategically balanced with the allocation of internal resources. Balancing budgetary allocation with resource availability is essential for a seamless crypto agility implementation. While a substantial budget facilitates comprehensive initiatives, the availability of skilled resources ensures the execution is carried out efficiently.

Allocating Budget

A significant portion of the budget should be earmarked for the development and nurturing of internal teams. This encompasses training programs, workshops, and potentially hiring experts in cryptography. Additionally, dedicating funds toward the establishment of specialized labs is paramount. These labs serve as the testing grounds for new cryptographic implementations, ensuring they integrate seamlessly within the existing infrastructure. Furthermore, a portion of the budget should be allocated toward product development. This involves creating robust frameworks that incorporate crypto agility as a core component, enabling products to adapt swiftly to evolving cryptographic landscapes.

At the executive level, it's prudent to explore the possibility of leveraging government incentives. Governments, recognizing the criticality of quantum resistance, may offer financial support for organizations investing in crypto agility. This could manifest as federal grants, tax incentives, or subsidies aimed at fortifying national critical infrastructure. Additionally, in cases where a rip-and-replace strategy is imperative, seeking government funds becomes crucial. This executive-level advocacy for government incentives amplifies the financial capacity for crypto agility and aligns organizational efforts with broader national security interests.

Low on Budget, High on Resources: Maximizing Efficiency

In scenarios where budget constraints are a reality, organizations can leverage their existing resources effectively. Conducting a comprehensive inventory of available resources, both in terms of personnel and technology, becomes paramount. This approach, while working with limited financial resources, ensures that the available manpower and infrastructure are utilized optimally. It allows organizations to strategically channel their efforts towards areas of highest impact.

Approach to Budget Allocation

In the journey toward implementing crypto agility, budget allocation is imperative. It must be aligned with the available resources, ensuring that the initiative is both financially sustainable and operationally efficient. By earmarking funds for internal teams, labs, and product development, organizations fortify their ability to adapt to emerging cryptographic landscapes. Moreover, exploring government incentives at the executive level amplifies the financial capacity, bolstering the national security posture. In cases of budget constraints, a judicious inventory of available resources ensures that efforts are channeled towards areas of highest impact. This comprehensive approach ensures that budget allocation is not merely an administrative process but also a strategic driver of crypto agility implementation.

Demonstrating ROSI and Business Value

To substantiate the investment in crypto agility, it is imperative to establish metrics for measuring its Return on Security Investment (ROSI). These metrics may include a reduction in security incidents, faster response times to emerging threats, and an improved alignment with evolving compliance standards. Furthermore, it is paramount to align the goals of the crypto agility initiative with broader business objectives. A resilient cryptographic infrastructure not only enhances security but also bolsters customer trust, competitive advantage, and ultimately organizational success.

In conclusion, adopting crypto agility is not solely a technical endeavor; it is a strategic imperative that demands executive commitment, astute leadership, and judicious resource allocation. By approaching crypto agility from a business perspective, organizations fortify their security posture, enhance operational resilience, and align their security initiatives with overarching business objectives. This comprehensive approach ensures the sustainable and effective implementation of crypto agility within the organizational framework.

COMMUNICATING THE INITIATIVE:
EDUCATING AND ENGAGING STAKEHOLDERS

Effectively communicating the crypto agility initiative is fundamental to its success. This involves educating key stakeholders, including leadership, risk management teams, and product development units, on the quantum threat and the proposed solutions. Additionally, leveraging the expertise of quantum professionals serves a dual purpose: analyzing risk and providing comprehensive education about the threat landscape and potential solutions.

Initiating the communication process involves elevating the awareness of leadership and decision-makers regarding the quantum threat. This encompasses providing a comprehensive overview of the potential impact of quantum computing on current cryptographic systems. Through detailed presentations, workshops, and informative materials, leadership gains a clear understanding of the urgency and necessity of the crypto agility initiative. It is crucial to frame the crypto agility initiative within a strategic context. Clearly outlining how crypto agility aligns with broader organizational objectives, including long-term security, compliance, and competitive advantage, ensures that leadership recognizes it as a critical component of the organization's overall cybersecurity strategy.

Engaging with risk management teams and bringing in quantum experts are essential for risk analysis and providing specialized education. These experts possess a deep understanding of the quantum threat landscape and can assess the potential risks associated with current cryptographic infrastructure. Moreover, they play a pivotal role in educating existing risk management teams about the intricacies of quantum threats and potential solutions.

Conducting risk workshops and risk simulations, facilitated by both quantum experts and internal risk management experts, provides a hands-on approach to understanding the quantum threat. These sessions allow risk management teams to engage with real-world scenarios, fostering a deeper comprehension of the risks posed by quantum computing.

Translating Threat Awareness into Product Resilience

For product development units, it is crucial to translate threat awareness into actionable plans for product resilience. This involves outlining a well-formulated product security and privacy set of requirements, elaborating on them through workshops focused on integrating crypto agility principles into product development lifecycles. By providing concrete examples and best practices, product teams can grasp how to embed crypto agility into their solutions.

