



The Quantum Execution Gap

Key findings from DigiCert's Quantum Readiness Outlook



70%

have deployed quantum-safe or hybrid certificates on a meaningful scale.

Quantum readiness has reached an execution gap

The transition to post-quantum cryptography (PQC) is underway, but deployment isn't keeping pace. New research from DigiCert reveals that while most IT and security leaders expect today's encryption standards to be broken within the next decade and are already planning, testing, or implementing post-quantum cryptography initiatives, **only 7% have deployed quantum-safe or hybrid certificates on a meaningful scale.**

The urgency isn't driven by breakthroughs alone. Attackers are already harvesting sensitive, encrypted data with plans to decrypt it once quantum computers are capable of breaking current encryption. As concern over these "harvest now, decrypt later" (HDNL) attacks grows, protecting long-lived assets is becoming an immediate priority, not a future consideration.

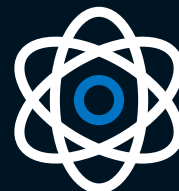
Preparing for quantum and becoming quantum ready are no longer the same thing. Bridging that gap will define the next phase of cybersecurity.

Discover how more than 1,001 IT and security leaders are approaching post-quantum cryptography, where readiness gaps remain, and the operational priorities shaping the future of cryptographic resilience.

The forces shaping the transition

Technology leaders are accelerating the transition. Google has targeted 2029 for its migration to PQC, and Microsoft has since committed to a similar strategy.

- Governments are raising expectations. A new U.S. Executive Order is accelerating the federal government's transition to PQC.
- The window to prepare is shrinking. As standards mature and adoption accelerates, organizations have less time to inventory cryptographic assets, prioritize migration, and begin deployment.



The quantum countdown has started

Key findings

85%

believe current encryption standards will be broken within a decade.



50%

More than half believe this will happen sooner, within the next five years.



7%

believe current encryption will remain secure for more than 10 years.



For most IT and security leaders, the question is no longer whether quantum computing will disrupt modern cryptography. It's how much time remains to prepare. The findings that suggest that organizations are planning against a shorter timeline than was widely assumed just a few years ago, making quantum readiness a near-term strategic priority instead of a long-term research initiative.

Tomorrow's breach could start today

Key findings



84% believe at least some of their encrypted data is vulnerable to HDNL attacks.

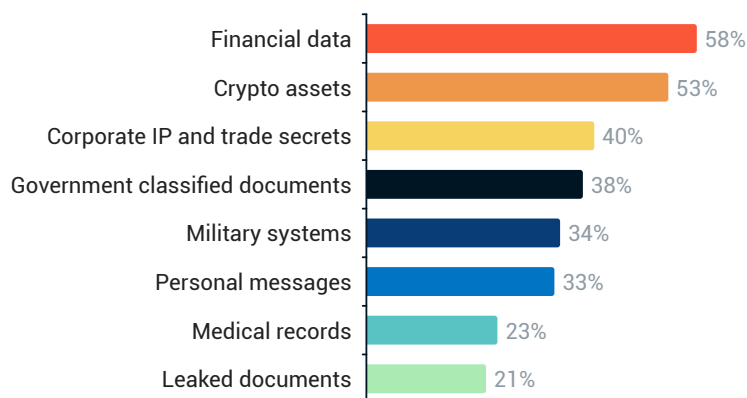


Financial transaction records and **banking data** were deemed most likely to be targeted first, followed by cryptocurrency private keys and wallets.



More than one third believe **over 25%** of their encrypted data is vulnerable.

What attackers will target first



Respondents didn't limit their concerns to traditional business data. They also pointed to politically sensitive disclosures and high-profile leaked documents like WikiLeaks-style disclosures and the Epstein files as examples of information that could remain valuable to attackers for years.

The findings underscore a broader shift in thinking. Quantum readiness is becoming as much a data protection challenge as it is a cryptography challenge, requiring organizations to identify which information must remain confidential for years, or even decades, and prioritize those assets for migration first.

The industry has moved beyond awareness

Key findings

87%

are planning, testing,
or implementing
PQC initiatives.

50%

have conducted
quantum risk
assessments.

45%

have developed
transition plans.

