The quantum clock is ticking

How quantum safe is your organization?

GSMA™

IBM

How IBM can help

Quantum computing has the potential to provide immense business value for clients, but it will also be able to break some of the most widely used cryptographic protocols in the world. Leaders face an imperative to understand the unique risk quantum technology poses to their systems and data and develop a quantum-safe strategy. IBM Quantum Safe provides a comprehensive set of tools, capabilities, and approaches combined with deep expertise to help organizations plan and execute their migration to quantum-safe cryptography. For more information visit https://www.ibm.com/quantum/quantum-safe

Foreword

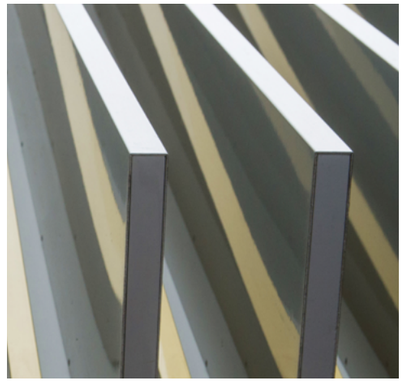
The world is hurtling toward a quantum-enabled future, and the imperative to prioritize quantum-safe readiness has never been more pressing. The rapid advancement of quantum computing poses a significant threat to the security of our digital landscape, and the consequences of inaction are too great to ignore. This is no longer a concern relegated to the IT department but a board-level concern that transcends industry boundaries.

The GSMA, recognizing the critical role of telecommunications in underpinning all industries, has been at the forefront of this effort since 2022. Through our Post Quantum Telco Network Task Force (PQTN TF), the GSMA is supporting its members in preparing for a post-quantum world. From publishing white papers on the security of telecommunications networks in the post-quantum era to providing guidelines on post-quantum safe use cases, the task force has made significant strides.

This report highlights that while quantum-safe awareness remains low, it is a strategic business imperative and competitive differentiator. As Sujith Surendranathan, Director, Database Security and Data Protection at Sun Life, astutely notes, “It’s important for all organizations to recognize that exposure to quantum threats exists independently of their adoption of quantum computing.”

We are delighted to support this timely, relevant report, which provides valuable insights and guidance to navigating the complexities of quantum-safe readiness. And as our membership grows, we are committed to empowering organizations with the knowledge and tools necessary to thrive in a post-quantum world.

Richard Cockle
Head of Connected Industries
GSMA



Key takeaways

While quantum-safe awareness is currently low, cybercriminals are harvesting data now with the goal of decrypting it later, once cryptographically relevant quantum computers become available.

Given our pervasive reliance on cryptography for securing digital transactions, quantum safety is a strategic business imperative and a competitive differentiator.

The digital economy is built on data integrity, with reliable cryptographic solutions being both the ultimate line of defense and an enhancement to business value. But sensitive data—such as financial information, personally identifiable information, phone data, network communications, and intellectual property—is already vulnerable.

Quantum-Safe Champions are acting *now*.

88% of QSCs actively assess their preparedness for quantum-safe security, three and a half times that of the least-ready organizations. 82% of QSCs have crypto-agility programs to transition applications and systems toward adopting quantum-safe cryptography solutions, three times that of their least-ready counterparts.

Quantum-Safe Champions prioritize new talent as a critical success factor two times more than global survey respondents.

Overall, talent scarcity is the biggest concern voiced by IBM Quantum-Safe clients.[1] Without the appropriate skills on board, quantum safety is unobtainable.

Why is quantum safe a board-level concern?

We can't state it more plainly: the exchange of business value is built upon reliable cryptographic standards. Yet, the everyday encryption we take for granted is now under threat—with profound real-world consequences.

First, we need to level-set the misconception that quantum computers are just an esoteric research project. In fact, quantum computing has progressed beyond lab experiments. For example, in June 2023, IBM Quantum and UC Berkeley demonstrated that quantum computers are beginning to outperform leading classical simulations by dramatically improving error mitigation.[2] More recently, IBM demonstrated the ability to improve the efficiency of quantum error correction by nearly a factor of 10.[3]

Increasingly, quantum computing is garnering media attention, with coverage in the *New York Times*,[4] the *Economist*,[5] and the US news show *60 Minutes*.[6] The possibilities for scientific, medical, and technical breakthroughs are both exciting and astonishing.

But the downside of quantum computing's ascendance? Security exposures. Significant ones.

Over the next several years, quantum computing capabilities will jeopardize widespread public-key cryptography (PKC) algorithms such as RSA and Diffie-Hellman. In fact, any classically encrypted communication is already vulnerable to exfiltration. That's because threat actors are already harvesting encrypted communications with the intention of decrypting that data once quantum decryption solutions are available—a technique known as "harvest now, decrypt later" attacks.[7]

The digital economy is dependent on cryptography for establishing and maintaining safe, secure exchanges of value. Once quantum computers become cryptographically relevant, sensitive data—such as financial information, personally identifiable information, phone data, network communications, and intellectual property—could be compromised. The result? Significant financial losses—and worse, a critical loss of trust with customers, partners, and stakeholders. In other words, trust itself is now under threat.

As Sujith Surendranathan, Director, Database Security and Data Protection at Sun Life, astutely points out, "Adopting new technologies like generative AI involves balancing enablement with inherent risks. It's important for all organizations to recognize that exposure to quantum threats exists independently of their adoption of quantum computing."

In short, implementing quantum-safe cryptography is not just sound in terms of security practices. Given our growing dependency on cryptography for the security and safety of our digital world, transitioning to quantum-safe cryptography is essential to preserving the integrity of digital trust mechanisms as a whole.

Recognizing this challenge, the IBM Institute for Business Value (IBM IBV), in partnership with Oxford Economics, surveyed 565 executives, including CxOs, across 15 countries and 13 industries—all representing organizations with a minimum $250 million in annual revenue. The IBM IBV then analyzed these responses to develop a Quantum-Safe Readiness Index (see Perspective, "Understanding the IBM Quantum-Safe Readiness Index"). This index is based on a systematic assessment of organizations' quantum-safe readiness. Assessment outcomes are intended to inform and guide strategic stakeholders about the timeliness and urgency of their quantum-safe transformation efforts.

"Adopting new technologies like generative AI involves balancing enablement with inherent risks. It's important for all organizations to recognize that exposure to quantum threats exists independently of their adoption of quantum computing."

