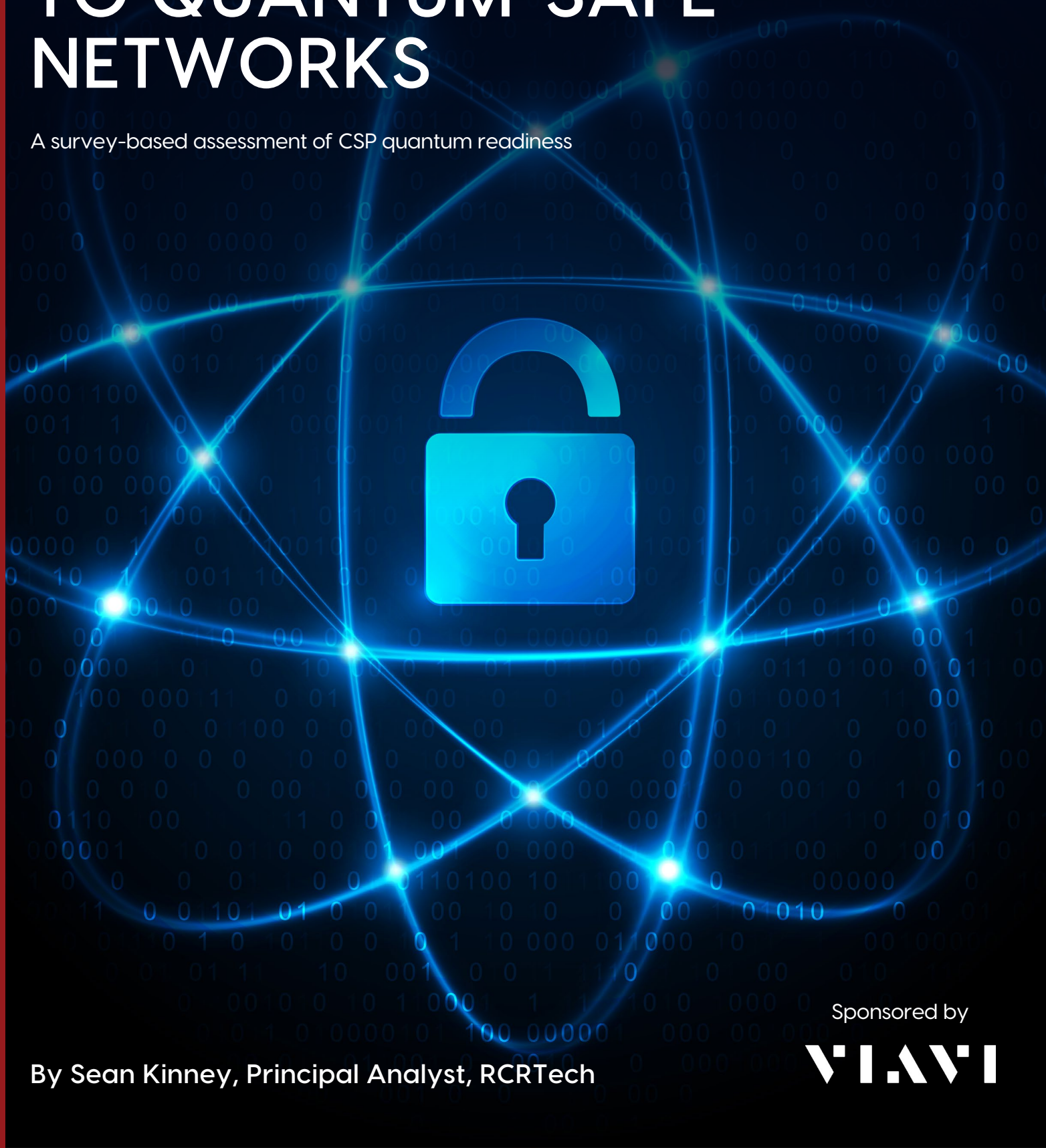
RCR Tech
NEWS. INSIGHT. IMPACT.

PREPARING FOR Q-DAY AND THE PATH TO QUANTUM-SAFE NETWORKS

A survey-based assessment of CSP quantum readiness



By Sean Kinney, Principal Analyst, RCRTech

Sponsored by

VIAVI

TO THE READERS:

Advances in quantum computing, coupled with the rise of "harvest now, decrypt later" strategies among cybercriminals, are heightening the urgency to safeguard data and networks. This has been underscored by several recent high-profile breaches, including in October 2025, when it was revealed that "vast amounts" of classified UK government data had been taken in a state attack. In addition, various healthcare data breaches affected more than 20 million people in the United States in 2025. The theoretical risks are beginning to feel significantly more tangible.

We enter 2026 with grounds for optimism: three post-quantum cryptography (PQC) algorithms have been standardized, major browsers and operating systems have enabled post-quantum key agreements by default, quantum key distribution (QKD) techniques and rollouts are advancing to secure the physical layer, and government mandates are in place to enforce these in critical applications.

VIAVI believes that test and measurement can be used to ensure the effectiveness of both PQC and QKD (and hybrid) security approaches as well as validating key management system (KMS) interoperability. To that end, we offer security frameworks and validation tools, including digital-twin networks, fiber monitoring, and fiber sensing that enable organizations to move quantum algorithms and architectures from theoretical models and lab environments into secure, real-world deployments.

So where does the service provider industry stand? VIAVI partnered with RCR Tech for this industry survey that assesses how service providers are preparing for quantum-era security risks. Participants provided insight into their organizations' current levels of quantum awareness, perceived risk, strategic posture, investment outlook and barriers to adoption.

We appreciate the respondents to this survey as well as the partnership with RCRTech and hope that you find it insightful and informative in your own journey toward the Q-Day milestone.

Dr. Sameh Yamany
Chief Technology Officer
VIAVI Solutions

CONTENTS

INTRODUCTION: QUANTUM RISK HAS ENTERED THE PLANNING HORIZON

Quantum computing is moving from theoretical promise to practical reality, and that shift has major implications for digital security. For communications service providers (CSPs), the concern isn't just about what's possible right now, but what will be possible soon. Quantum computers use fundamentally different principles than classical machines, enabling them to solve certain mathematical problems dramatically faster. That includes problems at the heart of the encryption methods we rely on every day, such as RSA and elliptic-curve cryptography (ECC). When these systems can be broken, the foundation of secure network authentication mechanisms, data protection and identity management begins to erode.