44%

have created
cryptographic
inventories.

The publication of the National Institute of Standards and Technology's (NIST) post-quantum cryptography standards in [August 2024](#) has given organizations a clearer path forward and accelerated planning efforts across industries.

The findings suggest that awareness is no longer the biggest barrier. More organizations are taking the foundational steps needed to support migration, from assessing quantum risk to inventorying cryptographic assets and developing transition plans.

Yet those activities haven't translated into widespread deployment. The industry has largely figured out what needs to happen next, and the challenge now is executing at enterprise scale.

Readiness is not distributed equally

Key findings

-  Preparedness varies more by **industry** than geography.
-  The **United Kingdom** reported the highest share of organizations identifying as leading edge (**18%**), followed by the **United States (17%)** and **Australia (10%)**.
-  Retail was the only major industry where more respondents reported being unprepared than highly prepared.
-  **Manufacturing** showed the greatest divide, with respondents split between feeling highly prepared and not prepared at all.

Quantum readiness varies by industry



MedTech,
+24.0



Telecommunications
& Media, **+21.6**



BFSI,
+16.2



Science &
Technology, **+16.0**



High Tech,
+13.5



Manufacturing,
+1.3



Retail,
-7.9

**Higher scores indicate industries that feel more prepared for the transition to post-quantum cryptography. Negative scores indicate being unprepared.*

The differences between industries suggest that some organizations are moving beyond planning while others remain in the early stages of the transition. As that gap widens, quantum readiness is becoming a competitive differentiator. Organizations that invest earlier in cryptographic visibility, migration planning, and crypto-agility will be better positioned to adapt as standards evolve, and customer and regulatory expectations continue to rise.

Some industries are beginning to converge a shared view of their readiness, while others remain much more divided. Yet, Manufacturing stood out as the most fragmented sector, with respondents almost evenly split between those who felt extremely prepared and those who felt not prepared at all. Retail told a different story, becoming the only major industry where more organizations reported being unprepared than highly prepared.

Complexity is the real challenge

Key findings

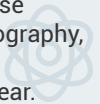
Most leaders believe it will take **3-5 years** to deploy quantum-safe encryption enterprise-wide.



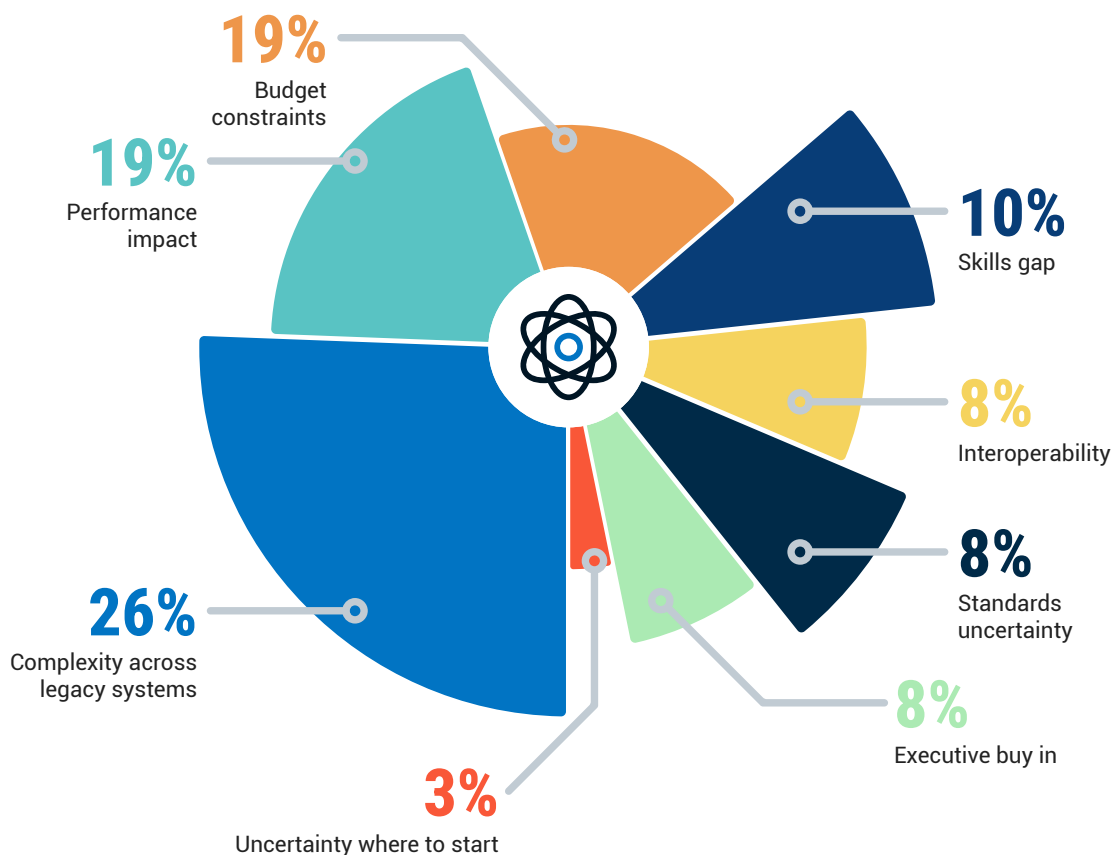
Complexity across legacy systems is the top barrier in making this happen.