Encouraging cross-functional collaboration between product development units and quantum experts fosters a dynamic environment for innovation. By working in tandem with quantum experts, product teams gain valuable insights into adapting products to be quantum resistant, thus ensuring they remain resilient in the face of emerging threats.

Fostering a Culture of Quantum Resilience

Effective communication of the crypto agility initiative is not only about disseminating information but also about fostering a culture of quantum resilience within the organization. By educating leadership, risk management teams, and product development units, organizations empower their teams to proactively navigate the quantum threat landscape. Leveraging the expertise of quantum professionals amplifies this effort, providing specialized knowledge and risk analysis. Through these collaborative efforts, organizations establish a foundation of knowledge and expertise that forms the bedrock of their crypto agility initiative.

Developing KPIs/Metrics for Crypto Agility and Quantum Resistance

In the dynamic landscape of cybersecurity, the establishment of clear KPIs and metrics is paramount. These serve as the compass guiding organizations towards robust crypto agility and quantum resistance. To ensure a shared understanding and language surrounding these critical concepts, it is imperative to establish comprehensive guidelines. These guidelines unify terminology and facilitate a structured approach toward measuring the efficacy of crypto agility strategies and quantum-resistance initiatives. By formulating well-defined crypto agility metrics and KPIs, organizations forge a path toward heightened security in the face of evolving cryptographic threats. These metrics not only quantify the progress made in implementing quantum-resistant strategies but also provide valuable insights into the overall cyber resilience of the organization. They serve as the cornerstone for informed decision-making, enabling organizations to adapt swiftly to the quantum era.

Importance of Consistent Crypto Agility KPI Tracking

The tracking of crypto agility KPIs consistently across the organization, products, and interactions with other stakeholders enables organizations to swiftly respond to new threats, including those posed by quantum computing. Consistent tracking ensures that the organization remains prepared for evolving security challenges. By measuring and reporting crypto agility KPIs, an organization can clearly articulate its preparedness to be quantum secure for the future:

1. **Providing Solutions for Quantum Resistance:** With quantum computing on the horizon, maintaining crypto agility is imperative. Regularly monitoring crypto agility KPIs enables timely adjustments to security measures as quantum technology advances.
2. **Navigating Constant Cryptographic Evolution:** Cryptographic algorithms are in a perpetual state of flux due to ongoing research, breakthroughs, and vulnerabilities. Regularly tracked KPIs serve as early indicators of when updates or changes are necessary.
3. **Ensuring Compliance with Evolving Standards:** Compliance with security standards and regulations is a fundamental aspect of maintaining trust and legality. Consistent KPI tracking aids in demonstrating adherence to evolving cryptographic standards.
4. **Minimizing Operational Disruptions:** A well-tracked crypto agility plan allows for seamless transitions between cryptographic algorithms, reducing disruptions to operations. This is particularly crucial in critical systems.
5. **Facilitating Interactions with Stakeholders:** Transparent and reliable crypto agility practices enhance the organization's credibility and trustworthiness in interactions with clients, partners, and regulatory bodies.
6. **Enabling Swift Responses to Cryptographic Breakthroughs:** In the event of a cryptographic breakthrough, an organization's crypto agility can determine how swiftly and effectively it can adapt to mitigate the impact.
7. **Supporting Product Resilience:** Crypto agility is equally vital for products. Consistent KPI tracking ensures that products can promptly adopt stronger encryption methods or replace compromised ones.
8. **Implementing a Quantum Risk Assessment:** Conducting Quantum Risk Assessment (QRA) or adding QRA practices into organizational risk assessments provides a structured approach to evaluating and enhancing crypto agility. The CARAF Assessment is an example of a QRA. Regularly tracking QRA metrics aids in maintaining a robust crypto agility strategy.
9. **Demonstrating Commitment to Security:** Consistent tracking of crypto agility KPIs showcases an organization's dedication to staying at the forefront of security best practices and technologies.
10. **Fostering a Culture of Security:** By emphasizing the importance of crypto agility and consistently tracking relevant KPIs, organizations instill a culture of security awareness among employees and stakeholders.
11. **Showcasing Organizational Maturity:** Mature organizations understand the significance of crypto agility and demonstrate it through regular KPI tracking. This showcases a proactive and forward-thinking approach to cybersecurity.

By consistently tracking crypto agility KPIs, organizations prepare themselves for the quantum era and demonstrate a commitment to robust cybersecurity practices. This proactive approach helps build trust with stakeholders, enhances operational resilience, and ensures compliance with evolving security standards. It is a cornerstone in the defense against emerging cryptographic threats. To meet or measure these KPIs, associated metrics must be used. We suggest breaking down the metrics into Organization and Operational Strategy metrics, and Product/Services Metrics.

