TechFinitive™

World Quantum Day 2026

Our thanks to all the technology professionals who shared their views for our World Quantum Day 2026. We were overwhelmed by the interest and volume of responses. For readability, we have included a wider selection of responses below.

What is one real-world problem that quantum computing could solve within the next decade that classical computing cannot?

The world needs an alternative to rare-earth, permanent magnets. We expect this specific area of materials science research to be one of the early use-cases of quantum computers. The simulation of natural materials is extremely challenging for classical computers. As quantum computers develop in the eFTQC era - they'll directly model quantum systems they can simulate these materials much more efficiently."

The U.S. Department of Energy has recognized this need and is funding research to use quantum simulation to develop more abundant and more sustainable magnets to power electric engines and turbines. Quantum algorithms from this work could be applied to other challenging problems in chemistry and materials science.

Théau Peronnin, CEO and co-founder of Alice & Bob

In my view, one of the most interesting candidates is not a generic compute problem but a trust problem: distinguishing genuine human identity signals from synthetic, coordinated, or replayed ones when the attack surface becomes too high-dimensional for classical shortcuts to remain reliable. In identity and biometrics, the next generation of fraud will not be just a fake face or fake voice in isolation; it will be multi-modal, session-aware, adaptive, and potentially coordinated by AI agents. One of the things I've been exploring is the idea that quantum feature spaces, quantum kernels, and related scoring methods may eventually help separate subtle fraud patterns, replay states, and liveness indicators that are difficult to represent compactly in classical systems at useful latency. I would not claim that this is commercially solved today, but I do believe this is a credible category of future advantage where quantum computing could materially expand what is defensible in high-assurance identity.

Ralph Rodriguez, President and Chief Product Officer, Daon

One of the most realistic near-term applications of quantum computing is optimization and simulation problems that become exponentially complex for classical computers,

particularly in financial markets, logistics, and materials science.

In finance and trading, for example, portfolio optimization across thousands of correlated assets with real-time constraints is computationally intractable with classical systems at scale. Quantum optimization algorithms could evaluate vast combinations simultaneously and produce better risk-adjusted portfolio allocations, liquidity routing, and derivatives pricing models.

Another area is molecular and materials simulation. Quantum computers can model quantum systems directly, something classical computers approximate inefficiently. This could accelerate development of new batteries, semiconductors, and pharmaceuticals within the next decade.

So the first real breakthroughs will likely not be consumer applications, but optimization, simulation, and cryptography-related problems where classical computing hits exponential limits.

Yoon Auh, Co-Founder of BOLTS Technologies

One of the most critical challenges quantum computing will solve within the next decade is the optimization of global power grids to accommodate the mass transition to renewable energy. As we move away from steady fossil fuels toward fluctuating sources like solar and wind, classical computers struggle to manage the Unit Commitment Problem (UCP), the complex calculation of when to start or stop generators to balance supply and demand in real-time. Quantum systems can process these billions of variables simultaneously, preventing energy waste and grid instability. This shift will allow us to secure the 3E+S standard (Energy Security, Economy, Environment, and Safety) and hit aggressive carbon-neutral goals that is mathematically impossible for today's hardware to manage.

Dippu Kumar Singh, Leader of Emerging Technologies at Fujitsu North America Inc.

Breaking encryption. That's the honest answer. Today's cryptography works because no classical machine can crack it in a useful time. A mature quantum computer could. We're not there yet, probably not for another seven or eight years at production scale, but the countdown is already running. So it won't solve a real-world problem. It will create a new one. And a huge one. Maybe there will be some other application in simulation, chemistry, or AI. But I believe cryptography will be impacted first.

Jiří Štěpán, CEO at Etnetera Group

What should every business leader understand about quantum computing right now?

There's a lot more thought about quantum than there is preparation for quantum in today's investment. Everyone right now is focused on AI, and rightfully so. Quantum is

much more in the pure science phase than in the business applicability phase. But there are real dangers that we need to do more than think about.

The strategy of “Harvest Now, Decrypt Later” is the biggest current threat that quantum is indirectly placing on companies that they should think about more. Digital thieves are currently collecting encrypted data with the intent to unlock it once quantum systems mature. Quantum computing will render anything encrypted with asymmetric encryption tools readable once they are released. As a best practice, everyone should shift to AES-256 encryption as standard at least. This level of encryption will be at least quantum resistant (256 bit encryption becomes more akin to 128 bit encryption in a quantum world).

Most companies are thinking about quantum in terms of data governance and compliance right now. I think we need to go a little deeper into it, and understand that quantum will not only impact us when it arrives, but expose our past assumptions as well. Having a mind towards marking data as compromised, and then taking steps to make that data ephemeral so that it is less impactful over time is a good best practice to evolve. Right now we have a little bit of time; we should use it.