Sujith Surendranathan
Director, Database Security and Data Protection at Sun Life

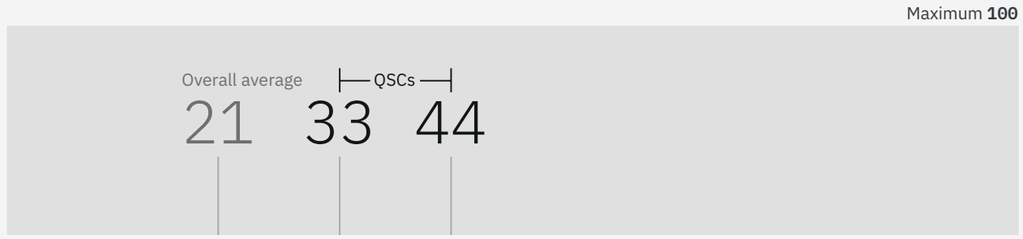
Perspective

Understanding the IBM Quantum-Safe Readiness Index

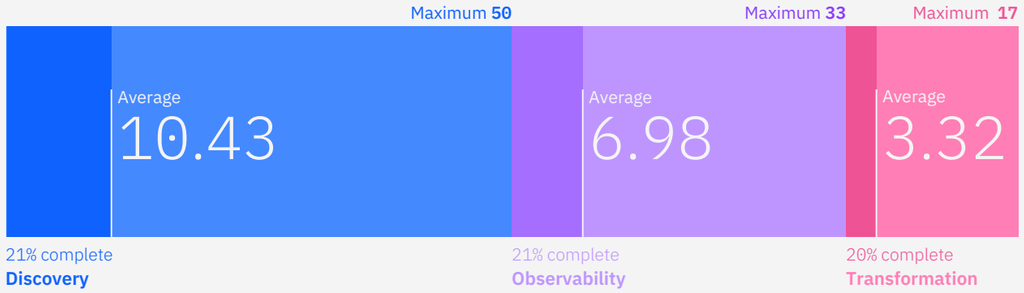
The IBM Quantum-Safe Readiness Index (QSRI) assesses the global state of readiness for security in the quantum era, as measured by the readiness of individual organizations. The QSRI is intended to help leaders and stakeholders understand how their organizations are progressing in their quantum-safe initiatives.

The QSRI evaluates 14 activities, or indicators, across three key areas: quantum-safe discovery, observability, and transformation (see figure). Scores provide an indication of the organization's relative progress in their journey to becoming a quantum-safe organization. These 14 indicators are grouped into the below three categories and weighted based on IBM's subject-matter expertise and experience with clients. Scores are calculated based upon a 100-point index, with 100 representing the maximum possible score. The QSRI is intended to assess (and re-assess) the quantum-safe readiness of an organization, industry, or region over time.

The average quantum-safe readiness score: 21 out of 100



Measuring progress towards quantum-safe readiness



As of the date of this study, global organizations average a score of 21 on a 100-point scale—in other words, they are currently at a low level of quantum-safe readiness. We have designated organizations with the highest QSRI scores—the top 10%—as Quantum-Safe Champions (QSCs). QSCs scored 33 or above, with 44 being the highest score attained by any organization (see figure).

Given quantum safety is only now gaining more visibility—with many organizations still in the planning stages—the quantum-safe readiness score is most influenced by early-stage activities such as an organization's discovery capabilities.

Over the past 18 months, IBM subject-matter experts have noted a distinct rise in the awareness and importance leaders are placing in quantum-safe transformation. Our expectation is that Quantum-Safe Readiness Index scores will rise as awareness continues to grow. As well, the Index itself will evolve as the technology matures.

Overall, organizations in our survey expect that, when starting from their current levels of quantum preparedness, it will take 12 years to fully integrate quantum-safe standards into their business. In fact, National Security Agency guidance requires full compliance with post-quantum cryptography (PQC) for National Security Systems by 2035. When considering those requirements—along with the lead time needed to identify cryptographic assets and dependencies, implement new standards, and align with partners—the time to begin quantum-safe initiatives is now.[8]

In this report, we explore how Quantum-Safe Champions are driving not only outperformance overall, but a forward-looking mindset that's innately attuned to establishing a quantum-safe culture. We highlight how QSCs cultivate a talent ecosystem. Then, we dive into how, when compared to their counterparts, QSCs report more resilient operations now—and anticipate greater resilience against quantum-enabled security risks. We include steps at the end of each section outlining how organizations can bolster their cybersecurity defenses as they make plans to implement pending quantum-safe standards. We explain some of the ancillary benefits associated with quantum safety, and how they can position quantum safety as a strategic differentiator.

Part one:
Creating competitive advantage
Quantum-safe strategy and investment

Organizations face multitudes of challenges in managing digital operations, from supply chain struggles to talent shortages to data breaches

The most astute organizations are nimble: they can negotiate the crisis of the moment and strategize for the future simultaneously. Even when mired in today's unknowns, they're thinking ahead, adept at turning uncertainty into opportunity.

For QSCs, quantum safety is part of a larger mission, a multifaceted organizational commitment to prioritize innovation.

Quantum-Safe Champions are setting the pace

Quantum-Safe Champions are laying the foundations for future success. With cryptographically relevant quantum computers still several years out, it takes a proactive, strategic mindset to not only embrace the urgency of quantum-safe cryptography—but to act on it.

Over the last three years, QSCs have outperformed their peers in a multitude of operational metrics, including agility and profitability (see Figure 1). That doesn't mean being quantum safe contributes directly to these advantages today. But for QSCs, quantum safety is part of a larger mission, a multifaceted organizational commitment to prioritize innovation and become more forward-thinking than peers. In fact, QSCs prioritize agility as critical to their organizational success four times more —a telling glimpse into their approach to operations.