This future point in time, often referred to as Q-Day, represents the point when quantum computers can realistically crack these current encryption standards. While that day hasn't arrived yet, it is no longer a theoretical milestone. Advances in quantum hardware, error correction and algorithm development are steadily narrowing the gap between laboratory systems and machines capable of practical cryptographic impact. As a result, Q-Day is moving into CSPs' planning horizons.

Across the telecom ecosystem, work is already underway to prepare for the transition to quantum-safe security. For CSPs, planning ahead is essential because the implications of Q-Day are far-reaching and systemic. Every SIM card, authentication server and encrypted connection depends on cryptographic algorithms to verify identity, protect subscriber data and secure communication between network components. If those algorithms are compromised, attackers could impersonate legitimate users, intercept or alter data, and disrupt the integrity of national and global communications infrastructure.

The risk extends well beyond consumer communications too, affecting enterprises, IoT deployments and government systems that rely on the same cryptographic foundations. Compounding the challenge is the longevity of telecom data. Encrypted traffic, credentials and metadata captured today may retain value for years, creating exposure even before quantum computers are capable of breaking encryption in real time.

Given the potential long-term impact, quantum risk is emerging today as a concrete security and planning consideration for CSPs. This raises a fundamental question: how prepared are they for Q-Day?

SURVEY OVERVIEW: MEASURING QUANTUM-READINESS SIGNALS

To assess how CSPs are preparing for quantum-era security risks, RCRTech partnered with VIAVI Solutions to survey our global audience of experienced CSP leaders and practitioners. More than 100 respondents participated, providing insight into their organizations' current levels of quantum awareness, perceived risk, strategic posture, investment outlook and barriers to adoption.

The survey was designed to measure directional readiness and capture how CSPs are thinking about quantum risk today — what they understand, what concerns them and where progress is already underway or stalled. In a market where quantum-safe networking remains an emerging discipline, these signals are often more revealing than hard deployment statistics.

As the results show, quantum security is no longer viewed as a distant or academic concern. Awareness is growing, concern about future exposure is widespread and interest in quantum-safe technologies is taking shape. At the same time, readiness remains uneven. Many organizations are still in early research phases, and confidence about long-term preparedness varies considerably.

The following chapters examine the survey findings in detail, pairing respondent feedback with technical and operational context. Together, the results help illuminate where CSPs stand today on the path toward quantum-safe networks, and where the most significant gaps between awareness, intent and execution remain.

AWARENESS OF Q-DAY IS HIGH, BUT NOT UNIVERSAL

Before examining the strategies CSPs are beginning to explore to mitigate the potential impacts of Q-Day, it is important to establish a baseline of awareness. While awareness does not equate to readiness, it does signal how seriously decision makers across the industry are treating the quantum threat.

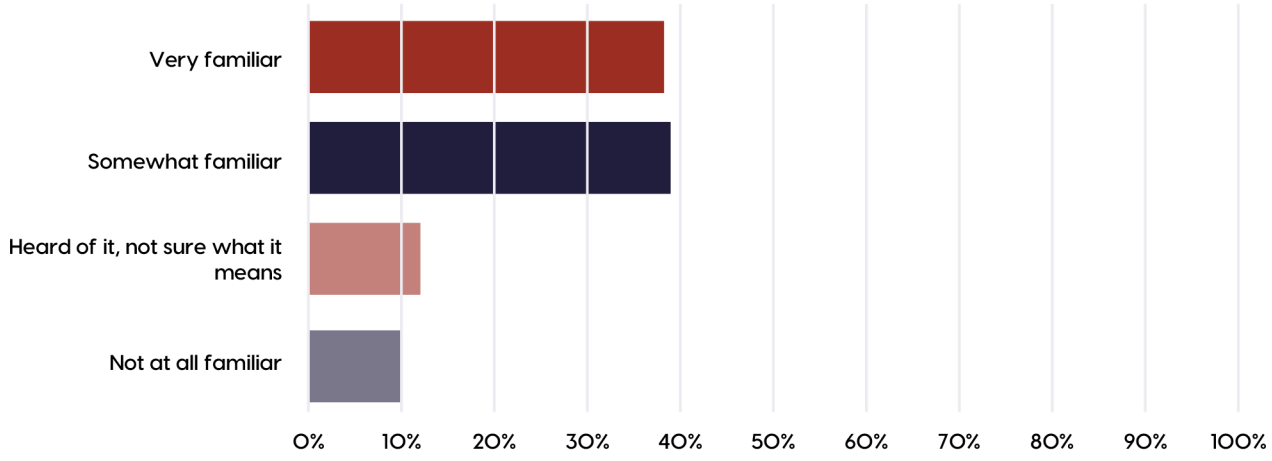
Survey results indicate that quantum risk has entered the mainstream consciousness of the telecom industry. A clear majority of respondents, 77%, say they are either "very familiar" or "somewhat familiar" with Q-Day, the point at which quantum computers become capable of breaking today's widely used public-key encryption. This level of familiarity suggests that quantum security is no longer confined to research teams or standards discussions.

However, the results also reveal important gaps. Nearly one-quarter of respondents report that they are unclear about the meaning of Q-Day or not familiar with the concept at all. In cryptography, partial understanding can be especially problematic. Large-scale networks depend on consistent assumptions about trust, identity and key management, and security architectures often fail at their weakest or least-updated points.

This uneven awareness helps explain why quantum-safe readiness across the industry remains limited. For many CSPs, Q-Day is still viewed as a long-term or future-facing issue, rather than a factor shaping current security planning. Awareness has increased, but it has not yet fully translated into urgency.

That distinction becomes more apparent when examining how CSPs assess the near-term risk of "harvest now, decrypt later" attacks wherein future quantum capabilities turn today's encrypted traffic into a lasting liability.

How familiar are you with the concept of Q-Day (when quantum computers will be able to break today's public-key encryption)?