We should also be looking at our development processes, our frameworks, and our development ideologies. AI is making us do that anyway; it’s worthwhile to have an eye to the horizon and also ask ourselves what this looks like in a quantum computing world as well. The hard part is, that a lot of this is conjecture at this point. But if there is a lesson of the past we can take forward with us it is to invest in the ability to change, to be agile, to learn, to experiment and grow. The companies that have that as part of their ethos will be best situated to both avoid the pitfalls and take advantage of quantum once it arrives commercially.

Daniel Nelson, Chief Product Officer at Park Place Technologies

---

The future is closer than most people think. Quantum computing is no longer a research-only technology. Several companies, including QuEra, have published realistic science-based roadmaps that deliver true business value within a couple of years. Early access programs are already running, and business leaders should understand that the preparation window is now, not when the hardware arrives. That means identifying which valuable problems in your organization are genuinely hard for classical computers, building quantum literacy within your senior technical teams, and engaging with quantum providers so you're not learning from scratch when production-ready systems come online.

Yuval Boger, Chief Commercial Officer of QuEra

Data encrypted today can be captured and stored, then decrypted later when quantum systems become powerful enough. This “harvest now, decrypt later” risk is already real. Waiting until the threat is immediate is too late. At the same time, approaches like fully homomorphic encryption (FHE) show a different path, where data can be used without ever being decrypted, reducing exposure altogether. Leaders should start now by

identifying sensitive, long-lived data, understanding exposure, and planning migration to new standards. This is not just a technical issue. It is a strategic risk.

Jeremy Bradley-Silverio Donato, COO at Zama

What is critical to understand now is that there will not be a single “quantum computer.” Different approaches will coexist, each suited to different problems. Just like today’s computing landscape, where we use different architectures depending on the need, quantum will evolve as an ecosystem: analog and digital systems, superconducting platforms, neutral atoms, photons, etc, each with its own strengths. For business leaders, the priority is not to pick a winner today, but to start understanding how these technologies map to their problems. This means learning, experimenting, and determining where quantum can add value to your business. The shift won’t happen overnight, but it will come faster than expected - and in many ways, it’s already happening. Just as GPUs unlocked AI, QPUs will enable new ways of processing information that are fundamentally out of reach for classical systems, while also opening the door to more resource-efficient approaches to AI.

Dr. Marta P. Estarellas, CEO of Qilimanjaro Quantum Tech

Quantum computing is following a development arc much like AI, and business leaders have a choice to make whether they want to be ahead of or behind the transformation to come.

AI developed over decades, with incremental advancements compounding until a set of new capabilities led to the "Chat GPT moment" that changed everything. At that stage, we learned there were two classes of businesses—those prepared to move and those scrambling to catch up. Quantum similarly has decades of hidden technology development underpinning where we are today, and it appears that the breakthrough moment is coming within the next several years. The initial breakthroughs will be narrow, as were the early business applications of AI tools, but relevance will rapidly expand.

The key difference is that this time, visibility on the technology through both quantum company public listings and the very recent arrival of AI has provided businesses with an opportunity to prepare. The Boston Consulting Group identifies that 90% of value capture from the $2T quantum opportunity will go to early adopters. Business leaders have to ask themselves whether they want to share in that 90% of scramble afterwards for the crumbs left behind.

Michael Biercuk, CEO at Q-CTRL

Most organizations are asking when Q-Day will arrive. That is the wrong question and it’s costing them.

The real risk is that adversaries are already harvesting encrypted data today and storing it for the moment quantum systems can decrypt it. For any data with a long lifespan, the exposure has effectively already begun.

What's failing now is leadership and execution. Too many organizations are treating this like a routine upgrade: running slow inventories and multi-year planning cycles while the risk compounds in the background. That playbook simply does not support the present risk.

This is the first security shift where delay creates permanent exposure. The priority should not be to predict Q-Day, it must be to act before it matters: open the budget, secure high-value long-lived data first, and incrementally transition your encryption to reduce the quietly building liability.

Meg Gleason, Head of Product at QuSecure

With the UK government recently announcing over £1 billion of funding on large scale quantum computers and £670million on the National Quantum Computing Centre (NQCC) over ten years, every business leader must understand the importance of early experimentation and capability building in the immediate term. Whilst today's quantum devices are error prone, have a few hundred qubits at most, and will be limited to relatively niche business problems, in ten to fifteen years we will see much larger and more powerful quantum computers, with errors in individual qubits detected and corrected by quantum error correcting codes.

Daniel Goldsmith, Senior Quantum Computing Technologist at Digital Catapult

---

Enterprise decisions made now will determine who captures disproportionate value from quantum computing. Quantum is becoming increasingly relevant to enterprises as hardware advances, but many organizations are not equipped to effectively deploy the technology. The key roadblock is the lack clarity of around where quantum can deliver value and what it will take to get there. When quantum efforts are not tied to business priorities, timelines and resource expectations, they remain isolated proofs of concept. To drive real progress, businesses must have a structured approach to identifying which applications matter and when and how to build them.

Sumit Kapur, CEO at Zapata Quantum

Quantum computing will not replace your computers, but it will break your encryption, so business leaders must start planning for post-quantum cybersecurity now. Standards have already been released, and with currently used encryption going away within the upcoming decade, the clock has already started counting down. You don't want to be left behind.

