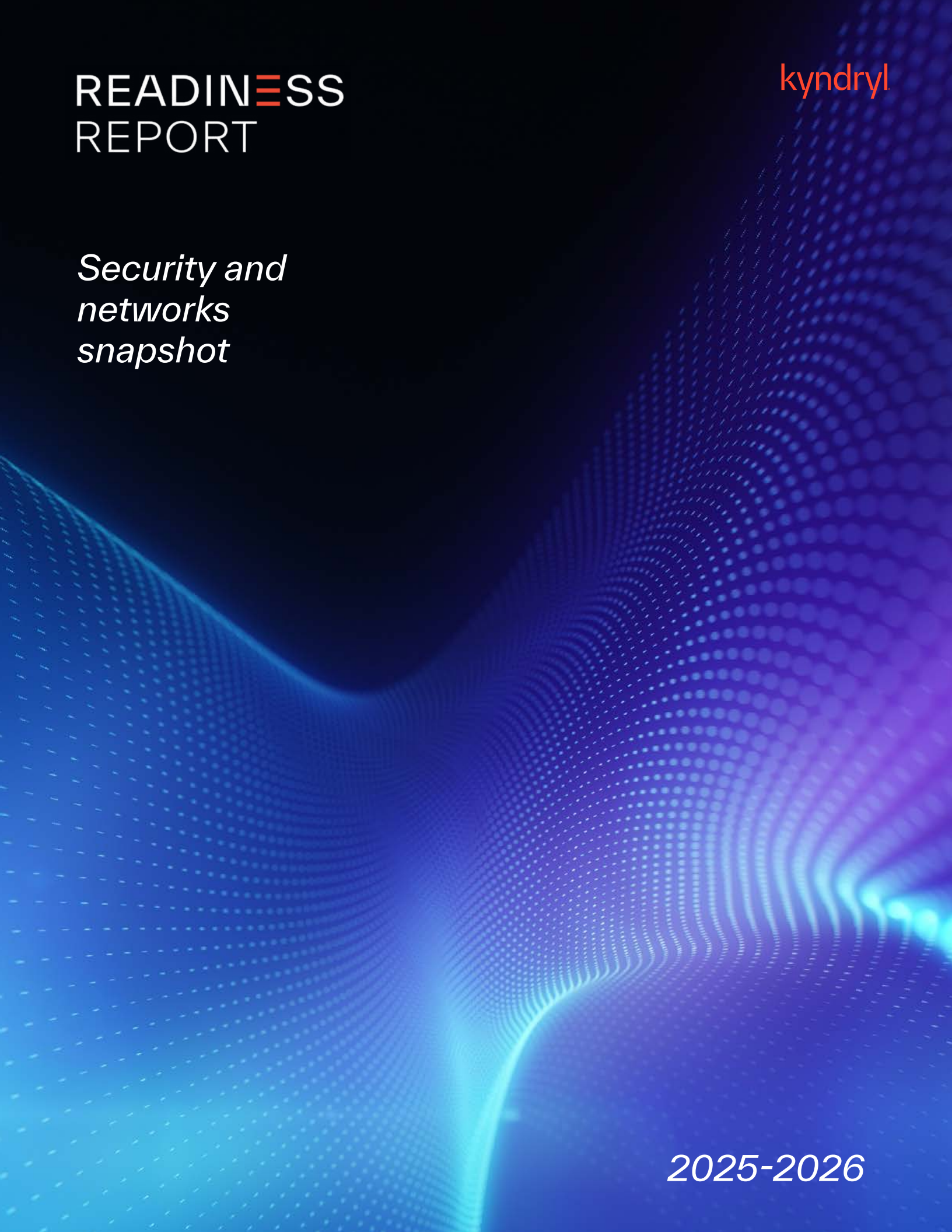
READINESS REPORT

kyndryl

Security and networks snapshot



2025-2026

Key takeaways

Quantum computing will redefine enterprise performance and innovation, while creating urgent risks for today's cryptographic infrastructure. Organizations must begin planning for post-quantum cryptography now, integrating it into network, application, supply chain and IT modernization strategies. While 62% of leaders are investing in quantum — and 20% question short-term ROI — only 4% rank it as the top near-term technology by impact. This gap between risk and return is where breaches and business disruption take root.

Sovereignty is reshaping architecture. 84% of leaders say data-sovereignty and repatriation rules have grown more important in the past year; 86% say alignment of cloud providers to regulations is increasingly critical; 91% say their cloud infrastructure offers flexibility to adapt to new or changing requirements. This is now a design constraint, not a compliance afterthought.