ORGANIZATIONAL & OPERATIONAL
STRATEGY METRICS

In this section, we delve into the metrics that can be used to meet and measure the crypto agility KPIs that relate to the Organizational and Operational Strategy holistically. These metrics serve as navigational guides for organizational leadership, offering a view of the organization's adaptability and readiness. By vigilantly monitoring these metrics, ensure that the crypto agility strategies align with the goals to equip the organization for the future cryptographic challenges with confidence. This proactive approach not only bolsters our cybersecurity posture but also bolsters our organizational resilience.

Examples of crypto agility metrics categorized under Organizational & Operational Strategy include:

1. **Cycle Time for Algorithm Implementation**:
    - **Definition:** Time taken to implement a new cryptography algorithm.
    - **Importance:** Shorter cycle times mean quicker response to threats and better crypto agility.
    - **KPI:** Providing solutions for quantum resistance; showcasing organizational maturity and agility to implement new cryptography algorithms.
    - **Calculation:** Total time taken to implement a new algorithm/number of algorithm implementations (hours). Can be represented as a score 1-10, where 1 is a very long time and 10 is short.
2. **Stakeholder Education and Engagement**:
    - **Definition:** The level of awareness and engagement of stakeholders (including employees, clients, partners) regarding crypto agility.
    - **Importance:** Well-informed stakeholders contribute to a more secure implementation process.
    - **KPI:** Facilitating interactions with stakeholders on quantum safe cryptography and crypto agility.
    - **Calculation:** (number of informed stakeholders / total number of stakeholders) x 100%, as stakeholder engagement index score = int (percentage/10).
3. **Cost of Implementation**:
    - **Definition:** The cost to replace the current cryptography algorithm with a new one.
    - **Importance:** Lower implementation costs mean more cost-effective crypto agility.
    - **KPI:** Implementing a quantum risk assessment.
    - **Calculation:** (Total cost of implementation / number of algorithm swaps), as a cost index score (1 = is a high cost, 10 = is low cost).
4. **Risk of Implementation**:
    - **Definition:** The risk associated with implementing a new cryptography algorithm.
    - **Importance:** Lower risk means a more secure crypto agility strategy.
    - **KPI:** Implementing a quantum risk assessment.
    - **Calculation:** Assign a numerical score (e.g., 1 to 10) based on the assessed risk associated with implementing a new algorithm.
5. **Resource Utilization Ratio**:
    - **Definition:** Efficient use of personnel and technology resources for implementing crypto agility.
    - **Importance:** Optimal resource allocation ensures cost effectiveness and operational efficiency.
    - **KPI:** Demonstrate organizational maturity on crypto agility.
    - **Calculation:** (Actual resource usage / maximum available resource capacity) x 100%, as effectiveness ratio index score = int (percentage/10).
6. **Implementation Readiness Assessment**:
    - **Definition:** Evaluation of organizational preparedness to implement crypto agility.
    - **Importance:** Ensures a smooth transition without disrupting operations.
    - **KPI:** Providing solutions for quantum resistance and crypto agility; minimizing operational disruptions.
    - **Calculation:** Assign a numerical score (e.g., 1 to 10) based on the evaluation of organizational preparedness for implementing crypto agility.

7. **Algorithm Replacement Frequency**:
    - **Definition:** How often cryptographic algorithms are replaced or updated.
    - **Importance:** Frequent updates demonstrate proactive adaptation to emerging threats.
    - **KPI:** Navigating constant cryptographic evolution.
    - **Calculation:** Number of algorithm replacements or updates within a specific period (year).
8. **Compliance with Evolving Standards**:
    - **Definition:** Adherence to changing industry and regulatory cryptographic standards.
    - **Importance:** Demonstrates commitment to maintaining security in a rapidly changing environment.
    - **KPI:** Ensuring compliance with evolving standards.
    - **Calculation:** (Number of standards adhered to / total number of applicable standards) x 100%, as compliance percentage: score = int (percentage/10).
9. **Response Time to Emerging Threats**:
    - **Definition:** Time taken to identify and implement countermeasures against new cryptographic threats.
    - **Importance:** Swift responses enhance security posture and resilience.
    - **KPI:** Enabling swift responses to cryptographic breakthroughs.
    - **Calculation:** Time taken to identify and implement countermeasures against new cryptographic threats (hours or days). Can be represented as a score 1-10, where 1 is a very long time and 10 is short.
10. **Incident Response Efficiency**:
    - **Definition:** Effectiveness of the response to security incidents related to cryptographic vulnerabilities.
    - **Importance:** Efficient responses minimize potential damage and mitigate risks.
    - **KPI:** Enabling swift responses to cryptographic breakthroughs.
    - **Calculation:** Assign a numerical score (e.g., 1 to 10) based on the evaluation of the effectiveness of the response to security incidents related to cryptographic vulnerabilities**.**
11. **Time to Recovery after Algorithm Change**:
    - **Definition:** Duration taken to return to normal operations after implementing a new cryptographic algorithm.
    - **Importance:** Efficient recovery ensures minimal disruption to operations.
    - **KPI:** Enabling swift responses to cryptographic breakthroughs.
    - **Calculation:** Duration taken to return to normal operations after implementing a new cryptographic algorithm (hours). Can be represented as a score 1-10, where 1 is a very long time and 10 is short.
12. **Success Rate of Algorithm Implementation**:
    - **Definition:** Percentage of successful implementations of new cryptographic algorithms.
    - **Importance:** High success rates indicate effective planning and execution.
    - **KPI:** Supporting product resilience.
    - **Calculation:** (Number of successful algorithm implementations / total number of attempted algorithm implementations) x 100%: score = int (percentage/10)
13. **Employee Training Progress**:
    - **Definition:** Percentage of employees trained in crypto agility and quantum-resistant concepts.
    - **Importance:** Well-informed employees contribute to a culture of security awareness.
    - **KPI:** Demonstrating commitment to security, fostering a culture of security.
    - **Calculation:** (Number of employees trained on crypto agility and quantum-resistant concepts / total number of employees) x 100%: score = int (percentage/10)