FIGURE 1

QSCs have outperformed their peers over the last three years on key performance measures

86%

outperform peers in agility

75%

outperform peers in efficiency and profitability

73%

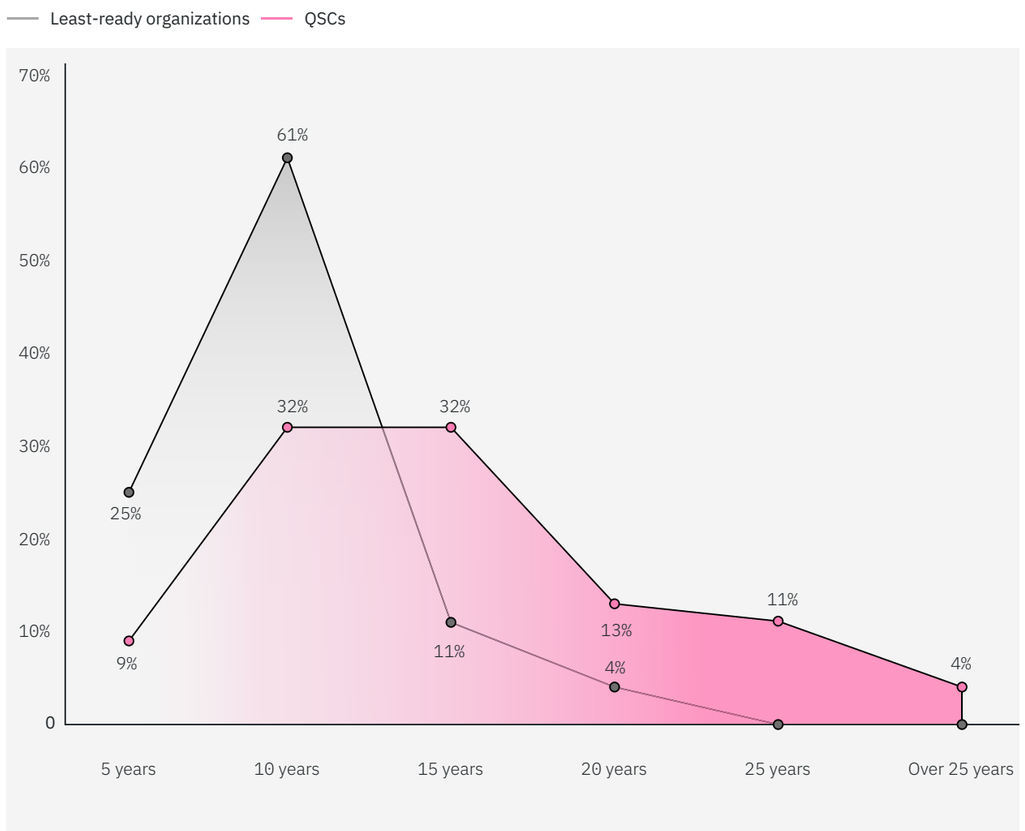
outperform peers in digital transformation

The time value of data

Quantum-Safe Champions have an important commonality: a need to keep their operational data secure and confidential over a longer period of time (see Figure 2). For example, in financial services, over 40% of organizations surveyed expect their data to be secure and confidential for a 25-year period or beyond. It's logical that they would adopt a preemptive stance toward building a secure, trusted data foundation, and anticipate pending quantum-enabled cybersecurity risks.

FIGURE 2

QSCs have a longer time value of organizational data

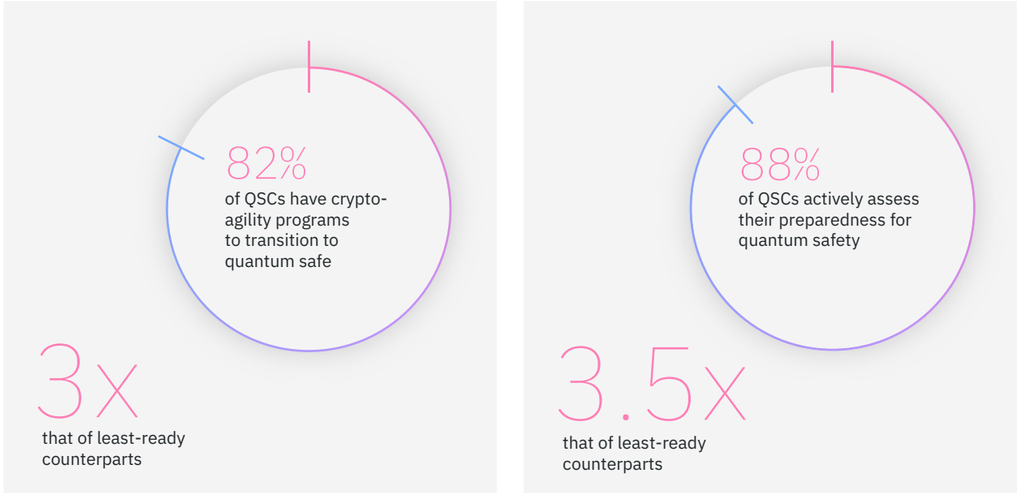


Keeping data secure for longer—both in terms of business and technical requirements—can contribute to another distinguishing feature of QSCs: a strong alignment of cybersecurity strategy with business and IT strategies. QSCs report 84% alignment of their cybersecurity strategy with their business strategy, two times that of the bottom decile. QSCs also report 73% alignment of their cybersecurity strategy and IT strategy.

Their proactive approach to data is just one way QSCs are realizing significant benefits over their least-ready counterparts (see Figure 3). A quantum-safe heartbeat is already core to their operations. Almost nine in ten QSCs actively assess their preparedness for quantum-safe security, more than triple that of their least-ready counterparts. 82% of QSCs already have crypto-agility programs to transition applications and systems to quantum safe. This is three times more than the bottom decile.

FIGURE 3

QSCs are investing now in their post-quantum future



"It's like running a marathon. We need to pick a pace that's right for our organization—reflecting our business priorities—and one that doesn't see us wasting time and then scrambling to catch up."

Paul Ballard
Technology Strategy and Enterprise Architecture Director, Nationwide Building Society (UK)

Leaders need to understand the clock is ticking. "The risk for me is the time it takes to implement quantum safe," says Paul Ballard, Technology Strategy and Enterprise Architecture Director at UK-based Nationwide Building Society.

"Implementing post-quantum cryptography may take a while. If we don't use our time wisely, we could be in trouble. It's like running a marathon. We need to pick a pace that's right for our organization—reflecting our business priorities—and one that doesn't see us wasting time and then scrambling to catch up."

Perspective

What is crypto-agility?[9]

Organizations use crypto-agility, also known as cryptographic agility, to promptly address potential threats to their data encryption. This approach enables organizations to adapt to alternative encryption standards without undergoing significant infrastructure changes. Cryptography, which involves the use of complex codes and algorithms to protect information and communications, is a crucial aspect of data security. Crypto-agility serves as an additional safety measure and can be viewed as an incident response mechanism—as well as a measure of enterprise responsiveness.

