Omdia
by informa techtarget

Quantum-Safe Networks

Omdia Interviews and Analysis

Authors: Sterling Perrin and Jim Hodges

February 2026

This Omdia White Paper was commissioned by Nokia.

Contents

This Omdia White Paper was commissioned by Nokia.

Executive summary

Always a top concern among service providers, network security is driving a new level of angst as they prepare for the elusive “Q-Day”—the moment when quantum computers become powerful enough to break today’s encryption algorithms. The timing of Q-Day is a matter of debate in academia and industry. Well in advance of Q-Day itself, “quantum safe” is becoming an emerging requirement among leading-edge users such as governments and financial institutions.

Cryptographically-relevant quantum computers (CRQCs) will have enough quantum computing power to quickly crack traditional systems that rely on problem-solving techniques such as integer factorization and discrete logarithm problems, including Rivest–Shamir–Adleman (RSA), elliptic curve cryptography (ECC), and Diffie-Hellman. New approaches to securing trust and the transmission of extremely sensitive data are needed, including the advent of artificial intelligence (AI) and machine learning (ML) data used for training large language models (LLMs) on GPUs in data centers.

Some techniques rely on well-known key distribution methods to deliver encryption keys to their endpoints, such as pre-shared symmetric key distribution, known as symmetric key infrastructure (SKI). Others include using different types of key sources, like the unique properties of quantum physics, called quantum key distribution (QKD). Some utilize new cryptographic algorithms purpose-built to be secure against potential threats posed by quantum computers. Dubbed post-quantum cryptography (PQC), this technique is used within existing public-key infrastructure (PKI). In all cases, transport networks play a crucial role in ensuring that in-flight data is secure from future quantum attacks.

This Omdia White Paper was commissioned by Nokia.

To better understand market expectations and plans for quantum-safe networks (QSNs), Nokia partnered with Omdia to complete a custom, interview-based study. Specifically, we conducted seven in-depth, one-to-one interviews with a global mix of service providers active in QSN. (See the ***Methodology*** section for more details.)

The topics covered in this report include the following:

- Strategic positioning and market drivers
- Technology and infrastructure readiness
- Risk management and resilience
- Customer readiness
- Offerings and business models
- Ecosystem engagement and collaboration

Key findings

The key findings of this report are as follows.

Strategic positioning and market drivers

- **The terms that best describe the current status of QSNs among interviewees are "exploration" and "planning."** It is early days, even among early adopters represented in this study.
- **Interviewees observed that building a quantum-safe infrastructure is a complex undertaking that will take many years, and they believe they need to remain ahead of the curve to be ready when customer demand accelerates.** The "harvest now, decrypt later" concept was also raised as a driver, but less frequently than the need to be prepared ahead of customer demand.
- **Companies selling network services in particular view quantum security as a means of differentiation and network monetization in a highly competitive telecommunications market.** Network operators believe that enterprises and governments will pay high premiums for quantum-secure connectivity services and expect the pool of such customers to increase over time. They want to be the trusted network provider to serve these customers.

This Omdia White Paper was commissioned by Nokia.

Customer readiness

- **Interviewees agreed that customers are at the earliest stages of building their quantum-safe strategies, but customer awareness of the threat of quantum computers and interest in identifying solutions have increased sharply over the past couple of years.** As one interviewee stated, "customers are more aware, more interested, and more engaged. They're asking what they need to do to begin their quantum-safe journey."

- **The rise of AI—including anxiety about its possibilities—is contributing to increased customer demand for quantum security.** Customers believe that the combination of advanced AI with the power of quantum computing is increasing the urgency to build QSNs.

- **Government agencies (including military and those responsible for critical infrastructure), utilities, large financial institutions, and private companies responsible for critical infrastructure are the prime early-stage markets for QSNs.** These entities all have a combination of urgent need and the budgets to make investments.

- **In other verticals, companies may recognize the need for quantum security but lack the required budgets to invest.** Healthcare was the most cited in this regard.

Technology and infrastructure readiness

- **One of the biggest areas of debate within service providers and among their customers is whether to build QSNs based on SKI, PQC, QKD, or a hybrid configuration.** While end customers may tend to lean one way or the other, the interviewees generally believe that they will need hybrid strategies that include all quantum security approaches.