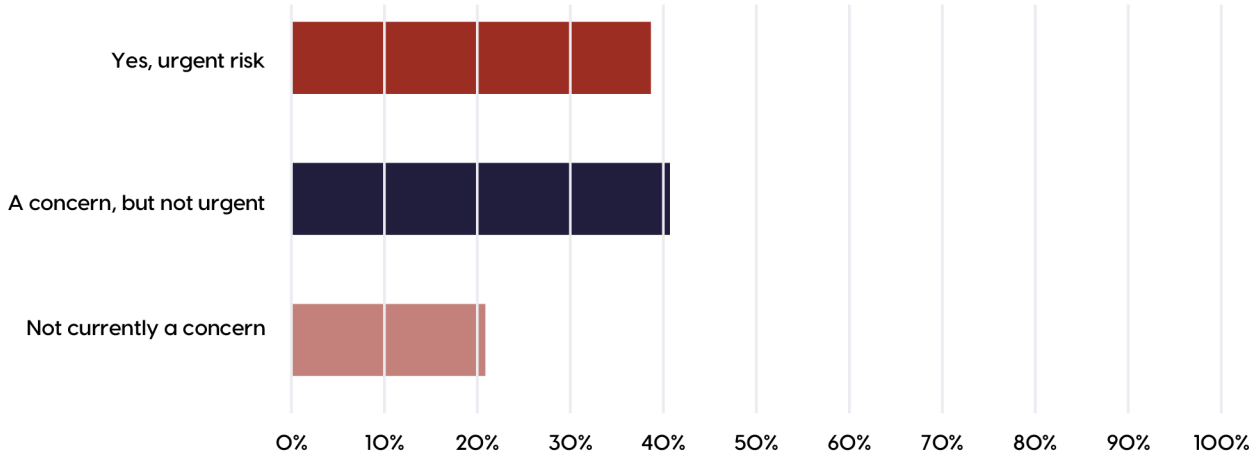
HARVEST NOW, DECRYPT LATER IS A FUTURE THREAT TAKING SHAPE TODAY

CSPs are a prime target for cyber adversaries, given the volume, sensitivity and contextual richness of the data they handle in the course of facilitating global communications. Subscriber credentials, signaling data, enterprise traffic, IoT communications and metadata all traverse CSP networks at scale. Today, those assets are already exposed to a wide range of threats from supply-chain compromises and edge-device exploitation to SIM swapping and credential theft. CSPs therefore operate in a complex and persistent cybersecurity environment even before quantum computing enters the picture.

Quantum computing does not replace these existing threats, but it fundamentally changes their time horizon. The most immediate quantum-related risk is known as "harvest now, decrypt later" (HNDL). Under this model, adversaries intercept and store encrypted data today with the expectation that it can be decrypted in the future once sufficiently powerful quantum systems become available. The attack depends on patience rather than on breaking encryption in real time.

For CSPs, this dynamic is particularly concerning because telecom data often has a long useful life. Encrypted traffic, authentication material, signaling

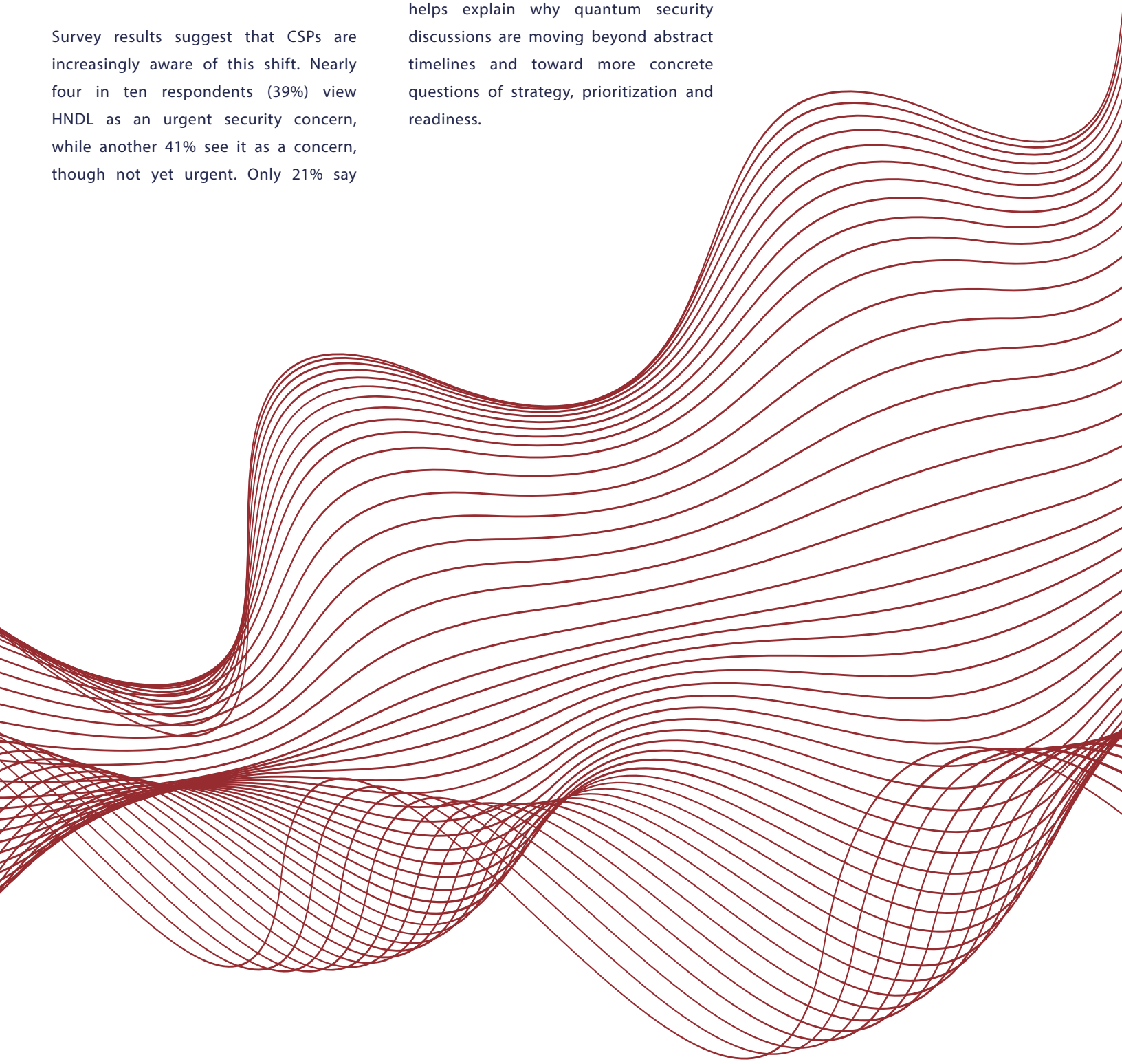
Do you consider "harvest now, decrypt later" (HNDL) a near-term security risk for your organization?