Crypto-agility is not only useful in response to known vulnerabilities but also in instances where an algorithm suddenly fails or when there has been a security breach. In these situations, quick action is necessary to minimize the impact of the incident. By implementing crypto-agility, organizations can help ensure that their data remains secure and protected from potential threats.

In summary, crypto-agility is a proactive approach to data encryption that enables organizations to adapt quickly to changing security needs. Crypto-agility is an essential component of a comprehensive security strategy, helping ensure that sensitive information remains secure and protected from potential threats. Crypto-agility is not only useful as a response to cryptographic vulnerabilities, it's an effective measure of an enterprise's operational agility as a whole.

Case study

Post-quantum cryptography for EU digital security[10]

In April 2024, the European Commission published a recommendation aimed at encouraging member states to develop and implement a harmonized approach to post-quantum cryptography. This synchronized strategy is intended to help ensure the EU's digital infrastructure and services are secure even before quantum computing capabilities become widely available. And an important caveat: integrating post-quantum cryptography into security measures does not require a quantum computer.

Quantum-safe cryptography is based upon mathematical problems that even quantum computers cannot resolve. Because quantum -safe solutions encompass people, processes, technology, and strategy, leaders must work together to facilitate coordination across security, technology, data, and architecture teams.

The European Commission is pledging to help EU member states develop a consistent, coordinated strategy. A key result: promoting interoperability between countries, with services and systems functioning seamlessly across borders.

While bringing numerous benefits, the advent of quantum computing will render some legacy data encryption solutions more vulnerable. Legacy encryption for data at rest is not (yet) vulnerable to quantum computing exploits.[11] Deploying quantum-safe cryptography is a critical defense in thwarting cyber criminals' abilities to exfiltrate sensitive data and gain operational leverage. And these regulations are not purely defensive in nature. Much as the advent of GDPR occasioned new approaches to data privacy—and prompted innovation and investment—quantum safe can spur broader transformation efforts in cryptography, data encryption, and digital communications.

Investing in a secure future

For many organizations, quantum safety is extended from their data security portfolio. And with the shift to AI operations, the value of their data is growing. The global average cost of a data breach in 2023 was $4.45 million, and in the US, the average cost was $9.48 million.[12] In response, budgetary commitments to cybersecurity are increasing across the board. Our research shows that in 2023, 10% of organizations' IT budgets were devoted to cybersecurity. This is up 25% from 2021 and is expected to increase by a further 22% by 2025.

Funding increases reflect board-level commitment. For any organization to be successful, senior executives and stakeholders need to encourage continued investments in quantum safe and recognize that the value of crypto-agility programs requires a collaborative effort.

"The Chief Information Security Officer (CISO) plays an important role here," observes David Boda, Chief Security and Resiliency Officer for Nationwide Building Society (UK). "The CISO needs to have built strong relationships with the board. They should be viewed as a trusted advisor. That way, when we say quantum safety should be on your agenda, the board is receptive."

"The CISO needs to have built strong relationships with the board. They should be viewed as a trusted advisor. That way, when we say quantum safety should be on your agenda, the board is receptive."

David Boda
Chief Security and Resiliency Officer, Nationwide Building Society (UK)

Steps to take

1. **Create awareness at the board level for your organization** to respond programmatically and strategically to the need for quantum safety. Gain sponsorship and support from your board.

2. **Communicate the business need for becoming quantum safe**, thereby elevating quantum safety to a joint business and IT initiative. Identify stakeholders and gain their buy-in.

3. **Assess and evaluate the risk-based cryptographic posture** of your organization with a view to remediation, as well as creating a competitive differentiator.

4. **Begin development of a robust plan for the transformation** of your organization to quantum safety and also, in the process, crypto-agility. Estimate investments required over the duration of the journey.

Part two:
A quantum-safe culture
Developing talent and subject-matter expertise

Without the appropriate skills, quantum safety is unobtainable. In fact, IBM Quantum-Safe consultants tell us talent scarcity is the biggest concern voiced by clients.[13] Not surprisingly, Quantum-Safe Champions prioritize new talent as a critical success factor two times more than global survey respondents in general.

This represents an opportunity for growth, with leaders expecting 12% of their technology workforce to expand skills enabling quantum-safe security standards over the next three years. But will that be enough? “The talent is not abundantly available,” concedes Sujith Surendranathan of Sun Life. “We’ve found challenges hiring externally for certain niche roles—but have found it beneficial to focus on developing our existing resources.”

Quantum safety is best thought of as an ongoing transformation—one that touches the broader organization.

One useful tactic that focuses on developing internal talent and thinking outside the box: a quantum-safe transformation team can come from experts across the organization. These in-house resources are tasked with keeping on top of remediation efforts associated with quantum-safe cryptography, in particular establishing priorities, identifying issues, and troubleshooting operational constraints. This team should have visibility—and develop expertise—across the entire quantum-safe transformation effort.[14]

Because cryptographic discovery activities are comprehensive and ongoing, and because crypto-agility must be practiced before it is perfected, quantum safety is best thought of as an ongoing transformation—one that touches the broader organization. This requires not only thinking about cryptography and data encryption in a new light, but also how we can use them more effectively. This starts with awareness and is reinforced through behaviors and executive decisions. Over time, the principles of quantum safety become part of the organization's sense of identity and sense of purpose. This is also an opportunity for organizations to modernize cryptographic implementations and establish cryptographic governance as a valuable practice going forward.

What makes transformation possible is investing in capabilities and the skills required to capitalize on them. Quantum safety must be more than a CISO-driven initiative. It's an ambitious call to action shaped by leaders across the organization and partners outside the organization (see case study "Post Quantum Telco Network"). This includes vendors, industry peers, customers, consumers, and quantum-safe consortia, as well as standards bodies such as the US-based National Institute of Standards and Technology (NIST).[15]

Case study

Quantum-Safe Singapore—The National Quantum-Safe Network Plus (NQSN+)[16]

In 2022, Singapore launched the National Quantum-Safe Network Plus (NQSN+), an initiative with the goal of implementing quantum-safe communications across Singapore. This builds on the launch of the National Quantum-Safe Network (NQSN), which was the result of a decade of quantum research from the Centre for Quantum Technologies (CQT), hosted by the National University of Singapore.