- **Crypto agility is clearly important to interviewees in this report.** Agility includes the ability to adopt asymmetric (math) and/or symmetric (entropy) key management when and where needed, but it also includes implementing quantum security across multiple transmission layers, as needed.

This Omdia White Paper was commissioned by Nokia.

Offerings and business models

- **"Exploration" best describes the general status of interviewees and potential end customers today.** Interviewees are largely focusing on:
  - Engaging with potential early adopter customers to understand their priorities and requirements.
  - Understanding budget levels and priorities of potential customers and exploring whether proposed quantum-safe solutions are economically feasible.
  - Spreading greater industry awareness of the need for QSNs.
- **The companies interviewed are also still defining which vertical industries are best suited for QSNs.** After verticals and their requirements are clearly defined, companies can hone their models and specific services to meet those needs and budgets.

Risk management and resilience

- **Crypto agility underpins cyber resilience strategies in three main ways:**
  - The ability to adopt SKI, PQC, and/or QKD when and where needed to address different levels of customers' security requirements.
  - The implementation of quantum-safe cryptography at multiple network layers.
  - The ability to swap in and out different PQC algorithms quickly and at scale to mitigate risks posed by a future crack of any of today's PQC algorithms. Such swapping is only possible in a defense-in-depth solution that offers crypto resiliency.
- **The general consensus was that insurance implications have not been part of QSN discussions to date—either with customers or regarding their internal infrastructure plans.** However, the interviewees found the insurance question intriguing and agreed it is highly relevant, suggesting that insurance risks will likely become more relevant over time as security breaches inevitably continue and QSNs mature.

Ecosystem engagement and collaboration

- **Within the quantum security ecosystem, trusted network vendors will play a crucial role.** The importance of network vendors, not just transport suppliers, as quantum security facilitators and trusted advisors was reinforced repeatedly throughout these interviews.
- **Most emerging quantum security vendors lack the longevity, financial stability, and/or customer relationships required to serve as trusted lead partners.** This situation provides an opening for network vendors in particular to take on a crucial lead partner and facilitator role in quantum security.
- **Based on these interviews, Nokia has several key strengths to position it as a lead partner for quantum security.** These strengths include the following:
  - A long communications heritage and financial stability, including in optical and IP networks.
  - Long-standing relationships with the groups leading quantum security strategy.
  - In-region market knowledge and presence.
  - Deep experience in building QSNs, evidenced through customer engagements and proofs of concept (PoCs).
  - Existing qualified complementary partnerships and proven interoperability with leading quantum security vendors.

Methodology

This analysis is based primarily on data and findings from a set of seven one-to-one interviews of networking companies conducted by Omdia. The seven companies include a combination of communications service providers (CSPs) (a.k.a. telecommunications service providers), research and education networks, and systems integrators.

Interviews were based on a common *Interview Guide* that was jointly developed by Omdia and Nokia. The seven interviews were conducted from November 2025 through January 2026 by Sterling Perrin, a senior principal analyst, and Jim Hodges, a research director, both at Omdia.

Analysis was supplemented by desk research on quantum security conducted by the analysts as well as insights gleaned from ongoing industry discussions on QKD, SKI, PQC, and cybersecurity.

All seven of the companies interviewed agreed to have their names used in the report. The networking companies interviewed for the project are as follows:

- BT (UK)
- Colt Technology Services (UK)
- GRNET (Greece)
- Kyndryl (US)
- Lyntia Networks (Spain)
- ORION (Canada)
- Tier 1 Asia Pacific CSP (anonymous)

Defining quantum-safe networks

In this report, Omdia uses the term “quantum safe” to describe the protection of the digital communication infrastructure—from the application layer down to the physical transport layer—against the threat of cryptographically-relevant quantum computers (CRQCs).

A quantum-safe network (QSN) combines multiple layers of protection within an agile and resilient defense-in-depth architecture to effectively defend against threats from both classical and quantum computers. The QSN should integrate three critical security pillars:

- **Post-quantum cryptography (PQC):** This involves implementing quantum-resistant mathematical algorithms within existing PKI frameworks. PQC is particularly well-adapted for application layer security, where ephemeral connections and frequent “handshakes” are the norm. PQC is also used in the network layer; IP Security (IPSec) is one example. NIST finalized the first set of PQC standards in August 2024, with an additional PQC algorithm approved in 2025, and others to be standardized over time. Although it is US-focused by mandate, NIST is widely recognized and adhered to globally in cybersecurity.
- **Symmetric key infrastructure (SKI):** To provide the best possible risk mitigation and cryptographic resiliency for high speed data transport, this encryption must be combined with a key distribution technique adapted to the specific network layer. SKI provides a different security architecture for the core infrastructure. It uses high entropy, cryptographically-secure keys derived from true random number generators (TRNGs) or quantum random number generators (QRNGs). In a quantum-safe architecture, SKI provides an out-of-band key distribution channel that keeps the key

management plane physically and logically isolated from the encrypted data plane. This isolation means that a compromise confined to the data path does not, by itself, expose keys.