The specific KPIs and associated metrics that are most relevant for your organization may vary based on your industry, size, and specific security requirements. It's important to tailor crypto agility metrics to align with your organizational goals and priorities.

PRODUCT/SERVICES METRICS

When it comes to products and software, two distinct realms emerge, each with its unique challenges and opportunities. Software, by nature, offers a remarkable degree of agility, with the potential for allowing swift implementation of new cryptographic standards and rapid response to emerging threats. This inherent flexibility empowers organizations to seamlessly transition between cryptographic algorithms, ensuring their security measures remain at the cutting edge. On the other hand, hardware, though foundational, often presents a more formidable challenge. Adapting cryptographic standards in hardware can be a meticulous process, requiring careful consideration of physical constraints to replacing hardware in the field. However, as we delve into the specific KPIs for products and software, it becomes evident that both realms play indispensable roles in the broader landscape of crypto agility. These metrics serve as guiding lights, illuminating the path to agile and resilient security measures, whether in the dynamic domain of software or the robust world of hardware. Through crypto agility KPI measurement and assessment, organizations can fine-tune their strategies, ensuring that their products and software remain cryptographic secure to the future quantum threat.

Here is example crypto agility specific metrics for the Product/Services View for Software and Hardware:

Software Products/Services:

14. **Algorithm Swap Time**:
    - **Definition:** The time taken to implement a new cryptographic algorithm in the software.
    - **Importance:** Reflects the software's agility in adapting to new cryptographic standards.
    - **KPI:** Minimizing operational disruptions; enabling swift responses to cryptographic breakthroughs; supporting product resilience.
    - **Calculation:** Total time taken for algorithm swaps / total number of algorithm swaps (hours). Can be represented as a score 1-10, where 1 is a very long time and 10 is short.
15. **Patch Deployment Efficiency**:
    - **Definition:** The speed at which security patches addressing cryptographic vulnerabilities are deployed.
    - **Importance:** Indicates the software's responsiveness to emerging cryptographic threats.
    - **KPI:** Minimizing operational disruptions; enabling swift responses to cryptographic breakthroughs; supporting product resilience.
    - **Calculation:** Total number of security patches deployed / time period in months or year. Can be represented as a score 1-10, where 1 is a very long time and 10 is short.
16. **Compatibility with Multiple Algorithms**:
    - **Definition:** The ability of the software to support and seamlessly transition between different cryptographic algorithms.
    - **Importance:** Demonstrates the software's versatility and readiness for algorithmic changes.
    - **KPI:** Minimizing operational disruptions; enabling swift responses to cryptographic breakthroughs; supporting product resilience; navigating constant cryptographic evolution.
    - **Calculation:** Expert evaluation based on the ability of the software to seamlessly transition between different cryptographic algorithms (on a scale 1-10).
17. **Crypto Module Update Frequency**:
    - **Definition:** How often cryptographic modules within the software are updated to incorporate the latest standards.
    - **Importance:** Indicates the software's commitment to staying current with cryptographic advancements.
    - **KPI:** Minimizing operational disruptions; enabling swift responses to cryptographic breakthroughs; supporting product resilience; navigating constant cryptographic evolution.
    - **Calculation:** Total number of crypto module updates / time period in years.

18. **Incident Response for Crypto Vulnerabilities**:
    - **Definition:** The effectiveness of response protocols in the event of security incidents related to cryptographic features.
    - **Importance:** Demonstrates the software's ability to swiftly mitigate cryptographic risks.
    - **KPI:** Minimizing operational disruptions; enabling swift responses to cryptographic breakthroughs; supporting product resilience.
    - **Calculation:** Expert evaluation based on the effectiveness of response protocols in the event of security incidents related to cryptographic features (on a scale 1-10).