NQSN prioritizes collaboration with universities, private companies, and government agencies, and its aim is to establish field-deployed test beds of quantum-safe technologies for trials, evaluation of security systems, and to support adoption. The organization has demonstrated the technical feasibility of deploying quantum-safe technologies, such as Quantum Key Distribution (QKD), to protect against vulnerabilities related to the emergence of cryptographically relevant quantum computers (CRQCs).

NQSN+ is an initiative of the Infocomm Media Development Authority (IMDA) and is contributing to the broader goal of a quantum-safe Singapore. NQSN+ will begin with a minimum of two network operators, each one constructing a nationwide, interoperable quantum-safe network that can serve virtually all businesses.

A key priority is driving international and local standardization of quantum-safe technologies. Along with Japan, Singapore will co-lead the first standardization of the QKD protocol framework at the ITU Telecommunication Standardization Sector (ITU-T). The group has also published the first reference specification to promote the deployment of QKD networks and facilitate adoption of quantum security both nationally and globally.

For Singapore to remain plugged into the global economy, international connectivity is key. Singapore's goal is to integrate NQSN+ with quantum-safe networks in other markets, facilitating the deployment of quantum-safe solutions at a global level.

Case study

The GSMA Post Quantum Telco Network Task Force—Preparing telcos for the quantum era[17]

Every day the world is more connected—and the telecommunications industry plays a vital role as steward for our digital networks. While companies have always worked relentlessly toward network security, new challenges—quantum challenges—are beckoning. A robust research community is exploring how quantum capabilities can be used for societal good.

The GSMA Post Quantum Telco Network Task Force (PQTN TF) was initiated by IBM and Vodafone at the 2022 MWC Las Vegas conference. Its goal? Preparing highly interconnected telecommunications companies for the secure data demands of the quantum era.

The task force now includes more than 55 companies and over 20 major operators. In February 2024, the task force released its *Post Quantum Cryptography – Guidelines for Telecom Use Cases* white paper. This paper provides a set of best practice guidelines that can be used to support the journey to quantum-safe cryptography in the context of the telecom ecosystem.[18]

The call to action is clear. Transitioning to quantum-safe cybersecurity standards and practices is not an overnight process. Indeed, this transition is expected to take several years and will require the management of many complex dependencies across supply chains and processes. Industry cooperation through working groups like the GSMA PQTN TF provide a forum for sharing information and best practices. In fact, a consortium can move its collective industry forward, as well as advance individual ecosystem players. Creating forward-looking quantum-safe transition plans is the key for thriving in the quantum future.

Sujith Surendranathan of Sun Life emphasizes the importance of collaboration in the industry, stating, “Without a doubt, we need our partners on this particular journey.” He adds that collaborating, even with competitors, can help with ideation and solutions that benefit the industry overall.

While he acknowledges that Sun Life predominantly participates in financial services working groups, he recalls the benefits of speaking early on with leaders from the telecom industry. “They were making significant advancements in the quantum readiness space, and some of our first learnings came from them.” In other words, keep an open mind to new approaches and new ways of working.

The call to action is clear. Transitioning to quantum-safe cybersecurity standards and practices is not an overnight process.

Steps to take

1. **Think creatively about talent.** Develop a talent plan that combines the right mix of training internal resources and bringing in external expertise. Embed internal training into the normal ongoing training and talent management curriculum of your organization.

2. **Establish collaboration** with industry peers, ecosystem partners, vendors, and even customers. Leverage industry consortiums and standards bodies; engage in their activities to contribute as well as learn.

3. **Build an internal quantum-safe center of excellence** that learns by executing proof of technologies and proof of concepts. Translate those experiences into best practices for your organization to adopt and follow.

Part three:
Cryptographic resilience
The ultimate goal of quantum safe

If we recognize the importance of data integrity and data security, and we understand the value of secure and trusted data, that's because cryptography is working in the background.

If we see the benefits of crypto-agility, that's because we understand our reliance upon data encryption. These are not just leading practices; they are the basis for greater resilience.

Compared to their least-ready counterparts, Quantum-Safe Champions report they are nearly three times more resilient overall.

Compared to their least-ready counterparts, Quantum-Safe Champions report they are nearly three times more resilient overall. Across multiple factors, QSCs exhibit markedly greater resilience, both in current practices and in anticipated levels of exposure and financial impact from quantum-triggered security threats. For example, QSCs report being five times more resilient in their network infrastructure and over two times more resilient in their data practices, among other metrics (see Figure 4).