- **Line-rate network encryption:** In high performance environments, the network layer must use recognized quantum-safe symmetric algorithms, such as 256-bit Advanced Encryption Standard using Galois Counter Mode, or Galois Message Authentication Code algorithm (AES-256 GCM or CTR-GMAC), to ensure high assurance confidentiality and integrity. To provide the best possible cryptographic resiliency for high speed data transport, this encryption must be combined with key distribution (asymmetric or symmetric) adapted to the specific network layers, such as PQC, SKI, or QKD.

A QSN complements quantum-safe applications and protects digital communications across some or all networking OSI layers from current and future threats. A quantum-safe defense-in-depth architecture uses a multi-layered security framework based on five essential attributes:

- **Trusted randomness:** Security starts with a trusted source of true randomness, meaning unpredictable numbers generated from physical processes, including classical and quantum phenomena.
- **Proper key length:** Standardizing on 256-bit symmetric keys provides the 2^{256} combinations required to resist both classical and quantum brute-force attacks.
- **Out-of-band (OOB) symmetric key distribution:** Keys are physically and logically separated from the data stream.
- **Strong data encryption:** Securely distributed keys are paired with algorithms like AES-256-GCM or CTR-GMAC for high assurance integrity.
- **Key rotation:** By refreshing the encryption key periodically, it creates the scenario of an ephemeral connection that is harder to tap, basically reducing the surface of attack.

By combining these five attributes, a QSN delivers end-to-end protection with cryptographic agility and resiliency. This approach mitigates the “harvest now, decrypt later” (steal secured information now to decrypt it later when CRQCs become mature) risk while improving performance.

This Omdia White Paper was commissioned by Nokia.

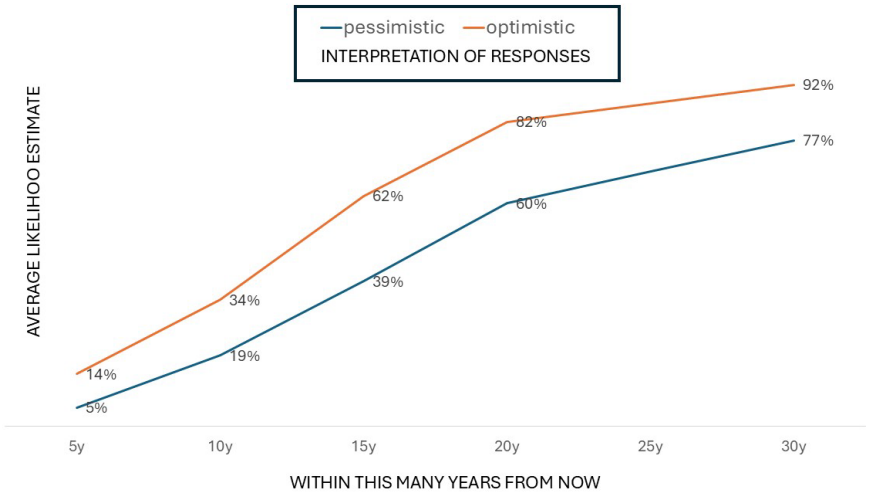
Strategic positioning and market drivers

Service providers interviewed for this report include some of the most progressive network operators developing QSNs, such as BT. However, the terms that best describe the current status of QSNs among interviewees are “exploration” and “planning.” While CRQCs are still projected to be years away, early adopters such as those interviewed for this study are strategically beginning their network planning with QSNs in mind.