Only **7%** report that more than half of their certificates currently use quantum-safe or hybrid cryptography, an increase of less than two percentage points since last year.



What's the biggest challenge organizations face in becoming quantum-safe?



The execution gap is driven by complexity, not a lack of awareness. For many organizations, PQC is no longer a technology upgrade, but a multiyear modernization effort spanning systems, applications, certificates, devices, and cryptographic assets across the enterprise.

The biggest barriers are no longer uncertainty or executive support. They're implementation complexity, performance, and budget. Organizations know where they need to go, but they're struggling with how to get there.

That's why cryptographic inventories, certificate visibility, migration planning, and crypto-agility are becoming foundational to quantum readiness. Organizations can't modernize what they can't see, and those that establish visibility early will be better positioned to prioritize migration, measure progress, and adapt as PQC becomes the new standard.

Conclusion

The research makes one thing clear: Organizations are no longer waiting for quantum computing to arrive before acting. The challenge now is whether they can complete the transition before today's encryption is broken.

That transition won't happen overnight. Most organizations expect it to take a few years, yet meaningful deployment has barely changed over the past 12 months. At the same time, industry leaders are accelerating their own timelines, and governments are beginning to mandate the transition, steadily compressing the window for action.

Organizations that begin early will have more time to discover cryptographic assets, prioritize migration, and modernize without disrupting operations. The leaders within these organizations will build the operational capabilities required to understand exposure, prioritize remediation efforts, adapt to evolving standards, and manage cryptographic change at scale. These capabilities will, in turn, also enable safe adoption of AI, reduced outages, and better crypto-agility.

Every year spent waiting leaves less time to complete the transition, while those that delay will face the same challenge under greater pressure, tighter timelines, and higher risk. The race to quantum readiness has already begun. The organizations that succeed will be the ones that start early enough to close the execution gap before they have no choice.

Moving from planning to execution

DigiCert's Quantum Central helps organizations operationalize quantum readiness through cryptographic discovery, remediation planning, readiness tracking, and educational resources designed to support the transition to PQC.

Visit Quantum Central



Methodology

This report is based on findings from an independent survey conducted by Propeller Insights on behalf of DigiCert in May 2026. The study surveyed 1,001 IT and cybersecurity decision-makers across three markets: the United States (500 respondents), the United Kingdom (251 respondents), and Australia (250 respondents).

Respondents represented organizations across a range of industries and company sizes and included professionals responsible for cybersecurity, IT infrastructure, risk management, compliance, digital transformation, and technology strategy. The survey explored organizational readiness and investment priorities related to artificial intelligence (AI), machine identity security, governance, cryptographic resilience, certificate lifecycle management, and emerging cybersecurity risks.

Data was collected through an online survey and analyzed in aggregate to identify trends, priorities, challenges, and opportunities shaping the future of intelligent trust. Percentages reported throughout this report may not total 100% due to rounding.

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management to secure infrastructure, software, devices, messages, and AI content, agents, and models. Learn why more than 125,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com

© 2026 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.