Networks are the center of enterprise performance. In today's AI-driven economy, the role of the network is pivotal to providing AI systems with high-quality, uninterrupted data flow. 20% of leaders say networks are a primary barrier to scaling recent tech investments. 25% of mission-critical networks, storage and servers are at end-of-service. Only 37% think their network is ready for future risk, despite 35% investing heavily in network upgrades.

Introduction

Security and networks have quietly powered digital operations for decades, but growing instances of IT complexity and fragmented functions or siloes have slowed incident response, weakened enterprise resilience and created potential operational blind spots. As AI accelerates, quantum threats loom and digital borders harden and become more complex to manage, resilience is no longer maintenance. It is now a strategic imperative.

What once lived only in IT now touches every corner of the C-suite. As AI rapidly reshapes business operations, converging forces are expanding the threat landscape — with cybercrime projected to cost trillions of dollars by 2030.

Quantum threats, tightening data sovereignty expectations and aging networks are intersecting to reshape how organizations secure, move and govern their data — making them inseparable challenges that must be addressed together to stay resilient.

These three forces are not separate risks — they are connected pressure points on the same system. Quantum computing threatens the encryption that networks rely on. Sovereignty regulations determine where and how infrastructure can be built. And the network is where both threats either get managed or get exploited. Organizations that treat them in isolation will find the gaps between them are exactly where disruption begins.

Enterprises that thrive will treat networks and security as agile, sovereignty-aware, quantum-ready platforms that keep intelligence and trust resilient and moving at business speed.

This report builds on the Kyndryl Readiness Report, drawing on insights from 3,700 business leaders from 21 countries to show how business and technology leaders are approaching these challenges — and how their organizations are evolving to stay current.

The quantum challenge

While many organizations are focused on the implications of AI, another transformational technology is also present: quantum computing.

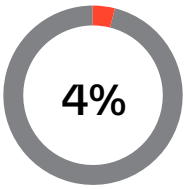
For years, cybersecurity has been defined by the pursuit of resilience — building systems that can withstand disruption rather than simply repel it. Yet the advent of fault-tolerant quantum computing introduces a threat unlike any before it, one that could unravel the cryptographic foundations underpinning the world's digital economy. This is no longer a theoretical discussion.

"Q-day" — when quantum machines can break today's cryptography — has experts and enterprise leaders recognizing the need for action this decade. Some governments around the world have set hard deadlines for migrations to quantum-resistant standards. Attackers are already harvesting encrypted data to decrypt later, raising stakes on long-lived, high-value information.

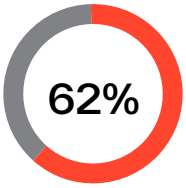
With the global cost of cybercrime projected to continue climbing and the quantum threat as a significant accelerant, this is not merely another technical risk to manage for businesses; it is a strategic challenge demanding immediate attention at the executive level. Understanding and preparing for the Post-Quantum Cryptography era is the new mandate for building true, long-term enterprise resilience.

Organizations should begin by establishing an executive-sponsored task force to lead quantum preparedness. Its first priority is a crypto census to identify all public-key cryptography in use. The census should highlight vulnerable systems, sensitive data and "harvest now, decrypt later" exposure.

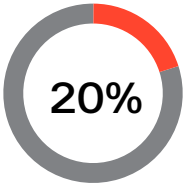
Based on these findings, leaders must create a roadmap for migration to post-quantum cryptography algorithms that include zero-trust controls across identity, endpoints, networks and data. Organizations should also engage expert partners that bring deep cryptographic and cross-identity experience.



of leaders name quantum as the single biggest-impact emerging technology over the next three years; most are focused on the potential of AI



of organizations report they are investing in quantum computing technologies



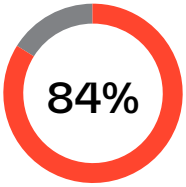
say quantum is a current investment they worry will not deliver positive ROI in the short term

Data sovereignty

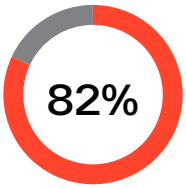
The era of frictionless cross-border data powering the world's digital economy is fading.

As governments grow more protective of their digital borders, many countries are tightening the rules around where data can go and who can touch it. Nations that once embraced open digital exchange are now retreating into operational silos, driven by concerns over security, competition, and geopolitical tension. The result is a landscape with far less openness and far more scrutiny — one where the simple act of moving data across borders has become a strategic, legal and political challenge for global enterprises.