Q-Day itself has not yet arrived, and it remains an unknown. The Global Research Institute (GRI) conducts an annual survey of expert leaders in quantum computing research to aggregate their best estimates of when CRQCs may become available. The GRI’s 2024 project surveyed 32 quantum computing experts globally. Among other questions, it asked the experts to assess the likelihood of a quantum computer being able to break RSA-2048 encryption within 24 hours. The upper bound, or “optimistic” or “bullish,” estimate ranges show, on average, a 34% likelihood of such a capable quantum computer within 10 years and 14% likelihood within five years. The lower bound, or “pessimistic,” range gives an average likelihood of 19% over 10 years and 5% within five years (see **Figure 1**).

For certain governments and companies, even the five-year expectations may indicate an intolerable quantum risk.

Figure 1: 2024 Opinion-based estimates of the likelihood of a digital quantum computer able to break RSA-2048 in 24 hours, as a function of time



Note: Range between the average of an optimistic (top value) or pessimistic (bottom value) interpretation of likelihood intervals indicated by respondents.

Source: *Quantum Threat Timeline Report 2024*, Global Risk Institute (GRI), December 2024

Interviewees observed that building a quantum-safe infrastructure is a complex undertaking that will take many years. Network operators need to have their QSNs in place when end customer demand arises, so they must operate a bit ahead of the demand curve.

BT's Senior Research Manager & Fellow, Andrew Lord, made the following statement:

> *Quantum-safe cryptography is about making systems secure for the quantum computing era, especially since the risk is already present. However, implementing these solutions will take years. At BT, we've embarked on a quantum-safe program, but it's a long-term effort. We have thousands of devices that need upgrading. This won't be a trivial task, so we need to act quickly. We also hope to position ourselves as a market leader, learning from our experiences and helping our customers on their own journeys.*
>
> *– Andrew Lord, Senior Research Manager & Fellow, BT*

An additional motivation for interviewees to invest in quantum security now is the "harvest now, decrypt later" risk scenario that is well-known in the cryptographic industry (and described earlier). The takeaway is that sensitive data is at risk from quantum computing today—even though CRQCs do not yet exist.

ORION CTO Robert Eveleigh is one of the interviewees who listed "harvest now, decrypt later" as one of the drivers for investing in quantum security now:

> *With Q-Day approaching quickly, it is likely we have already reached the point where data must be protected against imminent decryption—especially depending on how long the data needs to be stored. Some major state actors use a "harvest now, decrypt later" strategy, making this a pressing concern.*
>
> *– Robert Eveleigh, Chief Technology Officer, ORION*

Monetization is crucial, as the era of frontier R&D among telcos is over. The dotted line between research and revenue must be direct and short, which makes planning for an unknown Q-Day particularly challenging for telco researchers to justify budgets.

Several interviewees said that they are positioning QSNs as a way to differentiate in connectivity and gain customers that will pay high premiums for services that will be increasingly essential. End customers are still fairly new to the QSN topic and are often shocked when they learn about threats from quantum computing. When they see the security risks, they will come to CSPs for connectivity options and will expect products to help reduce those risks.

The two quotes below from Lyntia and Colt, respectively, support this thinking:

The bottom line is we see quantum-safe services as helping us differentiate in a wholesale market. It matters to end customers who are looking for future proof connectivity and data protection as well as for our integrator partners.

– Javier Ruiz Gomez, Head of Innovation, Lyntia

We see quantum-safe capabilities as a long-term investment in risk management and resilience. There is clear value in this for enterprises and institutions that must retain sensitive data for long periods, say beyond typical retention periods. We are considering how to position it and exploring options to best suit our customers' service-level requirements.

– Prasanna Sundaram, Director, Optical and Fiber Network Engineering, Colt Technology Services

---

This Omdia White Paper was commissioned by Nokia.

Customer readiness

Interviewees in this report agreed that customers are at the earliest stages of building their quantum-safe strategies, but customer awareness of the threat of quantum computers and interest in identifying solutions have increased sharply over the past couple of years. Interest is now accelerating, say interviewees. The quote below from Colt describes the evolution in customer prioritization:

> *When we started last year, it was mainly Colt raising the topic with our customers. We are now seeing inbound inquiries from some customers. I wouldn't call it "demand" in terms of product volume yet, but there is clearly increased traction: customers are more aware, more interested, and more engaged. They're asking what they need to do to begin their quantum-safe journey.*
>
> *– Prasanna Sundaram, Director, Optical and Fiber Network Engineering, Colt Technology Services*