records and metadata may be retained for years due to regulatory, operational or analytical requirements. Even if current cryptography remains secure in the near term, data collected today can become a durable liability if exposed later. In effect, quantum computing turns time itself into an attack vector.

Survey results suggest that CSPs are increasingly aware of this shift. Nearly four in ten respondents (39%) view HNDL as an urgent security concern, while another 41% see it as a concern, though not yet urgent. Only 21% say HNDL is not currently a concern. Taken together, these responses indicate broad recognition that quantum risk is not confined to a distant future state, but has implications for how data is protected and classified today.

This growing concern around HNDL helps explain why quantum security discussions are moving beyond abstract timelines and toward more concrete questions of strategy, prioritization and readiness.



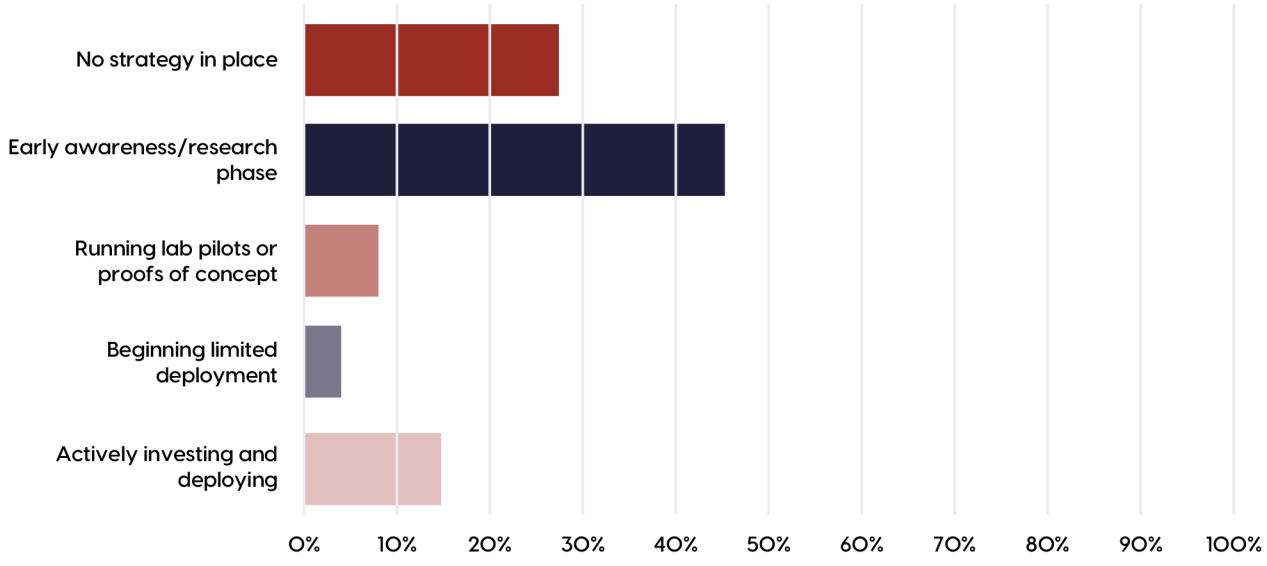
A STRATEGIC REALITY CHECK ON WHERE CSPS STAND TODAY

Awareness of quantum risk and concern about HNDL attacks do not automatically translate into action. To understand how CSPs are responding in practical terms, the survey examined the current state of quantum-safe security strategies across organizations. The results point to an industry that is engaged, but still early in its transition.

Just over one-quarter of respondents (26%) report that they have no formal quantum-safe security strategy in place today. This reflects the reality that quantum risk is still emerging relative to other, more immediate security and network priorities. The largest share of respondents, approximately 46%, say their organizations are in an early awareness or research phase. This posture suggests a deliberate approach to monitoring technology maturity, waiting for clearer guidance from standards bodies and assessing how quantum-safe mechanisms would integrate into existing network architectures.