Hardware Products/Services:

19. **Compatibility with Quantum-Resistant Algorithms**:
    - **Definition:** The hardware's capacity to support and integrate quantum-resistant cryptographic algorithms.
    - **Importance:** Indicates the hardware's readiness for the quantum era.
    - **KPI:** Enabling swift responses to cryptographic breakthroughs; providing solutions for quantum resistance.
    - **Calculation:** Expert evaluation based on the hardware's capacity to support and integrate quantum-resistant cryptographic algorithms (scale 1-10).
20. **Firmware Update Turnaround**:
    - **Definition:** The time taken to develop and deploy firmware updates addressing cryptographic vulnerabilities.
    - **Importance:** Reflects the agility of hardware in adapting to new cryptographic standards.
    - **KPI:** Minimizing operational disruptions; enabling swift responses to cryptographic breakthroughs; supporting product resilience.
    - **Calculation:** Total time taken for firmware updates / total number of firmware updates (hours). Can be represented as a score 1-10, where 1 is a very long time and 10 is short.
21. **Retrofitting Feasibility**:
    - **Definition:** The ease with which existing hardware can be retrofitted or upgraded to incorporate quantum-resistant features.
    - **Importance:** Determines the hardware's adaptability to quantum threats without requiring a complete overhaul.
    - **KPI:** Supporting product resilience.
    - **Calculation:** Expert evaluation based on the ease with which existing hardware can be retrofitted or upgraded to incorporate quantum-resistant features (scale 1-10).
22. **Hardware Replacement Cycle for Cryptographic Enhancements**:
    - **Definition:** How often hardware components are replaced or updated to enhance cryptographic capabilities.
    - **Importance:** Reflects the hardware's commitment to evolving cryptographic standards.
    - **KPI:** Supporting product resilience.
    - **Calculation:** Total number of replacements or updates for cryptographic enhancements / time period in years.
23. **Resistance to Side-Channel Attacks**:
    - **Definition:** The effectiveness of hardware in protecting against side-channel attacks targeting cryptographic operations.
    - **Importance:** Indicates the hardware's robustness in safeguarding sensitive information.
    - **KPI:** Supporting product resilience.
    - **Calculation:** Expert evaluation based on the effectiveness of hardware in protecting against side-channel attacks targeting cryptographic operations (scale 1-10).

CRYPTO AGILITY KPI SCORECARD

In this sample scorecard, each KPI is assigned a score out of 10, reflecting the organization's performance in that area.

These scores are hypothetical and should be based on actual assessments and goals set by the organization.

KPI	Metric Score (Time)
Organizational & Operational Strategy	
Cycle Time for Algorithm Implementation	7 (8 hours)
Stakeholder Education and Engagement	5
Cost of Implementation	7
Risk of Implementation	8
Resource Utilization Ratio	9
Implementation Readiness Assessment	7
Algorithm Replacement Frequency	2
Compliance with Evolving Standards	9
Response Time to Emerging Threats	6 (12 hours)
Incident Response Efficiency	9
Time to Recovery after Algorithm Change	7 (6 hours)
Success Rate of Algorithm Implementation	9
Employee Training Progress	8
Software Products/Services	
Algorithm Swap Time	8 (4 hours)
Patch Deployment Efficiency	8
Compatibility with Multiple Algorithms	9
Crypto Module Update Frequency	2
Incident Response for Crypto Vulnerabilities	9
Hardware Products/Services	
Compatibility with Quantum-Resistant Algorithms	7
Firmware Update Turnaround	9 (3 hours)
Retrofitting Feasibility	7
Hardware Replacement Cycle for Cryptographic Enhancements	1
Resistance to Side-Channel Attacks	9

SUPPLIERS, VENDORS VIEW

The complexity of designing, developing, and deploying quantum-safe algorithms will also extend to an organization's third-party partners. There may be several vendors that provide different services to the organization across the supply chain, from cloud services to endpoint detection. There are different protocols that may be in use – and different complexities involved in upgrading these vendor services.

As we move towards better crypto agility for new vendors, the crypto agility KPI scorecard may help add to the security parameters on which vendors should be evaluated. If they are going to be placed closer to an organization's critical operations, a chosen vendor should meet these KPIs at organization-set thresholds. For existing vendors, these KPIs would help evaluate whether (a) a vendor does not meet enough crypto agility parameters and needs to be replaced, or (b) a vendor can be provisioned to add upgrades to swap out existing encryption systems. These metrics inform the organization and provide critical insights to vendors and any third parties involved.

While the scorecard would help understand the extent of risk, with the scoring definitions set by the organization, they should be assessed in context based on actual risk to the vendor-provided system. Furthermore, when creating vendor contracts, organizations should also document assets that are affected for specific vendors, upgrade responsibility, the timeline and frequency of upgrades, and the response and recovery plan in case of an incident. Responsibility assignment is important to speed up the process of making changes to swap out algorithms, especially if the encryption equipment is on premise.