In addition to the increasing power of quantum computers, the Kyndryl interviewee, James Knights, said that the meteoric rise of AI is another factor driving customer anxiety about quantum threats, specifically, the combination of advanced AI with the power of quantum computing:

> *In 2024, we were working with early adopters who were beginning to explore quantum-safe security, while much of the market was still in an evaluation phase. In 2025, the rapid acceleration of AI fundamentally shifted perceptions. The convergence of AI and quantum computing has made the security implications immediate, driving a new level of urgency among customers.*
>
> *– James Knights, Principal, Network & Edge Center of Excellence, Kyndryl*

Probably the most concrete measures of gauging customer readiness to adopt QSNs are budgets. How much money have customers allocated to buy QSN services? Have customers allocated any budget at all?

This Omdia White Paper was commissioned by Nokia.

In this round of interviews, the consensus is that governments are the least constrained by budgets, followed by certain financial companies. Beyond these two customer segments, the cost of implementing QSNs is a primary barrier—even if companies recognize the necessity. Healthcare, in particular, was mentioned by several interviewees as recognizing the requirement, but this vertical may lack the budget to move forward with what is required.

Healthcare systems vary greatly, as some countries have public systems funded by governments or a mixed funding system of private and public agencies. In these scenarios, healthcare will follow regulations imposed by government agencies and will move more slowly.

Private healthcare systems have more liberty to adopt various methods and can impose a defense-in-depth approach incrementally that meets their network needs and budget constraints.

Knights from Kyndryl stated the following:

> *Technology investment priorities vary by industry. Defense organizations often operate with larger, long-term budgets, while financial services leaders tend to focus heavily on clear ROI. In sectors like healthcare and manufacturing, leaders often need to balance innovation with tighter spending constraints.*
>
> *– James Knights, Principal, Network & Edge Center of Excellence, Kyndryl*

Technology and infrastructure readiness

On the technology front, one of the biggest areas of debate within service providers and among their customers is whether to build QSNs based on SKI, PQC, QKD, or a hybrid configuration.

While end customers may tend to lean one way or the other, the interviewees generally believe that they will need hybrid strategies that include both. First, a service provider will serve multiple customers, so it will need services to address different requirements. Second, individual customers may require multiple technologies and security layers for the greatest resilience. As BT's Andrew Lord states:

> *It's not an either-or situation—it's both … Think of it like locking your house: you lock both the doors and the windows. Why would you secure only one? The future of cryptography and security involves a multi-layered approach. Hackers would need to break through multiple layers, and even if one layer is compromised—whether due to a backdoor or some other vulnerability—they would still face another equally challenging layer. It's frustrating when people position PQC and QKD as being in opposition. They're not. PQC should be implemented everywhere, while QKD is reserved for use cases where the highest level of security is required.*
>
> *– Andrew Lord, Senior Research Manager & Fellow, BT*

Colt's Prasanna Sundaram similarly expressed the need for coexistence of PQC, SKI, and QKD and envisions a potentially staged approach to technology adoption:

> *In many cases, a hybrid approach will be necessary. For example, from a regulatory standpoint, customers may prioritize compliance first and then move toward stronger security measures. We might start with PQC because it can be adapted more quickly, and as QKD technology evolves, [it] may be considered as an additional security layer.*
>
> *– Prasanna Sundaram, Director, Optical and Fiber Network Engineering, Colt Technology Services*

Technology coexistence bleeds into the topic of crypto agility, which is clearly important to those interviewed for this report. Crypto agility refers to the ability to quickly and efficiently transition between different cryptographic algorithms, protocols, and implementations without requiring significant changes to the underlying infrastructure or codebase.

Crypto agility includes the ability to adopt a variety of approved PQC algorithms that are ratified in the future and/or implement QKD within the various transmission layers in the physical network when and where needed (as BT's Lord notes in the above quote).

For Greek research network GRNET, such agility is a requirement to serve different types of customers:

We must stay agile and fully understand the needs of the end users we serve. Critical infrastructure operators, governmental users, and National Security Authorities each have different operational requirements and security expectations. At GRNET, through the HellasQCI project, our role is to validate encryption across all relevant scenarios and layers, since every community depends on a different part of the network stack. This is our main priority and the reason we pursue a comprehensive multi-layer testing approach, ensuring we are ready for real operational deployment.