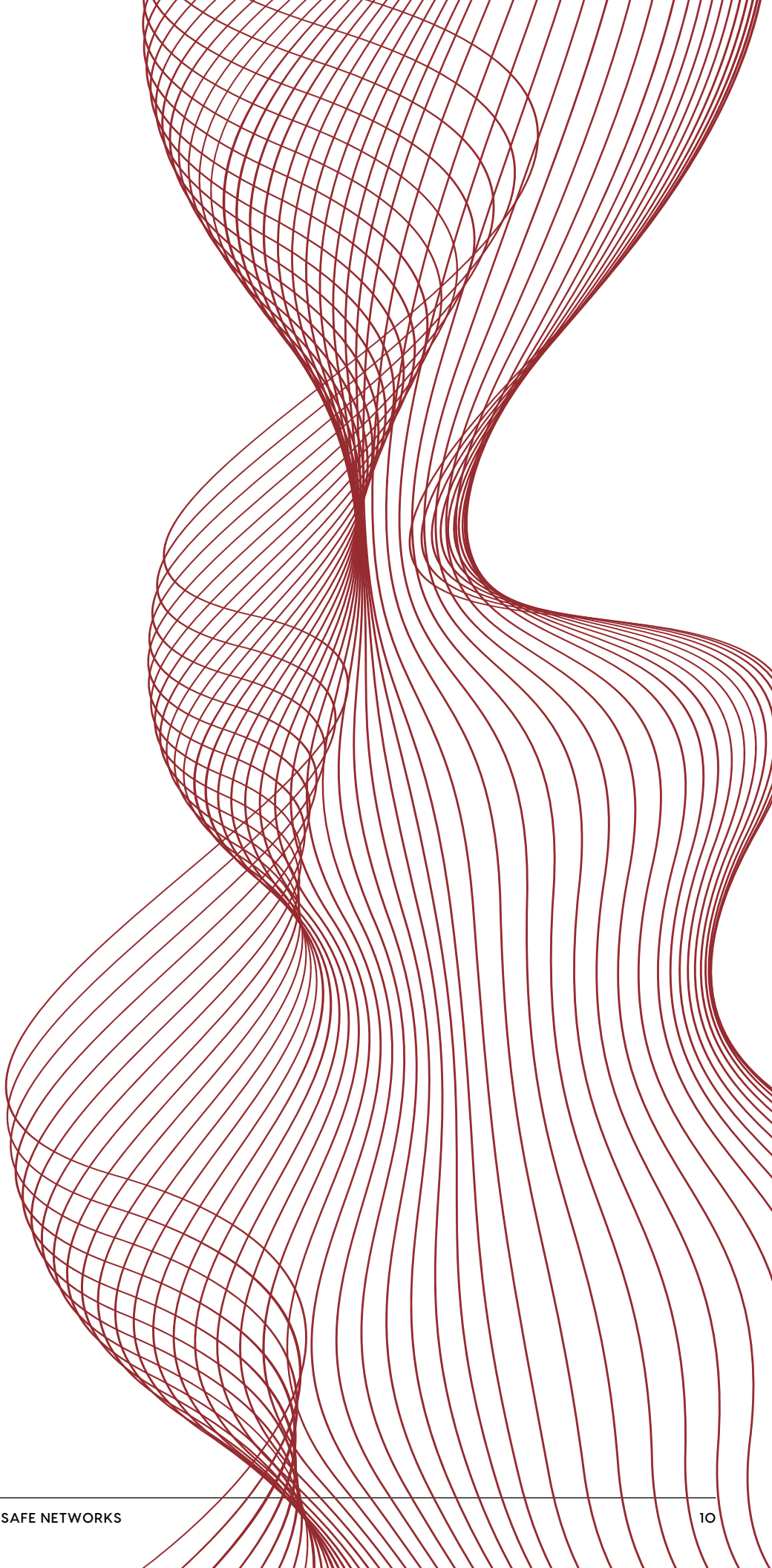
At the more advanced end of the spectrum, roughly 28% of respondents

Which best describes your organization's quantum-safe security strategy today?



indicate that their organizations are running lab pilots or proofs of concept, beginning limited deployments or actively investing in quantum-safe solutions. While still a minority, this cohort represents an important leading edge. Singtel, for instance, announced in October 2025 the launch of a "hybrid quantum-safe networks" program that integrates Quantum Key Distribution (QKD) with Post-Quantum Cryptography (PQC). The company said this approach "extends protection beyond core data centers and mission-critical sites to branch offices, remote facilities, cloud environments and overseas operations…This layered approach delivers cost-efficient, flexible and globally extensible protection against emerging quantum threats."

Most CSPs acknowledge the need to prepare for a quantum-secure future, but only a subset have begun converting that recognition into concrete action. This gap between awareness and execution underscores the central challenge of quantum readiness — aligning mitigation of long-term risk with near-term financial and operational realities.

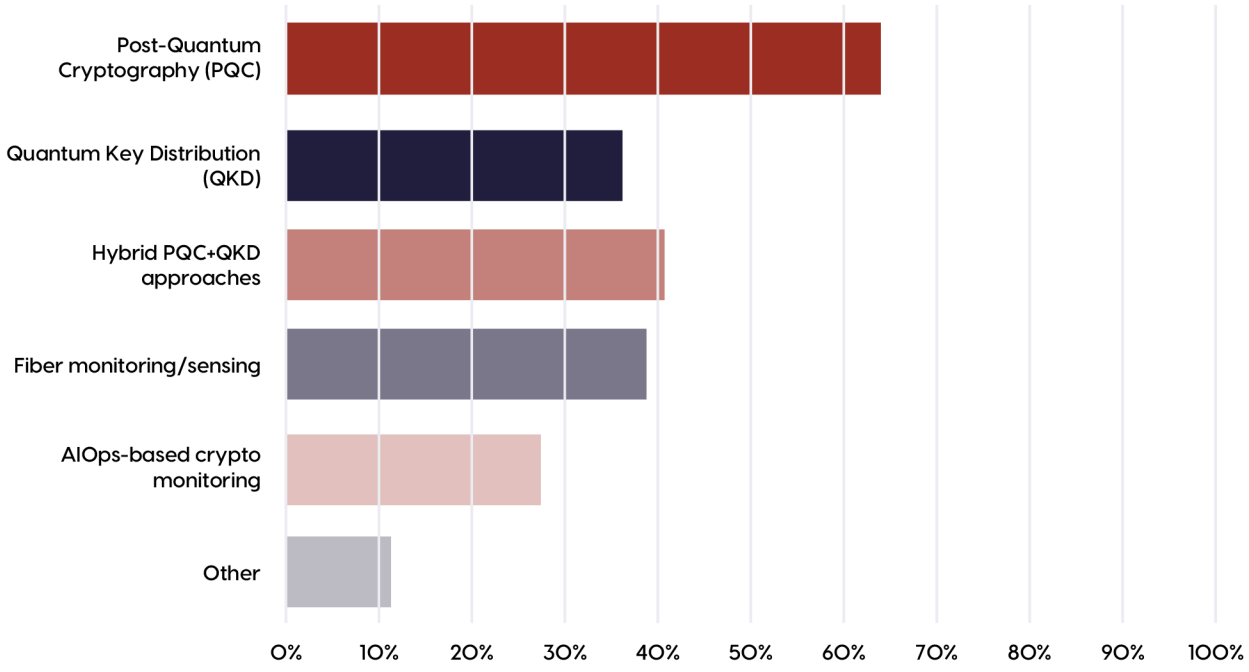


TECHNOLOGY PRIORITIES – PQC LEADS WHILE HYBRID EMERGES

Survey results show that CSPs are beginning to translate abstract quantum risk into tangible technology strategy development. When asked which technologies they are most likely to prioritize for quantum-safe security, PQC clearly emerged as the default path forward. Nearly two-thirds of respondents (around 64%) identified PQC as a priority, reflecting its ability to be deployed largely through software updates and integrated into existing protocols, devices and network functions.