RISK ASSESSMENT USE CASES

In the realm of telecommunications, the significance of cryptographic agility cannot be overstated. With the impending arrival of quantum computing, telecom networks face a pressing need to fortify their security measures. This section presents an array of use cases spotlighting the application of crypto agility scorecards within telecom enterprises. By evaluating various scenarios, ranging from network infrastructure to data transmission protocols, these use cases illuminate the critical role of crypto agility in mitigating potential threats. Each use case delves into how a tailored crypto agility scorecard serves as an invaluable tool, allowing telecom providers to assess their readiness, adaptability, and robustness against evolving security challenges in the face of the quantum revolution.

IoT Device Crypto Agility Assessment

Unlike conventional systems, many existing IoT devices in operation often rely on embedded hardware cryptography, which, due to its nature, may not be amenable to swift updates through traditional software patches. This use case delves into the specific challenges posed by IoT hardware constraints and outlines a pragmatic scorecard tailored to these devices. Through this assessment, we aim to illuminate the path for IoT adopters, offering insights into how to manage the security posture of these devices within the evolving landscape of quantum threats.

An assessment of an IoT device deployment that has hardware based cryptographic functions with a focus on crypto agility using the provided scorecard format:

Organizational & Operational Strategy Crypto Agility KPIs:

KPI	Metric	Comments
Cycle Time for Algorithm Implementation	N/A	Due to the hardware limitations, this KPI is not applicable.
Stakeholder Education and Engagement	8	Stakeholders are well informed about the need for hardware upgrades and understand the associated challenges.
Cost of Implementation	2	The cost of replacing the existing devices with new ones is high.
Risk of Implementation	7	There's a moderate risk associated with implementing new devices due to potential disruptions during the upgrade process.
Resource Utilization Ratio	6	Resources are efficiently allocated for planning and executing hardware upgrades.
Implementation Readiness Assessment	7	The organization has a solid plan for hardware upgrades, but the process is time consuming and costly.
Algorithm Replacement Frequency	N/A	Due to hardware constraints, this KPI is not applicable.
Compliance with Evolving Standards	6	The organization is committed to adhering to industry standards, but the hardware limitations pose challenges.
Response Time to Emerging Threats	2	Response time is relatively slower due to the need for physical upgrades.
Incident Response Efficiency	7	The organization has established effective incident response protocols, but hardware constraints may extend resolution times.
Time to Recovery after Algorithm Change	N/A	Due to hardware constraints, this KPI is not applicable.
Success Rate of Algorithm Implementation	N/A	Due to hardware constraints, this KPI is not applicable.
Employee Training Progress	9	Employees are well trained on the importance of hardware upgrades and their role in the process.

Product Software Crypto Agility KPIs:		
KPI	**Metric**	**Comments**
Algorithm Swap Time	N/A	Due to hardware constraints, this KPI is not applicable.
Patch Deployment Efficiency	N/A	Due to hardware constraints, this KPI is not applicable.
Compatibility with Multiple Algorithms	2	The device is limited in its ability to support multiple cryptographic algorithms.
Crypto Module Update Frequency	N/A	Due to hardware constraints, this KPI is not applicable.
Incident Response for Crypto Vulnerabilities	6	Although the device has response protocols, hardware constraints may impact the speed of implementation.

Product Hardware Crypto Agility KPIs:		
KPI	**Metric**	**Comments**
Compatibility with Quantum-Resistant Algorithms	3	The current hardware is not readily compatible with quantum-resistant algorithms.
Firmware Update Turnaround	2	Firmware updates are slow and require complete device replacement, resulting in longer turnaround times.
Retrofitting Feasibility	1	Retrofitting is highly challenging and not cost effective; new devices are the only viable option.
Hardware Replacement Cycle for Cryptographic Enhancements	3	The cycle is long due to the need for physical upgrades.
Resistance to Side-Channel Attacks	7	The hardware exhibits good resistance to side-channel attacks, providing a strong security foundation.

The transition to quantum secure cryptography assessment highlights the challenges faced by the IoT device in terms of crypto agility, especially due to its reliance on the use of hardware cryptography and the inability to be updated via software. The organization needs to carefully plan and allocate resources for hardware upgrades, considering the associated costs and time implications.

3GPP 5G Infrastructure Transition Scorecard with Crypto Agility Focus

As 5G infrastructure evolves, the urgent need to align with emerging cryptographic standards and fortify against quantum threats becomes paramount. This use case zeroes in on the development of a crypto agility scorecard tailored for the 3rd Generation Partnership Project (3GPP) 5G transition. Specifically, it assesses the infrastructure's readiness to embrace new standards, particularly those enhancing quantum resistance. With a focus on the implementation of PQC, this evaluation provides a pragmatic measure of the 5G network's crypto agility maturity. The scorecard, designed with key performance indicators attuned to the unique challenges of the 5G landscape, aims to offer telecom leaders a clear roadmap for ensuring robust security and operational resilience in the face of evolving cryptographic paradigms.