– Dr. Ilias Papastamatiou, Senior Project Manager, GRNET

As discussed earlier, SKI leveraging QKD or classic physics-based keys and PQC address the quantum-safe exchange of keys. Once keys are securely exchanged, AES-256 symmetric encryption is deemed quantum-safe for encryption (by NIST and others) at the physical layer (Layer 1), MAC layer (Layer 2), IP layer (Layer 3), or others.

The Asia Pacific Tier 1 CSP interviewed is in the exploration stage of building a quantum-safe strategy, but the Enterprise CTO interviewee is already focusing on crypto agility across multiple layers as a requirement:

[We] are actually working with a couple of our partners including Nokia and others to assess what is necessary to support agility across all network layers. It is in different stages of discussion. We are exploring everything that is possible and while we're still running a lot of detection on our own network and protecting our network, we see that for the next wave of security services, including quantum, we will need more collaboration with partners and SIs.

– Enterprise CTO, Asia Pacific Tier 1 CSP

Lastly, beyond fiber optics, satellite technology is increasingly important in QSN discussions. Fiber optics cannot be physically extended to all geographies, such as over mountainous regions, and reach is a significant limitation for QKD over optical fiber. To date, networks using conventional protocols such as BB84 are limited to about 100km without regeneration. Unrepeated reaches beyond 100–150km over fiber optics are possible but experimental.

Optical fiber loss is the main contributor to the reach limitation without the potential use of amplification and/or quantum error correction. These technologies are in R&D and are making progress as quantum communication becomes a key technology enhancement toward the next evolution beyond today's classic compute machine-to-machine communication.

Satellite transmission potentially addresses both of the fiber optics limitations. However, the technology is nascent compared to fiber-based QKD, and costs would be much higher.

In Omdia's discussions, one interviewee—GRNET—is currently pursuing satellite QKD as an adjunct to terrestrial QKD. GRNET's Ilias Papastamatiou said the following:

The satellite segment is essential for island territories and geographically fragmented regions, but it is equally important for every country. Without space-based capabilities, true QKD interoperability and trusted key exchange across Europe would not be possible. Satellite links work together with terrestrial networks to provide resilience and redundancy, allowing each EuroQCI hub to communicate through multiple independent paths. This multi-route approach is what ultimately ensures continuity of secure services at the European level.

– Dr. Ilias Papastamatiou, Senior Project Manager, GRNET

Offerings and business models

The interviews show that offerings and business models are nascent. Exploration is the general status, and interviewees are largely focusing on the following:

- Engaging with potential early adopter customers to understand their priorities and requirements.
- Understanding budget levels and priorities of potential customers and exploring whether proposed quantum-safe solutions are economically feasible.
- Spreading greater industry awareness of the need for QSNs.

These companies generally want to keep all options open as they learn more about customer needs. At this stage, it is too early to predict which models will prevail. Discussions are occurring with vendors about consulting on business models that can be adopted and on how best to help so that CSPs do not incur financial risks until the service-level offerings mature.

The service providers interviewed are still defining which vertical industries are best suited for QSNs. As noted, governments (particularly militaries and government-owned critical infrastructure) and large finance institutions are the best fit to date, combining market needs with budgets to cover the costs. Privately owned critical infrastructure is also a key vertical—and this can include telecommunications networks themselves, such as those that carry emergency services.

After verticals and their requirements are clearly defined, companies can hone their models and specific services to meet those needs and budgets.

Risk management and resilience

This section of the survey digs into issues about maintaining resilient QSNs and addressing risk management—from the perspective of both the service provider and the end customers.

For network operators, cybersecurity resilience is closely tied to crypto agility (as described earlier in the ***Technology and infrastructure readiness*** section).

Crypto agility underpins cyber resilience strategies in three main ways:

- The ability to adopt PQC, SKI, and/or QKD when and where needed to address different levels of customers' security requirements.
- The implementation of quantum-safe algorithms at multiple network layers so that a security breach at one layer will not compromise user data (i.e., a "belt and suspenders" strategy for QSNs).
- The ability to swap in and out different PQC algorithms quickly and at scale to mitigate risks posed by a future crack of any initial PQC algorithms. It is worth noting that crypto agility can be achieved at the application layer only with crypto resilience at the network layer.

Omdia asked interviewees about whether they and their end customers have considered the insurance implications of quantum threats. In other words, we asked about the operators' ability to protect their investments through external underwriters.