This preference aligns closely with industry momentum. PQC algorithms standardized by NIST are designed to replace vulnerable public-key schemes such as RSA and ECC while preserving existing trust models. For CSPs managing vast, heterogeneous networks, PQC offers a scalable way to address quantum risk without requiring fundamental changes to physical infrastructure. It

Which technologies are you most likely to prioritize for quantum-safe security?

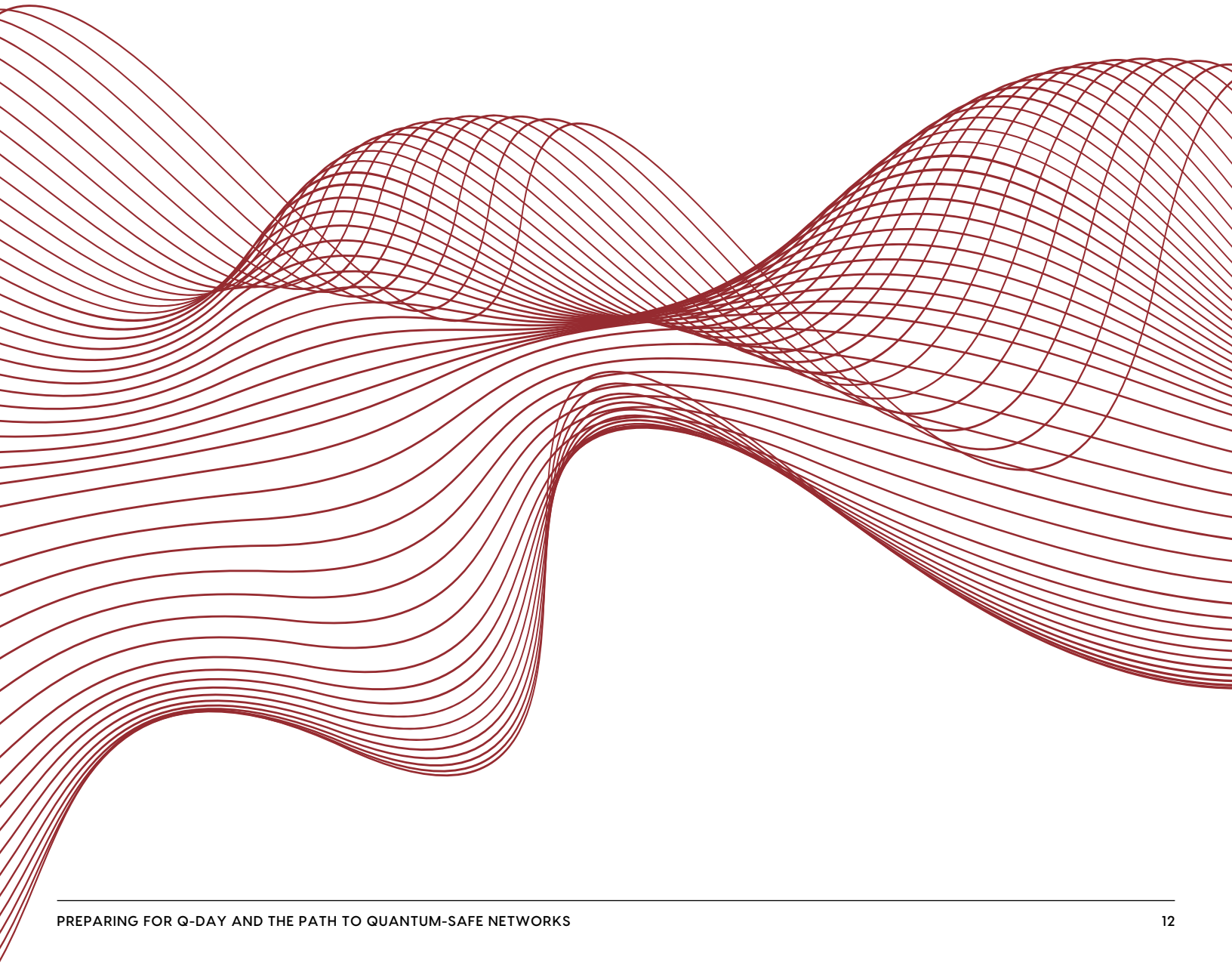


also fits naturally with ongoing work in 3GPP, where post-quantum mechanisms are being studied for future security frameworks.

At the same time, interest in QKD remains significant, with roughly 37% of respondents selecting it as a priority. QKD's appeal lies in its physics-based security guarantees, which make it attractive for protecting the most sensitive links, such as inter-data center connections or critical control paths. However, its reliance on specialized optical infrastructure and tight operational constraints means it is generally viewed as a targeted, high-assurance solution rather than a universal replacement for classical cryptography.

Notably, more than 40% of respondents expressed interest in hybrid PQC/QKD approaches — an approach early adopters like Singtel are using. Rather than viewing PQC and QKD as competing alternatives, many CSPs are exploring layered architectures that combine PQC's scalability with QKD's highest-assurance key exchange. Standards efforts across ETSI, ITU-T and the GSMA are helping define how these technologies can coexist within coherent security frameworks.

Respondents also highlighted the importance of fiber monitoring and sensing (39%) and AIOps-based crypto monitoring (27%). These complementary priorities suggest understanding that quantum-safe security will result from hardware- and software-based approaches that span the physical and operational layers of the network.