Quantum's real power lies in solving a few critical problems years down the line, so build expertise and identify high-impact use cases today to stay ahead.

Kawin Boonyapredee, CISO Advisor at KnowBe4

Quantum is not a faster computer. It's a different class of problem solver.

Near term, it won't replace classical systems. It will sit beside them and tackle very specific problems where today's methods break down: optimization, materials discovery, complex simulations.

The real issue for leaders isn't "when do I deploy quantum." It's whether their organization even knows which of their problems could benefit.

Two practical moves now:

- Inventory your hardest computational bottlenecks.

- Start tracking credible ecosystems like IBM and Google, not the hype cycle.

Also, don't ignore security. Post-quantum encryption isn't theoretical. It's a timeline issue.

Bottom line: quantum won't hit you all at once. It will show up quietly in edge use cases and then compound fast.

Matt Hasan, Ph.D., CEO at aiRESULTS and Founder, The AI Humanist Movement

---

Every business leader should understand that quantum computing is no longer just a moonshot science story; it is becoming a strategic architecture story. Most executives understandably focus on post-quantum cryptography, and they should, because cryptographic migration is now a real board-level planning issue. But the broader lesson is that quantum will affect trust in two ways: first by forcing changes to the cryptographic foundation of digital systems, and second by opening new possibilities in how we model risk, anomaly, liveness, and authenticity. My own view is that the winners will not be the companies that simply swap one algorithm for another at the last minute. They will be the ones that build quantum-ready trust stacks now: PQC at the foundation, with stronger anomaly sensing, replay defense, and liveness or provenance controls layered on top.

Ralph Rodriguez, President and Chief Product Officer, Daon

Given the acceleration of quantum computers and their capabilities, the time it takes to train talent, and the growing potential use cases, organizations need a roadmap for how they will derive value from quantum computers – the who, what, when, where, why, and how? The good news is that while we wait for hardware to mature, there are increasing options to see return on investment today using quantum-inspired techniques, which use principles of quantum physics and run on today's CPUs and GPUs. Done properly, quantum-inspired techniques provide value today (for instance, in machine learning and simulations) while also providing the opportunity to learn about the techniques used to program quantum computers. And once the hardware comes online, these techniques can pivot to run on future machines, helping futureproof talent and technology while realizing value today

Scott Buchholz, Quantum Computing Lead at Deloitte

As the quantum threat gets closer, the security conversation around AI needs to change. To date, it's been focused on the data that goes in: how it is collected, stored, governed and encrypted. But once data is used to train or fine-tune a model, the model becomes part intellectual property, part decision engine and part attack surface. In effect, it becomes a crown-jewel asset. For companies building with AI, that changes the conversation entirely.

It is not enough to think of AI security as a perimeter problem, and this is especially true as we enter the post-quantum era. There's an enormous national conversation going on around this. Protecting the cloud environment is necessary. Protecting the database is necessary. But once AI becomes part of the product, new risks appear inside the system itself. Companies need to consider security systems that cover the full model lifecycle: what data enters the system, how models are trained and fine-tuned, how they are exposed, how access is monitored, how abuse is detected, and how privacy leakage is tested before systems reach production.

Companies don’t need to slow innovation, but they do need to treat model security as a priority. Practical questions for leadership teams to ask: what controls can be deployed now—access controls, query monitoring, abuse detection and privacy testing—to reduce exposure? What systems do we need to minimize the risk of misuse?

Jeremy Samuelson, EVP AI and Innovation at Integrated Quantum Technologies

---

Every executive should be asking 'what is our company's quantum strategy and plan'. A few thoughts on what each company should be doing:

- Understand the pros and cons of *quantum vs. traditional compute.
- Develop a strategic plan for quantum adoption.
- Explore potential use cases through *'playgrounding' and proofs of concept (outside of security). There are obvious use cases in finance and pharma, but there are many large-scale, complex use cases that can warrant some proofs of concept, like networking and complex data issues.
- Ensure that there is knowledge and a plan (and preferably a current implementation) to follow data protection and key encryption best practices to protect from quantum key decryption capabilities.
- Ensure quantum security capabilities are followed as a risk factor.

This does not need to be accomplished personally by every business leader, but it should be a corporate-level plan that business leaders are familiar with.

Yvette Kanouff, Partner at JC2 Ventures

Every business leader should understand that, for the foreseeable future, quantum computing is not a replacement for classical computing or today’s supercomputers, but rather a complement to them. The most practical near-term path is hybrid, connecting quantum systems with existing high-performance computing infrastructure to tackle narrow, high-value problems where classical methods start to hit limits. That is why the

early commercial focus is less about science fiction and more about two very concrete areas: security and optimization. On security, the issue is immediate because sensitive data encrypted today could still be vulnerable to “harvest now, decrypt later” attacks, and NIST has already finalized its first post-quantum cryptography standards. On optimization, the opportunity is in problems like logistics, scheduling, portfolio construction, and complex simulations, where quantum can eventually serve as an accelerator inside a broader classical workflow. For most companies, the right move today is not a massive quantum budget, but rather to start preparing for post-quantum security and to run disciplined pilots that connect quantum tools to existing compute environments, so the organization builds real capability before the technology fully matures.