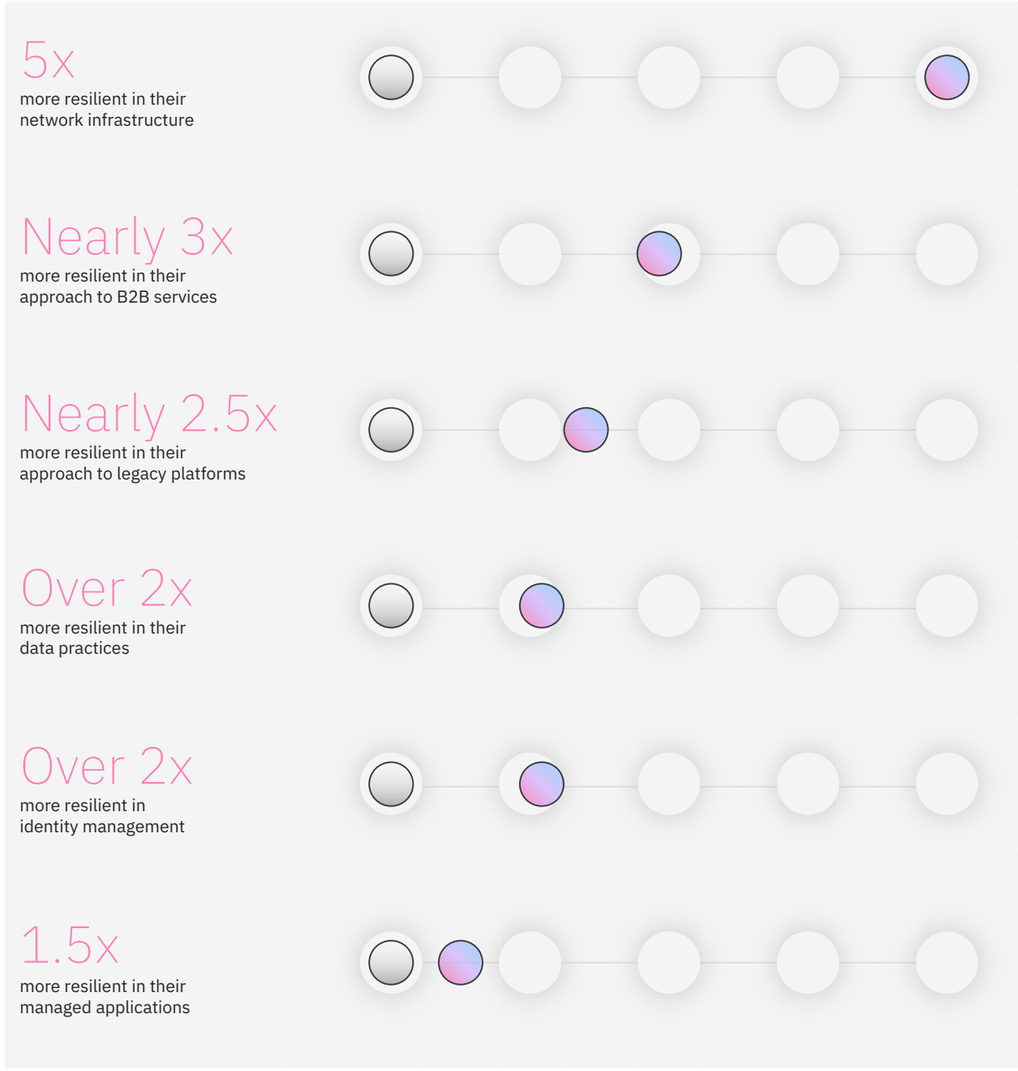
And these changes aren't made in isolation: quantum safety extends to the organization's ecosystem partners. "For example, it's crucial for us to engage with our supply chain to ensure they're quantum safe," notes Paul Ballard at Nationwide. "We need to understand their level of awareness, their plans, and their commitment to quantum safety. We're less concerned about the big players but rather the smaller tier two and three suppliers. Our safety is only as strong as the weakest link in our partnerships, so it's essential that we work together to create a secure landscape for our customers."

"Our safety is only as strong as the weakest link in our partnerships, so it's essential that we work together to create a secure landscape for our customers."

Paul Ballard
Technology Strategy and Enterprise Architecture Director, Nationwide Building Society (UK)

FIGURE 4

QSCs are markedly more resilient than other organizations



QSCs are turning forward thinking into forward positioning. Their greater operational resilience means they are better positioned to address traditional cybersecurity risks. But they are also more attuned to quantum-enabled security risks—for the most part better anticipating exposures and assessing financial impact from a variety of quantum-triggered security risks (see Figure 5). These include:

- **Denial of service (DoS)**, which is defined as an attack that occurs when legitimate users cannot access information systems, devices, or other network resources due to the actions of a cyber threat actor. A DoS doesn't just impact enterprise networks; it impacts all downstream economic activity from partners to individual users. A DoS can be difficult to differentiate from typical network activity—pushing out incident response times and prolonging its economic impact.[19]

  Compared to the least-ready organizations, QSCs report a nearly six times lower likelihood of a DoS. In line with their strong cybersecurity strategy and high levels of resilience, QSCs expect a seven times lower financial impact associated with DoS attacks.

- **Data loss** involves the exposure of proprietary, sensitive, or classified information through data leakage.[20]

  Because QSCs value their organizational data and recognize the risks of data loss more than peers, they are more attuned to data security. While QSCs report an over two times lower likelihood of a data loss from a quantum-triggered security event, they expect a nearly three times lower impact.

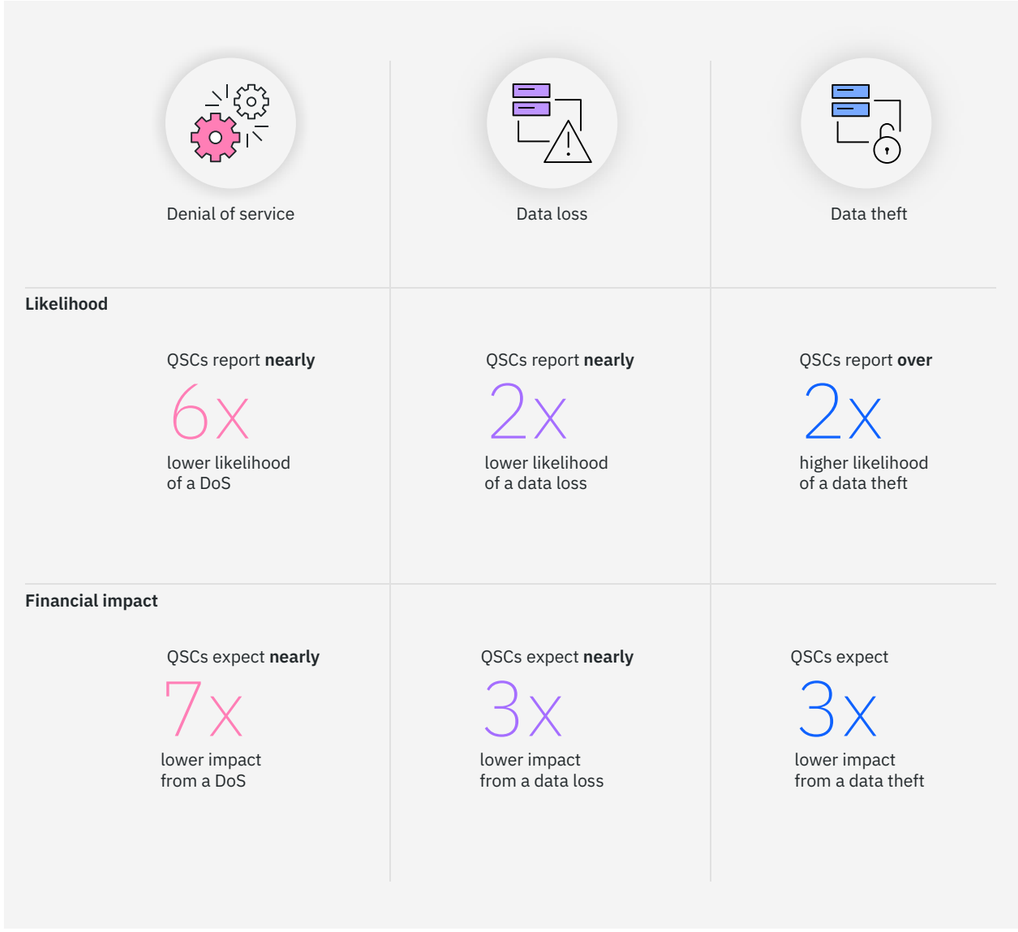
- **Data theft** is the act of illegally stealing digital information from an organization for financial gain or with the intent to sabotage business operations.[21] This is especially true of "harvest now, decrypt later" tactics.