An assessment of the transition to 3GPP 5G infrastructure with a focus on crypto agility using the provided scorecard format:

Organizational & Operational Strategy Crypto Agility KPIs:		
KPI	**Metric**	**Comments**
Cycle Time for Algorithm Implementation	3	The transition may experience extended cycles due to the time-consuming process of defining and implementing 3GPP standards for quantum-resistant cryptography.
Stakeholder Education and Engagement	8	Stakeholders are well informed about the importance of aligning with 3GPP standards and implementing quantum-resistant cryptography.
Cost of Implementation	7	Although the cost may be significant, it's necessary to ensure compliance with 3GPP standards and implement quantum-resistant cryptography effectively.
Risk of Implementation	5	The risk is moderate due to the complexity of aligning with evolving 3GPP standards, but it's essential for long-term security.
Resource Utilization Ratio	6	Resources are allocated efficiently to stay updated with 3GPP standards and to implement quantum-resistant cryptography effectively.
Implementation Readiness Assessment	6	The organization has a solid understanding of the challenges posed by evolving 3GPP standards. However, the long standardization process may delay readiness.
Algorithm Replacement Frequency	2	The frequency may be low due to the extended duration of 3GPP standardization processes.
Compliance with Evolving Standards	7	The organization is committed to complying with 3GPP standards, recognizing their crucial role in ensuring interoperability and security.
Response Time to Emerging Threats	4	The response time might be slower due to the need to align with 3GPP standards before implementing quantum-resistant cryptography.
Incident Response Efficiency	6	Incident response is well structured, but the implementation of quantum-resistant cryptography might add complexity.
Time to Recovery after Algorithm Change	4	The transition might result in longer recovery times due to the need to align with 3GPP standards before implementing quantum-resistant cryptography.
Success Rate of Algorithm Implementation	5	Success rates may be impacted by the complexity of aligning with 3GPP standards and implementing quantum-resistant cryptography.
Employee Training Progress	7	Employees are well trained on the importance of aligning with 3GPP standards and implementing quantum-resistant cryptography.

Product Software Crypto Agility KPIs:		
KPI	**Metric**	**Comments**
Algorithm Swap Time	6	The time taken for algorithm swaps is reasonable, considering the adherence to 3GPP standards.
Patch Deployment Efficiency	5	Patch deployment might take longer due to the need for compliance with evolving 3GPP standards.
Compatibility with Multiple Algorithms	7	The product exhibits good compatibility with various cryptographic algorithms, aligning with 3GPP standards.
Crypto Module Update Frequency	3	The update frequency might be lower due to the extended standardization process in 3GPP.
Incident Response for Crypto Vulnerabilities	6	Incident response protocols are effective, but may require adjustment to accommodate the implementation of quantum-resistant cryptography.

Product Hardware Crypto Agility KPIs:		
KPI	**Metric**	**Comments**
Compatibility with Quantum-Resistant Algorithms	3	Compatibility with quantum-resistant algorithms might be challenging due to the evolving nature of 3GPP standards.
Firmware Update Turnaround	5	Firmware updates may take longer to ensure compliance with 3GPP standards for quantum-resistant cryptography.
Retrofitting Feasibility	4	Retrofitting might be feasible, but the extended standardization process may affect its practicality.
Hardware Replacement Cycle for Cryptographic Enhancements	6	The cycle may be extended due to the need for aligning with 3GPP standards before implementing quantum-resistant cryptography.
Resistance to Side-Channel Attacks	7	The product exhibits strong resistance to side-channel attacks, providing a robust security foundation.

This assessment reflects the challenges and considerations associated with the transition to 3GPP 5G infrastructure, especially in the context of crypto agility and adherence to evolving 3GPP standards.

RECOMMENDATIONS
CALL TO ACTION

In the face of the looming quantum threat, organizations must take decisive action to fortify their systems against potential breaches. The store now, decrypt later scenario presents a palpable risk, underlining the urgency of preparedness. Prioritizing the implementation of crypto agility is paramount, extending beyond product integration to encompass well-defined organizational strategies. This involves:

- **Establish a dedicated Crypto Agility Team:** Form a task force responsible for overseeing the implementation of crypto agility strategies, comprising experts from various departments for a comprehensive approach.
- **Implement Systematic KPI Monitoring:** Set up a consistent process for tracking crypto agility KPIs across the organization, products, and stakeholder interactions. This enables timely adjustments to security measures.
- **Adopt a Quantum Risk Assessment Framework:** Incorporate a structured QRA framework like CARAF to evaluate and enhance crypto agility, providing a methodical approach to identifying vulnerabilities and adapting to emerging threats.
- **Prioritize Stakeholder Education:** Ensure all stakeholders are well informed about crypto agility's importance. This fosters a culture of security awareness and contributes to a more secure implementation process.
- **Invest in Employee Training:** Allocate resources for training employees in crypto agility and quantum-resistant concepts. A well-informed workforce is crucial for a robust security posture.
- **Foster a Culture of Security Awareness:** Emphasize the significance of crypto agility throughout the organization, encouraging employees to stay updated on emerging threats and best practices in cryptography.
- **Plan for Quantum-Resistant Solutions:** Prepare your organization to transition to quantum-resistant cryptographic algorithms, ensuring that your security measures remain effective in the face of evolving technology.
- **Collaborate with Industry Experts:** Engage with industry initiatives, standards bodies, and experts to stay abreast of the latest developments in crypto agility and PQC. This collaborative approach enhances your organization's readiness.
- **Regularly Review and Update Strategies:** Keep your crypto agility strategies dynamic and responsive by conducting regular reviews. This ensures that they remain aligned with evolving cryptographic standards and emerging threats.
- **Document and Communicate Progress:** Maintain clear records of your crypto agility initiatives and communicate updates to internal and external stakeholders. This showcases your organization's commitment to security.
- **Prepare for Quantum Threats Today:** Start performing quantum-focused risk assessments now to prepare for potential future threats, even before functional quantum computers become a reality.
- **Stay Proactive and Forward Thinking:** Understand that crypto agility is an ongoing process. Being proactive and forward-thinking in your approach to cybersecurity positions your organization as a leader in adapting to emerging threats.