Anthony Georgiades, Founder and General Partner, at Innovating Capital

---

A qubit on its own is not enough - it’s the whole system that matters. Over the past year, we have seen quite clearly how the focus is moving towards the critical control elements: low-latency links between classical and quantum systems, calibration that sits close to the hardware, and more open architectures so developers can build without being locked into one approach. Hybrid QPU–HPC integration has been discussed for a while, and now it’s about putting those systems together. We have a much clearer understanding of the latency requirements for error correction. The open question is whether the full stack, meaning control, compute, and everything in between, can be integrated in a way that actually scales. That’s really the challenge in front of us.

Yonatan Cohen, CTO, Quantum Machines

Most business leaders are asking the wrong question about quantum computing — “When will it be useful?” Instead, they should be asking, “where could it quietly make today’s assumptions obsolete?” Quantum advantage won’t arrive as a broad, overnight replacement for classical systems. It will show up in potentially in areas such as optimisation, material science and cryptography. The practical implication is not to invest blindly in quantum hardware, but to identify which parts of your business rely on problems that scale poorly due classical computing and begin experimenting there. In parallel, leaders should treat quantum as a strategic timing issue – too early and you waste resources, too late and you inherit disrupted supply chains, broken security assumptions or competitors with structurally better solutions.

Tay Lip Sing, Co-founder and CEO of Affirmo Technology

A top level understanding is probably sufficient for now: Quantum computing represents a fundamentally new way of performing calculations, at a scale and speed we have never seen before. The critical implication is that it has the potential to break all current encryption methods, instantly. NIST published its post-quantum cryptography standards in 2024, which signals that the industry is taking this seriously, even if a production-ready quantum computer does not yet exist.

Jon Abbott CEO and Co-Founder at ThreatAware

When do you realistically expect quantum computing to impact your industry -- and what will that first impact look like?

For digital identity, authentication, and biometrics, I expect the first real impact to arrive well before a dramatic 'quantum breaks everything' moment. The first visible impact will be architectural, not theatrical: more urgent crypto-agility programs, PQC transition planning around signatures, credentials, firmware, device trust, and long-lived authentication infrastructure, and more serious thinking about how to defend against future machine-speed fraud. In parallel, I expect R&D teams to keep exploring how quantum methods might strengthen fraud detection, replay resistance, and liveness in regulated sectors such as banking, healthcare, and government. So, the first impact on our industry will likely look less like a headline-grabbing quantum login experience and more like a redesign of the trust stack underneath identity systems.

Ralph Rodriguez, President and Chief Product Officer, Daon

We realistically see quantum computing as a long term challenge, not an immediate shock. Its first impact on crypto will probably be a new wave of security upgrades across wallets, exchanges, and custody services. The key point is simple. The industry will have to adapt before quantum becomes a practical threat.

Martin Košťál, Chief Growth Officer at Coinmate

Quantum computing looms on the horizon and with it the potential for catastrophic data compromise. Quantum is expected to allow attackers to break encryption rendering all sensitive data vulnerable but just when that threat will be realised remains an unknown. A year? Ten years? It's certainly coming which is why threat actors are thought to be hoarding encrypted data in the expectation they'll be able to decrypt it in the future. IBM predicts we can expect early networked Quantum in the early 2030's. But our expectation is that a nation state will make inroads with the technology before then, into 2027 or 2028 after which Pandora's Box will be open. If that happens, it's the security sector that will need to step up first because we can expect to see mass data dumps on the dark web, mass credential abuse, and it declared 'open season' on corporate systems. Organisations therefore need to start familiarising themselves now with the NIST post quantum cryptographic standards released last year, the innovative algorithms it refers to, and begin to plan how they will migrate their existing data assets to become quantum-ready.

Gary Mounsor, Senior Cybersecurity Consultant at e2e-assure

Is quantum computing overhyped today, or are businesses underestimating how disruptive it will be?

I think it will be hugely disruptive, if and when a production-ready quantum computer is achieved. However, the potential impact is so significant that I am not sure you can ever fully prepare for it. There are only a handful of quantum computers in existence today, they are as expensive as a nuclear programme to build and run, and unlike AI, I believe they will be tightly regulated. For those reasons, I don't think it warrants urgent attention right now, with one caveat: if your organisation holds data that needs to remain sensitive for ten years or more, it is worth being aware that adversaries could theoretically be harvesting encrypted data today with the intention of decrypting it later.

Jon Abbott CEO and Co-Founder at ThreatAware

Quantum computing isn't overhyped, but it's misunderstood. Most businesses are treating it like the next upgrade to today's systems, when in reality it's a completely different paradigm. Comparing quantum to classical computing is like comparing an aeroplane to a rocket ship – both modes of transport, but the rules, scale and possibilities are fundamentally different.