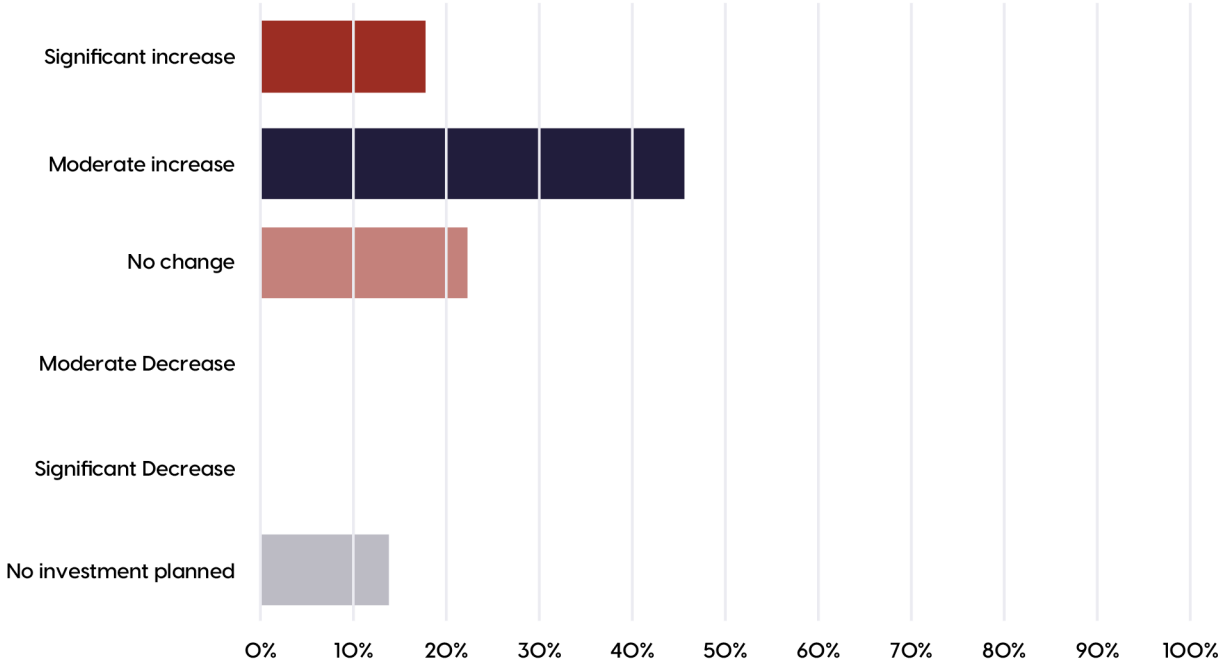
INVESTMENT OUTLOOK – MOMENTUM AND HESITATION

With the importance of quantum-safe networks widely recognized and technology preferences beginning to take shape, survey respondents also provided insight into how CSPs expect their investment levels to evolve. Nearly two-thirds of respondents (64%) say they anticipate a moderate or significant increase in spending on quantum-safe solutions over the next two to three years, indicating growing momentum and a shift toward actionable planning.

At the same time, the data reflects a measured approach rather than a rush to deploy. Twenty-two percent of respondents expect no change in investment levels, suggesting that existing security budgets or pilot programs are viewed as sufficient in the near term. Another 14% report no investment planned through the 2027–2028 timeframe, underscoring that quantum-safe initiatives must still compete with other priorities, including 5G expansion, cloud transformation and AI-driven network automation.

In sum, CSPs are beginning to allocate resources for quantum readiness, but most are pacing investment in line with standards maturity, operational clarity and clearer business justification.

How do you expect your organization's investment in quantum-safe solutions to change over the next 2–3 years?



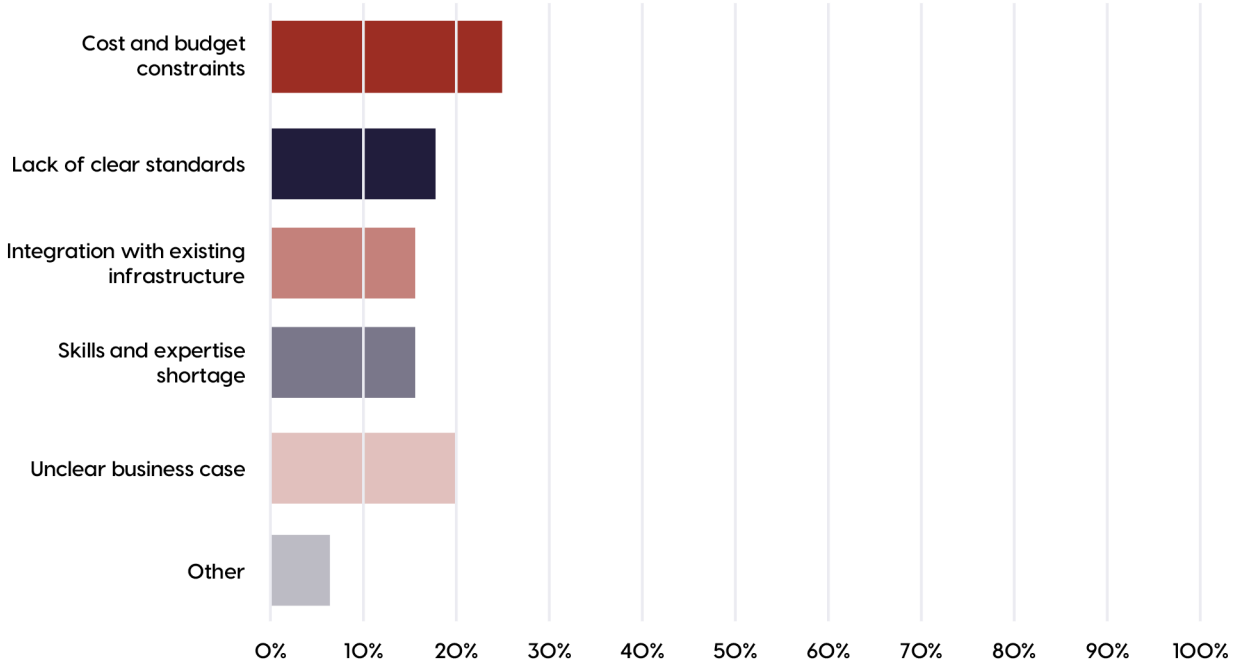
THE BARRIERS TO QUANTUM-SAFE ADOPTION

When asked to identify the biggest obstacles to adopting quantum-safe security, survey respondents point first to cost and budget constraints (about 25%). On its own, that result is unsurprising given that budget pressure is a constant for CSPs. More telling, however, is that in this context cost constraints also reflect uncertainty around timing, return on investment and when quantum risk must be addressed relative to other priorities.