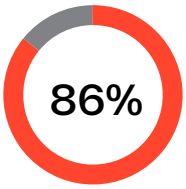
As data sovereignty rises on the executive agenda, it will become a defining constraint on business strategy, forcing enterprise leaders to rethink how they store data, architect applications, innovate and compete. For enterprises that built their technology estates during a more optimistic era of globalization, this shift introduces profound complexity. At the same time, data sovereignty demands a thoughtful and nuanced response — one that balances compliance with ambition, protects data without limiting progress and recognizes that the future of innovation will depend as much on where information lives as on what companies do with it.



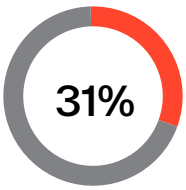
say emerging data sovereignty and repatriation regulations have become more important in the past year



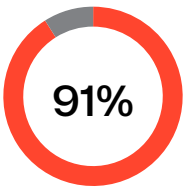
are concerned about rising geopolitical instability and tensions



say regulatory alignment of cloud providers is becoming increasingly important



of leaders cite regulatory or compliance concerns as primary barrier limiting ability to scale recent technology investments



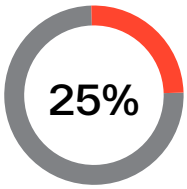
say their cloud infrastructure gives flexibility to adapt quickly to new/changing regulatory requirements

Networks and security modernization

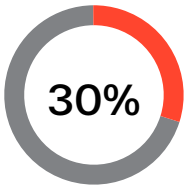
Throughout the digital era, enterprise networks quietly powered digital operations — reliable, functional and largely invisible. But as AI redefines how organizations operate, that era of static, backstage IT infrastructure is ending. The modern enterprise now runs on data in motion, not data at rest. And the network has become the determining factor in whether that data translates into insight, autonomy and competitive advantage.

AI systems depend on uninterrupted, high-quality data flows. Hybrid environments stretch across clouds, applications, systems and devices. Threats move autonomously, exploiting every gap in legacy systems. And the expectations placed on digital experiences leave no room for latency or downtime. In this environment, traditional networks don't just slow business down; they actively constrain innovation.

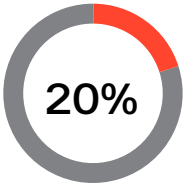
As organizations shift toward real-time decision-making and AI-driven operations, the network becomes the new center of enterprise performance. Modern, automated networks enable the agility, security and scalability needed to keep pace with growing demand. Businesses that modernize aren't simply upgrading infrastructure — they are redesigning the operational backbone of the digital business.



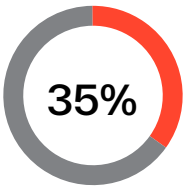
of mission-critical networks, storage, and servers are at end-of-service



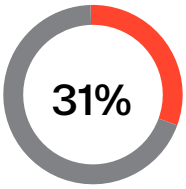
of respondents who experienced a cyber-related outage cite their networks as the cause



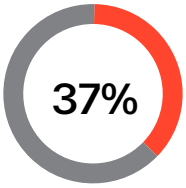
of respondents say that their networks are a primary barrier to scaling their recent technology investments



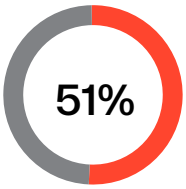
of organizations are investing "heavily" into network infrastructure



investing "heavily" in 5G or 6G technologies



of business leaders think their network infrastructure is ready to manage future risks and disruptive forces



experiencing positive ROI from network infrastructure investments

Conclusion

A decade ago, resilience meant withstanding disruption. In the AI era, the convergence of cascading systemic risks – technical, financial, societal and geopolitical dynamics – means organizations must be prepared to withstand, respond to and recover from potential disruptions and turn risks into advantage. The path forward is deliberate design: quantum-ready cryptography, sovereignty-by-design data pipelines and agile networks that allow data to move securely at the speed of business.

What companies should do now

Launch a quantum task force and crypto census. The task force should identify and take inventory of the systems using today's common encryption methods. Based the assessment results, prioritize upgrading the most sensitive areas first to defend against cyber attackers who steal encrypted data now and plan to unlock it in the future.

Modernize networks to unlock AI performance. Phase out old, outdated equipment and introduce tools that automatically monitor and improve network performance. Upgrade systems so data can move quickly and smoothly, which is essential for scaling AI.

Set clear standards for secure and compliant system design. Create design guidelines that explain how to handle encryption, where data is allowed to live and how to protect it. Require that new systems follow these rules to mitigate potential risk from future attacks.

Use a scorecard to track progress. Regularly check how well your enterprise is moving toward stronger encryption, meeting data-location requirements, improving the speed and reliability of data movement and phasing out outdated technology to show clear progress toward modern, resilient operations.

kyndryl

This report was not printed.

Company Headquarters

One Vanderbilt Avenue, 15th Floor
New York, New York 10017

kyndryl.com