The risk isn't that companies are overestimating quantum, it's that they're applying old thinking to something that will render those assumptions obsolete. When it arrives at scale, the way we solve problems, secure data and design systems will have to be rethought from the ground up.

Anthony Cusimano, Director at Object First

The honest answer is both. Quantum computing is overhyped when it is marketed as if every enterprise will need a quantum product strategy next quarter, or as if near-term hardware will magically replace classical systems. But businesses are underestimating how disruptive it will be in security, trust infrastructure, and long-horizon platform design. The mistake is to think disruption only begins when there is a fully mature, fault-tolerant machine at scale. In reality, disruption begins earlier, when credible timelines change board priorities, standards, procurement language, and product roadmaps. That is why I believe the market should think beyond 'PQC only' and start preparing for a broader quantum identity future in which cryptography, fraud detection, replay defense, and liveness assurance all evolve together.

Ralph Rodriguez, President and Chief Product Officer, Daon

It is really a superposition of the two. In some ways quantum computing is overhyped, and at the same time many businesses are underestimating its potential to disrupt. This really has to do with timelines, market drivers, and a lack of understanding of quantum computing. Quantum computers will be disruptive, but both the applications and hardware are still being developed. The unknown potential easily leads to hyping, which is true of most emerging markets. Yet, because the applications and the hardware needed for real impact are still being developed, many businesses are likely underestimating or at least not focusing on how it will affect their work. Businesses should understand that not every headline signals a revolution in the field, but taken all together, significant progress

is being made. Quantum computing will arrive and provide real value for those prepared to adopt and deploy.

Corey Stambaugh, Director of The Capital of Quantum

The idea of quantum computers entirely replacing classical data centres is definitely hype, but the shift towards 'hybrid' data centres is very real - where CPUs, GPUs, and Quantum Processing Units (QPUs) will work together. We won't see data centres start ripping out server racks and replacing them with quantum before 2030 at the earliest. The real data centre revolution is happening in the software layer. For enterprises, the big bottleneck is the months of custom integration code required to make QPUs operate as accelerators for existing High-Performance Computing (HPC). Fixing this is what will deliver more immediate, measurable ROI for enterprises today.

Dan Holme, Co-Founder & CEO, Qoro Quantum

I have a very contrarian opinion on quantum computing. I think quantum computers based on qubit entanglement will never work, at least not as well as people hope they will. Sharing Albert Einstein's opinion, I haven't reconciled with the Copenhagen interpretation of quantum mechanics and believe that quantum entanglement is only an expression of deeper physical phenomena, which cannot be used for such parallel computation. That's why quantum computers are so elusive and always several years ahead. By the way, that doesn't mean quantum mechanics won't make computers faster - it certainly will, just not through qubits.

Jan Čurn, CEO and co-founder Apify

Both. There is real hype, and some companies' roadmaps are probably based on science-fiction and not just science, but most businesses are making the opposite mistake: assuming quantum is a decade away and ignoring it entirely. The reality is that forward-thinking companies in pharma, materials science, finance, and logistics are no longer waiting for a perfect machine before engaging. They understand that if they don't, they will find themselves years behind competitors who started preparing early. The disruption won't arrive all at once, and it will reward the organizations that treated this transition seriously before it became obvious.

Yuval Boger, Chief Commercial Officer of QuEra

How should organisations be preparing today for the security risks posed by quantum computing?

The impact of quantum computing isn't a future problem, it is a present-day vulnerability for any enterprise that handles sensitive data. Many organizations rely on current or even outdated encryption standards to protect their data, but adversaries are already using

‘Harvest Now, Decrypt Later’ tactics to intercept and store encrypted data with the intent to retroactively decrypt it later.

To protect long-term data integrity and prepare for the security risks posed by quantum computing, business and procurement leaders must treat post-quantum cryptography (PQC) as a mandatory security feature to be integrated into all new sourcing and supplier management solutions. Deploying PQC now instead of treating it as a post-quantum compliance task demonstrates a commitment to security that builds trust and directly influences modern buying decisions

Akhilesh Agarwal, President of P2P Solutions and Technology at apexanalytix

---

The threat from quantum computing is not a future problem; it is happening right now. Adversaries are actively harvesting encrypted data today, banking on the certainty that quantum computers will soon give them the power to decrypt it at will. This "harvest now, decrypt later" reality means that any sensitive data in transit is already at risk, regardless of when quantum capability fully matures. The clock started the moment the first packet was intercepted and stored, and organisations that are waiting for a definitive quantum timeline before acting are already behind. The immediate priority must be deploying data-centric security, protection that is attached to and travels with the data itself, over any app, any infrastructure, anywhere. This is not about securing the network perimeter or trusting that cloud controls will hold. It is about ensuring that data, wherever it moves and whatever path it takes, remains cryptographically useless to any adversary. The right approach delivers consistent, quantum-safe enforcement applied directly to every flow, from server workloads to the edge, without requiring changes to applications, networks, or architectures. Organisations can be protected in months, not years. With that foundation in place, the broader work of identifying and addressing embedded cryptography across legacy applications and infrastructure can follow in a structured, manageable way. That longer-term programme is important, but it should never be the reason to delay protecting data that is already in motion and at risk today. Act on what is immediate and certain and build the rest of the programme from a position of security rather than exposure.