These recommendations collectively form a robust crypto agility framework, demonstrating a commitment to strong cybersecurity practices. This proactive approach builds trust with stakeholders, enhances operational resilience, and ensures compliance with evolving security standards. Remember, regular measurement and assessment of associated metrics are crucial to evaluating progress and fine-tuning strategies.

In the landscape of cryptographic agility, it's crucial for risk assessments to acknowledge the inherent constraints of certain scenarios where achieving crypto agility might be challenging or, in some cases, unattainable. Recognizing that not every system or context permits seamless transitions between cryptographic algorithms is a pragmatic approach, such as for hardware constraints. In these instances, the focus shifts to a comprehensive risk acceptance strategy. Understanding and articulating the limitations in achieving crypto agility form an integral part of risk assessment. The key is to ensure that the level of risk acceptance aligns with the organization's overall risk tolerance and security objectives. By identifying the level of crypto agility through KPI metrics, while transparently acknowledging situations where crypto agility might be limited and support a well-defined risk acceptance stance, organizations can make informed decisions that balance security requirements with the practicalities of specific environments. This nuanced approach contributes to a more resilient and adaptable cybersecurity posture.

Furthermore, adopting a quantum risk assessment framework for crypto agility, complemented by a well-defined set of metrics, will be instrumental in ensuring quantum resilience. These metrics inform the organization and provide critical insights to vendors and any third parties involved. They stand as informed measures of the organization's level of crypto agility, offering a clear and comprehensive view of its preparedness against emerging quantum threats.

This proactive stance, rooted in a strategic and well-informed approach, serves to protect sensitive data and uphold the integrity of critical systems, fortifying them for the quantum revolution on the horizon.

REFERENCES

[1] Shor, P. W., (November 1994) "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science. p. 124-134. https://ieeexplore.ieee.org/document/365700.

[2] Gidney, C., Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, https://quantum-journal.org/papers/q-2021-04-15-433/.

[3] NIST IR 8105, Report on Post-Quantum Cryptography, https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf.

[4] Deloitte, Preparing the trusted internet for the age of quantum computing, https://www.deloitte.com/global/en/our-thinking/insights/topics/risk-management/crypto-agility-quantum-computing-security.html

[5] Quantum Threat Timeline Report 2022, Global Risk Institute, https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/.

[6] Ma, C., Colon, L., Dera, J., Rashidi, B., Garg, V. (2021). CARAF: Crypto Agility Risk Assessment Framework, Journal of Cybersecurity. https://academic.oup.com/cybersecurity/article/7/1/tyab013/6289827

[7] Commercial National Security Algorithm Suite 2.0, https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF.

[8] National Cybersecurity Strategy Implementation Plan – July 2023, https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov.pdf.

[9] National Institute of Standards and Technology Cryptographic Module Validation Program, https://csrc.nist.rip/groups/STM/common_documents/DESTranPlan.pdf.

[10] Replacing classic encryption with NIST-backed Post Quantum Cryptography (PQC) will be a major undertaking affecting the data, systems, devices, and networks we rely on daily, https://quantumxc.com/pqc-migration/.

ACRONYMS AND ABBREVIATIONS

3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
CARAF	Crypto Agility Risk Assessment Framework
CNSA	Commercial National Security Algorithm Suite
CRQC	Cryptographically Relevant Quantum Computer
DES	Data Encryption Standard
IoT	Internet of Things
KPI	Key Performance Indicator
NIST	National Institute of Standards and Technology
PKI	Public-Key Infrastructure
PQC	Post-Quantum Cryptography
QCTA	Quantum-Capable Threat Actors
QRA	Quantum Risk Assessment
QSCII	Quantum-Safe Communications and Information Initiative
ROSI	Return on Security Investment
RSA	Rivest-Shamir-Adleman
TLS	Transport Layer Security

COPYRIGHT AND DISCLAIMER

ATIS-I-0000098

Published January 2024

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

www.atis.org
For information, contact ATIS at (202) 628-6380.