  For QSCs, data security is key to their business strategy—and therefore a source of potential risk. QSCs report over two times higher likelihood of a quantum-triggered data theft for their organizations. But they expect a three times lower financial impact from such a theft. Rather than fret about their risk exposure, QSCs are focusing on action and accountability—shifting quantum safety from a long-term objective into specific investments and new capabilities.

FIGURE 5

QSCs are attuned to traditional and quantum-enabled cybersecurity risks.

Their greater reliance on secure, trusted data drives greater awareness of both the likelihood and financial impact of these security risks.



The metrics speak for themselves. By implementing robust security measures, constantly evaluating the evolving nature of quantum cybersecurity risks, and course-correcting their roadmap as needed, QSCs are well-positioned to navigate any risks posed by the emergence of cryptographically relevant quantum computers.

Perspective

The IBM Quantum-Safe roadmap[22]

Turning quantum-safety into a competitive advantage

As organizations prepare for the quantum era, they also need to know where and how to protect their data and systems from future cryptographically relevant quantum computers. With so much converging at once—new algorithms, standards, best practices, and guidance from government and standards organizations—the IBM Quantum-Safe roadmap (see figure) guides enterprises through the major milestones that can lead to a successful implementation of new quantum-safe cryptographic standards.

✓ First generation available ↻ On target ○ Planned

	2022	2023	2024	2025	2026+
Regulatory milestones	NIST selects algorithms for standardization	Federal agencies plan for PQC adoption	NIST publishes PQC standards	CNSA 2.0: preference to PQC-compliant vendors	Vendors complete transition to PQC
Consortia	✓ Open Quantum Safe (OQS) ✓ Post-Quantum Telco Network	✓ NCCoE ✓ PQC Coalition (MITRE)	✓ Payments (EPAA, NACHA) ✓ PQC Alliance (Linux Foundation)	○ Critical Infrastructure Protection Coalition	
IBM services		✓ Quantum-safe preparation & advisory	↻ Application modernization ↻ Platform modernization	○ Security platform modernization	○ Quantum-safe talent transformation
IBM Quantum-Safe technology	**IBM Quantum Safe Remediator**—*Transform* ✓ Adaptive proxy ↻ TLS, VPN, SSL ✓ Performance benchmarking ↻ Crypto-agility framework ↻ Encryption ↻ Key/certificate management ○ Automated remediation ○ LLM-based recommendation				
	IBM Quantum Safe Advisor—*Observe* ↻ Dynamic scan ↻ Cryptographic inventory ↻ Cryptographic posture mgmt ↻ Risk-based prioritization ↻ Enriched metadata ○ AI-driven risk analysis				
	IBM Quantum Safe Explorer—*Discover* ✓ Static scan ✓ CBOM generation ✓ CI/CD integration ↻ Custom library support ↻ Remediation recommendation ○ LLM-assisted scanning				
Algorithms, protocols, standards, libraries	✓ Key encryption: CRYSTALS-Kyber ✓ Digital signature: CRYSTALS-Dilithium, FALCON	✓ Cryptography Bill of Materials (CBOM)	↻ MAYO, UOV, SQISign ↻ OpenSSL		
IBM infrastructure		✓ IBM z16, IBM Hyper Protect Crypto Services, IBM Tape Storage, Hardware Security Modules (HSM)	↻ IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power		

Steps to take

1 **Conduct a comprehensive discovery of cryptographic usage** across your organization using automated tools. Use this inventory to develop a transformation plan that includes crypto agility as a first-order consideration. Use the risk-based assessment conducted earlier to prioritize the activities in this transformation plan.

2 **Develop a comprehensive set of external dependencies** and a plan to manage them—primarily for the management of participants in the organization's software supply chain.

3 **Develop and operationalize an iterative execution plan** that enables learning and improvement from each cycle. Validate that crypto agility is infused in each iteration.

4 **Set up ongoing governance and management constructs** so that the discovery of cryptography, management of the cryptographic posture, consideration of crypto agility, and so forth are not once-and-done activities but become embedded business-as-usual operational and execution constructs.

About the authors

Ray Harishankar

IBM Fellow
IBM Quantum
linkedin.com/in/rayharishankar/
harishan@us.ibm.com

Dinesh Nagarajan

Executive Partner and Global Portfolio Leader for Identity, Data & Application Security and Cloud Platforms Security and Security for AI
IBM
https://www.linkedin.com/in/dineshnagarajan/
Dinesh.Nagarajan@uk.ibm.com

Dr. Walid Rjaibi

Distinguished Engineer, CTO, Data Security
IBM
linkedin.com/in/walid-rjaibi-phd-cissp-8325077/
wrjaibi@ca.ibm.com

Gerald Parham

Global Research Leader, Security and CIO
IBM Institute for Business Value
linkedin.com/in/gerryparham
gparham@us.ibm.com

Veena Pureswaran

Research Director
IBM Institute for Business Value
https://www.linkedin.com/in/veenapureswaran/
vpures@us.ibm.com

Expert contributors

We would like to thank the following individuals for their contributions and insights: Sara Aboulhosn, Jai Arun, Jennifer Janecheck, Priya Kurien, Hebatallah Nashaat, Chris Nay, Rob Parsons (Nationwide Building Society [UK]), Lily Patel, Antti Ropponen, Yolanda Sanz (GSMA), Lucy Sieger, and Lory Thorpe.

Study approach and methodology

In conjunction with Oxford Economics, the IBM Institute for Business Value interviewed 565 executives, including CXOs, with primary responsibility for their organization's technology and innovation strategy. Of these, over 100 executives had primary responsibility for their organization's quantum strategy.

Respondents came from 15 countries that are globally inclusive and regionally representative. Respondents came from 13 industries, all representing organizations with at minimum $250 million in annual revenue.

Our primary research objective was to better understand organizations' current level of quantum-safe readiness. To do so, we assessed their progress on various initiatives and practices associated with quantum safety.