Simon Pamplin, Chief Technology Officer at Certes

Organizations should start with disciplined inventory and trust mapping. They need to know where public-key cryptography sits inside their business, not just in obvious places like VPNs and certificates, but in authentication services, signing systems, device identity, secure boot, admin access, credential issuance, and archived signed records. From there, they should prioritize crypto agility and phase in PQC where the lifespan and blast radius justify urgency. My own belief is that this should be paired with a second track that many organizations still overlook: planning for more sophisticated fraud. If attackers become better resourced, more automated, and more coordinated, then quantum-era resilience will require more than new algorithms. It will require better anomaly sensing, stronger replay defense, and higher-assurance liveness and provenance controls across the identity stack.

Ralph Rodriguez, President and Chief Product Officer, Daon

Thanks to the National Institute of Standards and Technology, we are at least in a position where we can prepare. Many top IT service providers are already implementing post-quantum cryptography. The challenge is really performing the cost-benefit analysis of when to act. Companies have a number of cyber threats to deal with, many of which are clear and present. Focusing on a future risk can be hard when you are worried about meeting investors' expectations for returns or next quarter's financial statements. But that is the world we live in, you have to have a plan for the future. So organisations should start by inventorying their systems for vulnerabilities (especially hardware), understanding their planned upgrade cycles, and ensuring they are positioned to migrate as soon as possible.

Corey Stambaugh, Director of The Capital of Quantum

Organizations must treat quantum security as a workforce challenge, not just a technology one. While everyone focuses on encryption upgrades and vendor timelines, most security teams lack the basic quantum knowledge needed to implement, validate, or defend post-quantum cryptography. The organizations that will handle the transition smoothly are those already building quantum literacy into their teams today, so when the migration becomes urgent, their people actually understand what they're doing. Start training now, before the crisis hits.

Nick Misner, COO at Cybrary

Preparing for quantum risk isn't a technology upgrade; it's a timing decision. The migration to quantum-safe security will take years, not quarters, and adversaries aren't waiting. Organizations should embed quantum readiness into existing initiatives: zero trust, network modernization, and supply chain risk. So progress starts now, without new friction. Where does one start? Start with a hard truth: you can't secure what you can't see. Most organizations have no clear inventory of where cryptography lives across their environment. The first move is visibility, identify it, quantify the risk, and prioritize what matters. From there, build crypto agility so you can replace vulnerable algorithms without rebuilding your business. The companies that move now will migrate on their terms, the rest will migrate under pressure. The biggest mistake is waiting for certainty; by the time quantum risk is obvious, it will already be too late.

Peter Bentley, Chief Operating Officer at Patero

Quantum computing will eventually break the assumptions behind much of today's public-key cryptography, and that means teams need to start planning for crypto agility now. You do not want to be in a position where you have to rip out core network infrastructure under pressure. The real risk is the lead-up: the long transition period where attackers may already be collecting data now to decrypt later. That's why organizations should focus on making their networks adaptable, software-defined, and

ready for post-quantum cryptography as it matures. The right answer is to design for change. If your network is built to evolve, you can adopt quantum-safe capabilities without a disruptive overhaul.

Adam Ierymenko, Founder of ZeroTier

The race for post-quantum encryption has geopolitical stakes, but it's not just a problem for the NSA," says Nick Martin, CEO of Cyber Guardian Consulting Group. "Every company storing sensitive customer data is under threat. Small and mid-size businesses without million-dollar IT budgets are quietly facing an existential security crisis, and the time to act is now.

Cyber Guardian is one of the early pioneers implementing Post-quantum ML-KEM encryption, which combines the principles of machine learning and cryptography to create encryption schemes that even a quantum computer cannot break. While fully capable quantum computers are not yet here, Martin says many hackers are actively stealing encrypted files knowing they can eventually unlock them under a "harvest now, decrypt later" strategy.

Think of today's encryption like locks on a vault," says Martin. "Quantum computers are like a key that can open all existing locks. Post-quantum encryption, like ML-KEM, changes the entire concept of the lock so that even the most advanced key won't work. From finance to healthcare to retail, we're working with companies to ensure sensitive customer or proprietary data remains secure decades into the future. This issue impacts everyone.