The general consensus was that insurance implications have not been part of QSN discussions to date—either with customers or regarding their internal infrastructure plans. The primary focus at this early stage has been on establishing and meeting technical requirements.

However, the interviewees found the insurance question intriguing and agreed it is highly relevant. This suggests that insurance risks are likely to become more relevant over time as security breaches inevitably continue and as QSNs mature.

ORION's CTO made the following comment on this topic:

> *The average cost of a cyber breach keeps rising. Because of this, some [insurance] carriers are exiting or have exited or reduced participation in this market—they can't figure out how to manage the risk and still make a profit … This creates an additional burden on the community, which now has to find ways to protect itself. Some organizations are turning to self-insurance schemes or cooperatives to address the issue. In some cases, insurance companies outright refuse to provide coverage. If you don't have the necessary controls in place, they won't sell you a policy—no matter how much you're willing to pay.*
>
> *– Robert Eveleigh, Chief Technology Officer, ORION*

Ecosystem engagement and collaboration

Market complexity breeds ecosystems, and the emerging market around quantum security is highly complex. All interviewees agree that deep partnerships are essential. Encryption and transmission are separate functions, with different vendors typically supplying each. Furthermore, because it is a new area of cybersecurity, vendors developing PQC and QKD products are not the expected cybersecurity vendors. Many are newer, small companies, some of which come from academia. Many are not profitable but receive government funding to continue their leading-edge R&D.

Within the quantum security ecosystem, trusted network vendors (such as Nokia) will play a crucial role. The importance of network vendors, not just as equipment suppliers, but as quantum security facilitators and trusted advisors, was reinforced repeatedly throughout these interviews.

Among the companies interviewed for this report, the Asia Pacific Tier 1 CSP is at an earlier stage in evaluating quantum-safe products. For the Enterprise CTO, the role of network suppliers and their expertise in the evaluation process is clear, as stated below:

> *We work very closely with our partners and OEMs. We lean on them because they are the ones who develop the products and ensure that the underlying infrastructure they provide is always up and running. We have very regular conversations with them to understand what products they will be delivering and what infrastructure they are running in their labs. We visit their labs regularly.*
>
> *– Enterprise CTO, Asia Pacific Tier 1 CSP*

Among interviewees, the Asia Pacific CSP is not alone in its reliance on trusted supplier partners for quantum security expertise. It was a common theme in interviews, even among those who are relatively advanced in QSN. Service providers base their brand on their network reliability and security, and there are many untested startups in today's quantum security ecosystem.

Given the high stakes, there is a preference for an established and trusted supplier to take the lead in quantum security integration.

Lastly, Omdia addresses the positioning of Nokia itself as a preferred partner in the emerging quantum security ecosystem. Several interviewees referenced Nokia directly as a key partner, including Lyntia, as quoted below:

> *Nokia has strong expertise in quantum-safe technologies and solid regional market knowledge. Technological maturity and supply chain resilience are critical criteria for us when working with strategic partners.*
>
> *– Javier Ruiz Gomez, Head of Innovation, Lyntia*

Based on these interviews, Nokia's key strengths as a lead partner for quantum security include a combination of the following:

- Long communications heritage and financial stability, including in optical and IP networks.
- Long-standing relationships with the groups leading quantum security strategy.
- In-region market knowledge and presence.
- Deep experience in building QSNs, evidenced through customer engagements and PoCs.
- Existing partnerships and proven interoperability with leading quantum security vendors, such as with QKD.

This Omdia White Paper was commissioned by Nokia.

Appendix

Methodology

This analysis is based primarily on data and findings from a set of seven one-to-one interviews of networking companies conducted by Omdia. Interviews were based on a common *Interview Guide* that was jointly developed by Omdia and Nokia. The seven interviews were conducted from November 2025 through January 2026 by Sterling Perrin, a senior principal analyst, and Jim Hodges, a research director, both at Omdia GTM Telecom Insights and Advisory.

Analysis was supplemented by desk research on quantum security conducted by the analysts, as well as insights gleaned from ongoing industry discussions on QKD, PQC, and cybersecurity.

Sterling Perrin, Senior Principal Analyst, Optical Networks & Transport, GTM Telecom Insights and Advisory
sterling.perrin@omdia.com

Jim Hodges, Research Director, Cloud & Security, GTM Telecom Insights and Advisory
jim.hodges@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Get in touch

www.omdia.com
askananalyst@omdia.com