Overall, across all industries and regions, the Quantum-Safe Readiness Index (QSRI) currently indicates low levels of readiness: 21 on a 100-point scale. The QSRI is based on 14 indicators across the categories of discovery, observability, and transformation.

Appendix

In May 2023, the IBM Institute for Business Value (IBV) published *Security in the quantum computing era: The risk is real, the need is now.*

The report covers quantum safety concepts in detail and also provides an action guide, "Gaining quantum-safe momentum," detailing tactical steps that align with recommendations from the Cybersecurity and Infrastructure Security Agency (CISA), a US federal government organization.[23] These recommendations were used to develop the indicators of quantum-safe readiness for the QSRI and can be adapted to address the unique needs of any particular organization. To access the action guide and full report, visit https://ibm.co/quantum-safe-encryption

About GSMA

The GSMA is a global organization unifying the mobile ecosystem to discover, develop, and deliver innovation foundational to positive business environments and societal change. Its vision is to unlock the full power of connectivity so that people, industry, and society thrive. Representing mobile operators and organizations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Industry Services and Solutions, Connectivity for Good, and Outreach.

Related reports

The Quantum Decade

The Quantum Decade: A playbook for achieving awareness, readiness, and advantage. Fourth edition. IBM Institute for Business Value. December 2023. https://ibm.co/quantum-decade

Security in the quantum computing era

Security in the quantum computing era: The risk is real, the need is now. IBM Institute for Business Value. May 2023. https://ibm.co/quantum-safe-encryption

Make quantum readiness real

Make quantum readiness real: Driving business utility with ecosystems, innovation, and talent. IBM Institute for Business Value. December 2023. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-readiness

Notes and sources

1 Based on internal IBM information.

2 “IBM Quantum Computer Demonstrates Next Step Towards Moving Beyond Classical Supercomputing.” IBM Newsroom. June 14, 2023. https://newsroom.ibm.com/2023-06-14-IBM-Quantum-Computer-Demonstrates-Next-Step-Towards-Moving-Beyond-Classical-Supercomputing

3 Letzter, Rafi. “Landmark IBM error correction paper published on the cover of Nature.” IBM Quantum Research Blog. March 27, 2024. https://www.ibm.com/quantum/blog/nature-qldpc-error-correction

4 Montague, Zach. “The Race to Save Our Secrets From the Computers of the Future.” *The New York Times*. https://www.nytimes.com/2023/10/22/us/politics/quantum-computing-encryption.html

5 “How to preserve secrets in a quantum age.” *The Economist*. July 13, 2022. https://www.economist.com/science-and-technology/2022/07/13/how-to-preserve-secrets-in-a-quantum-age

6 Pelley, Scott, Aliza Chasan, Denise Schrier Cetta, and Katie Brennan. “Quantum computers could solve problems in minutes that would take today’s supercomputers millions of years.” CBS News. December 3, 2023. https://www.cbsnews.com/news/quantum-computing-advances-60-minutes/

7 Harishankar, Ray, Dr. Sridhar Muppidi, Michael Osborne, Dr. Walid Rjaibi, and Dr. Joachim Schaefer. *Security in the quantum computing era: The risk is real, the need is now.* May 2023. https://ibm.co/quantum-safe-encryption

8 “Cybersecurity Advisory: Announcing the Commercial National Security Algorithm Suite 2.0.” National Security Agency. Accessed May 2, 2024. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

9 Gillis, Alexander S. “What is crypto-agility?” TechTarget. Accessed April 19, 2024. https://www.techtarget.com/searchenterpriseai/definition/crypto-agility

10 “Commission publishes Recommendation on Post-Quantum Cryptography.” European Commission. Press release. April 11, 2024. https://digital-strategy.ec.europa.eu/en/news/commission-publishes-recommendation-post-quantum-cryptography

11 “Introduction to Quantum-safe Cryptography in TLS.” IBM Cloud. February 23, 2024. https://cloud.ibm.com/docs/key-protect?topic=key-protect-quantum-safe-cryptography-tls-introduction

12 *Cost of a Data Breach Report 2023*. IBM Security. Accessed April 19, 2024. https://www.ibm.com/reports/data-breach

13 Based on internal IBM information.

14 Harishankar, Ray, Dr. Sridhar Muppidi, Michael Osborne, Dr. Walid Rjaibi, and Dr. Joachim Schaefer. *Security in the quantum computing era: The risk is real, the need is now.* May 2023. https://ibm.co/quantum-safe-encryption

15 Ibid.

16 “Singapore launches Southeast Asia’s first quantum-safe network infrastructure to help businesses tap on quantum-safe technologies.” Infocomm Media Development Authority (IMDA). June 6, 2023. https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/sg-launches-southeast-asias-first-quantum-safe-network-infrastructure

17 Sanz, Yolanda. “Readying the mobile industry for a post-quantum future.” GSMA Newsroom. September 27, 2023. https://www.gsma.com/newsroom/article/readying-the-mobile-industry-for-a-post-quantum-future/

18 *Post Quantum Cryptography – Guidelines for Telecom Use*. GSMA. February 22, 2024. https://www.gsma.com/newsroom/gsma_resources/pq-03-post-quantum-cryptography-guidelines-for-telecom-use-cases/

19 “Understanding Denial-of-Service Attacks.” Blog. Cybersecurity & Infrastructure Security Agency. February 1, 2021. https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

20 “Data loss.” NIST Computer Security Resource Center. Accessed April 19, 2024. https://csrc.nist.gov/glossary/term/data_loss

21 “What is data theft?” DataSecurity Plus. Accessed April 19, 2024. https://www.manageengine.com/data-security/what-is/data-theft.html

22 “IBM Quantum Safe Roadmap.” IBM. Accessed May 1, 2024. https://www.ibm.com/quantum/assets/quantum-safe/IBM_Quantum_Safe_Roadmap.pdf

23 “Prepare for a New Cryptographic Standard to Protect Against Future Quantum-Based Threats.” Cybersecurity & Infrastructure Security Agency (US). July 5, 2022. https://www.cisa.gov/news-events/ alerts/2022/07/05/prepare-new-cryptographic-standardprotect-against-future-quantum-based-threats

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | May 2024

This document is printed on chlorine-free 100% post-consumer paper meeting Forest Stewardship Council (FSC) responsible forestry certification. The energy used to manufacture this paper was generated through renewable green energy. Please recycle.

ibm.co/quantum-safe

IBM