Nick Martin, CEO of Cyber Guardian Consulting Group

The threat from quantum computing is not a future problem; it is happening right now. Adversaries are actively harvesting encrypted data today, banking on the certainty that quantum computers will soon give them the power to decrypt it at will. This "harvest now, decrypt later" reality means that any sensitive data in transit is already at risk, regardless of when quantum capability fully matures. The clock started the moment the first packet was intercepted and stored, and organisations that are waiting for a definitive quantum timeline before acting are already behind. The immediate priority must be deploying data-centric security, protection that is attached to and travels with the data itself, over any app, any infrastructure, anywhere. This is not about securing the network perimeter or trusting that cloud controls will hold. It is about ensuring that data, wherever it moves and whatever path it takes, remains cryptographically useless to any adversary. The right approach delivers consistent, quantum-safe enforcement applied directly to every flow, from server workloads to the edge, without requiring changes to applications, networks, or architectures. Organisations can be protected in months, not years. With that foundation in place, the broader work of identifying and addressing embedded cryptography across legacy applications and infrastructure can follow in a structured, manageable way. That longer-term programme is important, but it should never be the reason to delay protecting data that is already in motion and at risk today. Act on what is

immediate and certain and build the rest of the programme from a position of security rather than exposure.

Simon Pamplin, Chief Technology Officer at Certes

Companies should be protecting against the harvesting of data that's happening today by foreign adversaries. These countries are collecting encrypted data because they're betting that quantum security will soon allow them to decrypt it. The UK government, for instance, recently warned its citizens that the Chinese had stolen every UK person's data for these purposes.

The way to prepare against these attacks is to layer in quantum networking security today. This technology is unbreakable, secured by the laws of physics, and even Albert Einstein famously dismissed it as impossible. But there are real-world use cases being deployed around the world already, and classical security cannot touch what quantum security can do.

Using quantum networking hardware, like Qunnect's Carina, is one way to do this. Carina is the technology present in New York City, Berlin, New Mexico, and many other places. It provides provable security that immediately knows when it's been breached. Adopting this type of technology will secure communications today and indefinitely if it's adopted by companies.

Noel Goddard, CEO of Qunnect

Adversaries are already using 'Harvest Now, Decrypt Later' tactics, and - if Google's latest predictions are correct - Q-Day could arrive as early as 2029. Migrating data and asset protection infrastructure to post-quantum cryptography (PQC) is a multi-year journey, spanning data in motion, data at rest and data in use. Meaning universal migration should have already started. A year on from NIST's quantum-safe standards, we're seeing organisations start to move from planning PQC to deployment. Large enterprises such as Mastercard are already advocating early adoption, particularly in the finance sector. Yet, without standardised benchmarks for quantum risk and readiness, many organisations continue to underestimate the threat. Research from the 2026 Global State of Post-Quantum and Cryptographic Security Trends report shows that only 38% of organisations globally are currently transitioning to PQC. In 2026, leaders need to take decisive action to protect how identities are issued, verified, and trusted in a post-quantum world.

Robert Hann, Global VP of Technical Solutions at Entrust

Quantum computing doesn't only pose a risk in the future. Cybercriminals are already preparing for 'Q-Day' - the day on which quantum computers can break current public-key encryption.

Businesses need to act immediately, but with focus. Becoming crypto-agile is critical. Organisations must understand what cryptography they use, where it is deployed, and

what it protects. This visibility is essential to assess risk and prioritise change. From there, implement quantum-resistant encryption across your most critical connections.

Google recently warned that Q-Day could arrive by 2029, sooner than previously expected. This is driving “harvest now, decrypt later” attacks, where encrypted data is stolen today and decrypted in the future. Once quantum computers break current encryption, there’s no going back.

Richard Meeus, Director of Security Technology and Strategy EMEA at Akamai

---

Quantum computing will directly affect enterprise security, so organisations must start preparing for this significant change. The biggest near-term concern is not that quantum computers break everything tomorrow, but that adversaries can steal encrypted data today and decrypt it later.

Organisations should already be inventorying their cryptographic dependencies, prioritising high-value and long-term retention data, and pushing vendors for clear post-quantum migration plans. That preparation should be phased. In practice, this starts with the most exposed parts of communications security, such as key exchange in TLS/IPsec, testing in sandboxed environments to assess performance impact, and then extending across internal infrastructure and critical services that store or process the most sensitive data.

The organisations that will handle this best are the ones building crypto-agility into their infrastructure now, rather than waiting until the last minute

Neil Thacker, Global Privacy & Data Protection Officer at Netskope

---

First, conduct a comprehensive inventory of where and how encryption is used across your systems, including stored data, data in transit, devices, and vendor services. Understanding your current dependencies is essential for prioritising upgrades.

Second, engage your vendors early. Quantum resilience is not just an internal issue. Organizations need to work closely with their suppliers and partners to make sure that the broader ecosystem, including third-party platforms, is committed to migrating to post-quantum cryptography standards.

Finally, begin exploring quantum-native tools that can strengthen your security posture today. One example is Quantum Random Number Generators (QRNG), which produce truly random numbers by measuring unpredictable behaviours at the quantum level, such as how particles move or change state. Unlike traditional ‘pseudo-random’ number generators, which are based on algorithms and can be reverse-engineered, QRNGs eliminate vulnerability and offer a stronger foundation for encryption.