That uncertainty shows up clearly in the next tier of responses. Roughly one-fifth of respondents cite an unclear business case, while 18% point to standards uncertainty. These concerns are closely linked. CSPs are reluctant to commit to large-scale deployments while specifications continue to evolve across bodies such as NIST, 3GPP and the GSMA. Operational factors also play a meaningful role. About 15% of respondents cite integration challenges, and a similar share point to skills and expertise shortages. These barriers echo challenges CSPs are already encountering with AI adoption.

Taken together, the results suggest that the primary blockers to quantum-safe adoption are not solely technological, but organizational. This is where testing, validation and crypto agility become critical. By validating performance, interoperability and upgrade paths in realistic environments, CSPs can reduce uncertainty, strengthen the business case and begin converting long-term quantum risk into actionable, near-term decisions.

What is the biggest barrier to quantum-safe adoption in your organization?



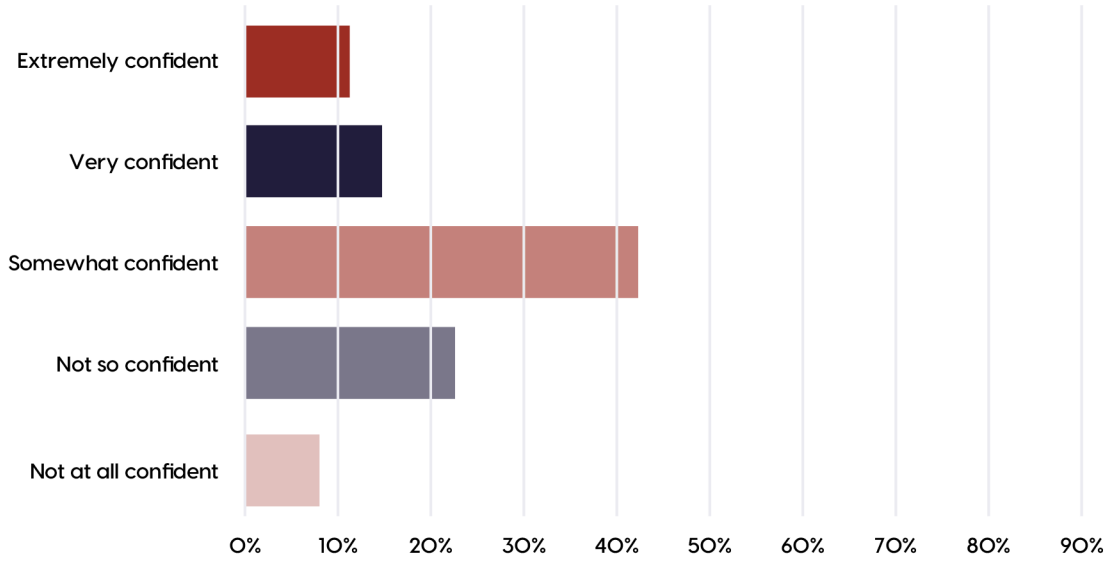
HORIZON 2030 – CAUTION RATHER THAN CERTAINTY

When asked how confident they are that their organizations will be quantum-safe by 2030, survey respondents expressed caution more so than conviction. About 26% say they are very or extremely confident, while the largest share (42%) report being somewhat confident. At the other end of the spectrum, nearly one-third of respondents (31%) say they are "not so confident" or "not at all confident" that their organizations will be prepared by the end of the decade.

These results are best understood as a reflection of the sheer systemic complexity involved in navigating the path to quantum-safe. This is a situation where the path doesn't necessarily lead to a single destination. Becoming "quantum-safe" is a layered transition that touches cryptography, key management, devices, transport and operational processes across long-lived, multi-vendor networks. Confidence here is also a reflection of a strong standards foundation, at least optics into a positive business case and the assumption that the relevant skillsets can be acquired or developed.

It's also important to note that uncertainty at this stage is entirely rational. The takeaway from responses to this particular survey question is that CSPs believe substantial progress is possible while they execute on other transformation activities. Bridging this confidence gap will depend on proving that quantum-safe technologies can be integrated, operated and evolved reliably at network scale.

How confident are you that your organization will be quantum-safe by 2030?



CONCLUSION: ON THE PATH TO QUANTUM-SAFE, VALIDATION IS THE DECISIVE STEP

Across the survey results and broader industry discussion, the macro conclusion is that quantum-safe networking is not a single technology choice but the ability to operate new security mechanisms with confidence at scale. In that sense, testing and validation represent the link between awareness and assurance.

Quantum-safe technologies introduce new variables into already complex networks. QKD must be validated at the optical layer to ensure stable key generation under real-world conditions. PQC requires benchmarking to understand performance impacts, interoperability across vendors and upgrade paths over long equipment lifecycles. Hybrid architectures add further complexity, demanding rigorous testing of key management, failover behavior and crypto agility. Digital twins and neutral, multi-vendor test environments play a critical role in making these challenges manageable before changes touch live networks.

This emphasis on validation directly addresses the barriers surfaced in the survey. It helps clarify the business case, builds confidence as standards mature and reduces integration risk by exposing issues early. Most importantly, it shifts quantum readiness from abstract planning to operational reality.

ACKNOWLEDGEMENTS

VIAVI

Our test, monitoring, assurance, and resilient position, navigation and timing solutions enable and secure critical infrastructure ranging from data center ecosystems and communication networks to military, aerospace, railway and first responder communications. In addition, we develop and advance technologies used in high-volume optical applications across anti-counterfeiting, consumer electronics, aerospace, industrial and automotive end markets.

From testing, assuring, and securing the largest communications networks around the globe, to the coatings and filters that make your car's spatial sensing possible, our technologies have a diverse impact on the world. Discover how we enable new possibilities that touch every area of life.

Learn more

RCR Tech
NEWS. INSIGHT. IMPACT.

Preparing for Q-Day and the path to quantum-safe networks

A survey-based assessment of CSP quantum readiness

By Sean Kinney, Principal Analyst, RCRTech