Rob O’Connor, EMEA CISO at Insight

Organisations need to get ready for quantum by doing the following:

1. Act now - The threat is no longer theoretical, so it's time to get familiar with blueprints and strategies that can support the right approach for your organisation. The Australian Signals Directorate (ASD) recommends that by the end of 2026, organisations should have a refined plan for their transition to post-quantum cryptography (PQC). The transition plan should account for organisations' security goals, risk tolerances, dependencies and the value of their data.
2. Replace legacy technology - Malicious actors intentionally target these systems because they have an expansive, intricate attack surface and are easier to breach. Legacy technology is already a liability, but quantum computing will accelerate the need for modernisation and the adoption of quantum-resistant solutions. Starting quantum migration early will help IT and security teams better handle the threats they face today, particularly through investments in automation.
3. Prioritise proactive cyber exposure management – Identify and execute appropriate proactive and reactive efforts to build resilience against cybersecurity threats. Traditional security approaches that are reactive, fragmented, and blind to the full attack surface are obsolete. Prioritize platforms that offer a multilayered detection engine and pre-emptive insights into vulnerabilities being actively weaponised, allowing organisations to act before attackers strike.

Nadir Izrael, CTO and Co-Founder at Armis

The greatest quantum risk isn't a decade away - it is the "harvest now, decrypt later" reality we face today. Bad actors are already stockpiling encrypted data, banking on future quantum power to render today's defenses obsolete. For most leaders, the priority shouldn't be the hardware; it must be the identity architecture.

Identity is the final control plane, and in the era of autonomous AI, that plane is expanding. Under our new Blueprint for the Secure Agentic Enterprise, we are moving the industry toward a model where every AI agent is treated as a first-class identity. If your security relies on implicit trust or long-lived tokens, you are already vulnerable to both future quantum decryption and immediate agentic action risk.

Organisations must transition to identity-first governance - providing continuous verification and a kill switch for every human and non-human identity. Hardening this foundation is the only way to build the agility required to stay ahead of the quantum threat.

Dan Mountstephen, Senior Vice President & General Manager, Asia Pacific & Japan, Okta

---

Building a crypto-agility roadmap is a must. Start with discovery: identify where legacy algorithms like RSA and ECC are used across your identity stack, from SAML signing certificates to SSH keys. Many organisations lack full visibility into their cryptographic footprint, making future transitions harder. The goal isn't immediate overhaul, but to build an architecture that supports algorithm agility i.e. the ability to swap out cryptographic algorithms without re-engineering the entire system.

It’s imperative that businesses make a start today because a recent Caltech report suggests the total number of stable Qbits required to build a fully realised quantum computer which could then be used to crack crypto algorithms is now in the range of tens of thousands - not, as previously believed, the tens of millions. That equates to a shorter runway and more aggressive timelines for achieving crypto-agility.

As quantum computing advances, make sure your vendors are preparing too. This can be achieved by adding a post-quantum cryptography (PQC) roadmap section to security vendor questionnaires and RFPs to assess vendor readiness. You should also ask your IdP, PAM, and secrets management vendors about their plans to support NIST’s standards. If a vendor lacks a PQC roadmap, it may be time to reassess their long-term fit.

Brad Bowers, Lead Field CISO Global at SHI

Honestly, it feels a lot like the millennium bug all over again. Until we have a fully production-ready quantum computer, we cannot truly understand its capabilities and limitations, and therefore we cannot be certain whether the encryption methods we are developing today are genuinely quantum-proof.

That said, NIST published its post-quantum cryptography standards in 2024, which is a meaningful stake in the ground and worth being aware of. If you don't already have an inventory of all the encryption in use across your estate, that is a good place to start, though building a complete picture across every device and application is a significant undertaking. A more pragmatic approach is to prioritise your external-facing equipment and your most sensitive internal data sources first. For each, understand which encryption standard is in use and whether it needs to be upgraded to align with the new post-quantum standards. And apply common sense to remediation: if a device is due for replacement in two years, leave it. Focus your effort where it will have the longest shelf life.

My strong view is that we have far more immediate and pressing threats to focus on, such as the speed at which AI-powered malware can swarm a network once inside. Get all of your other defences right first, and only then would I consider quantum a priority.

Jon Abbott CEO and Co-Founder at ThreatAware

Organisations should treat the quantum threat as immediate, not theoretical. Tomorrow’s quantum computers will be capable of undermining the encryption and signature algorithms that form the bedrock of digital trust, and the risk is already materialising through “harvest now, decrypt later” attacks. Preparing for this shift means beginning the transition to post-quantum cryptography now – starting with a comprehensive inventory of all cryptography-based processes and the structured planning of migration strategies across systems and devices. This is not a simple technical upgrade, but the most extensive cyber migration ever undertaken. The temptation to delay may be strong, but doing so would be a critical strategic mistake.

Benoit Jouffrey, VP Innovation & Technology for Cyber & Digital at Thales