Post Quantum Cryptography

Pqc

The State of Quantum Readiness in 2024

Integration challenges, budget, and skilled labor top list of key obstacles in global survey of IT professionals.

KEYFACTOR

ACCUTIVE SECURITY

Protect Your Data Today from 'Steal Now, Decrypt Later' Attacks

Did you know that many hackers steal encrypted information because they hope to decrypt it later? To protect against "steal now, decrypt later" attacks, modern businesses have started to weave PQC into their existing technologies.

On the one hand, quantum computers hold immense potential for solving complex business problems. But their ability to break widely used encryption raises serious concerns about the security of data and critical infrastructure everywhere.

What you'll learn in this report

- How organizations are preparing for the transition to post-quantum security
- Challenges and roadblocks that must be overcome
- Tips for establishing crypto-agility
- Resources and next steps for learning more about quantum-safe cryptography

Preparation is key

Steal now, decrypt later is a very real threat. So feeling "quantum ready" is similar to how you would prepare before any predicted storm – and that's by **paying attention, planning, and fortifying your defenses**. How well you prepare today will make all the difference for your organization's future.

Every organization needs to prepare for the post-quantum future. Every industry will be affected, from government agencies and financial services to healthcare, retail, manufacturing, and more.

Yet new insights from Keyfactor and market research leader Vanson Bourne reveal that organizations are very concerned about their ability to adapt – and they all face multiple obstacles when plotting a realistic timeline. One of the main takeaways from the survey is this: quantum-readiness isn't just a "technology problem" but rather, it's a fundamental change in how businesses operate.

Ready to learn more? Let's dive into the PQC survey results.

Exploring the State of Quantum Readiness in 2024

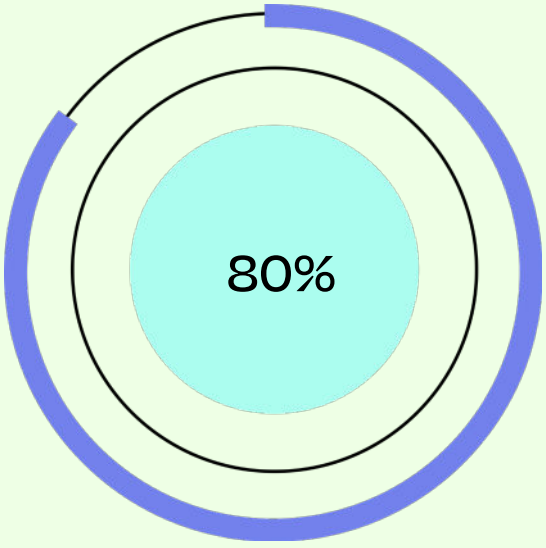
It's the topic on everyone's minds – how are we preparing for PQC?

That's why in the yet-to-be-released PKI & Digital Trust Report, Vanson Bourne's industry researchers added a new section devoted entirely to understanding how global organizations are addressing post-quantum readiness.

In this snippet report, you'll see a sneak peek of a few of the PQC-related questions that will be featured in Keyfactor's forthcoming deep dive into PKI & Digital Trust. The data is based on 1,200 interviews from IT security professionals working in all major industries in the U.S., Canada, and Europe.

The following questions look at how companies are preparing for changes in cryptography, their obstacles, their timelines, and their action steps!

01. My organization is concerned about the ability to adapt to risks and changes in cryptography.



Key takeaway

Most respondents are concerned about the future. Indeed, 80% agree or strongly agree they are concerned about the ability to adapt to risks and changes in cryptography.

02.

What primary obstacles, if any, is your organization encountering in the process of getting ready for PQC?

Difficulty in finding skilled personnel for PQC initiatives

43%

Lack of executive support

31%

Uncertainty regarding the pace of PQC adoption

43%

Limited budget and resources for PQC implementation

45%

Lack of understanding of PQC

37%

Regulatory or compliance concerns

38%

Integration challenges with existing security infrastructure

44%

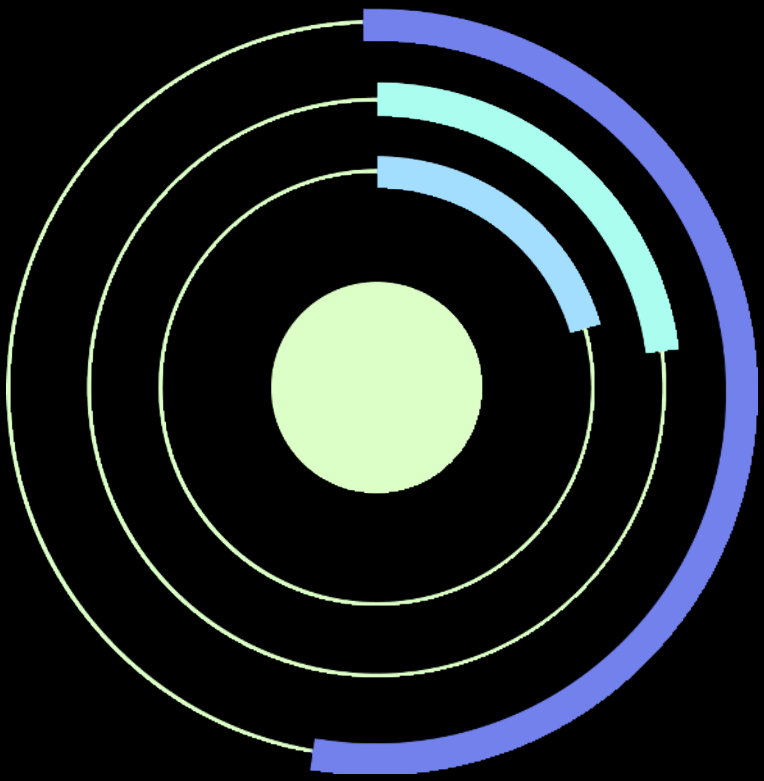
Key takeaway

Respondents revealed that significant challenges stand in the way of PQC readiness. IT and security teams will be hard-pressed to acquire the skills and knowledge required to implement new standards. One of the biggest challenges will be interoperability between servers, applications, HSMs, and other critical infrastructure.

03.

How long do you believe it will take your organization to transition to PQC?

TOTAL : **1 163** | MEAN : **4**



1-2 years **(23%)**

2-5 years **(57%)**

5-10 years **(20%)**

More than 10 years **(0%)**

Don't know **(0%)**

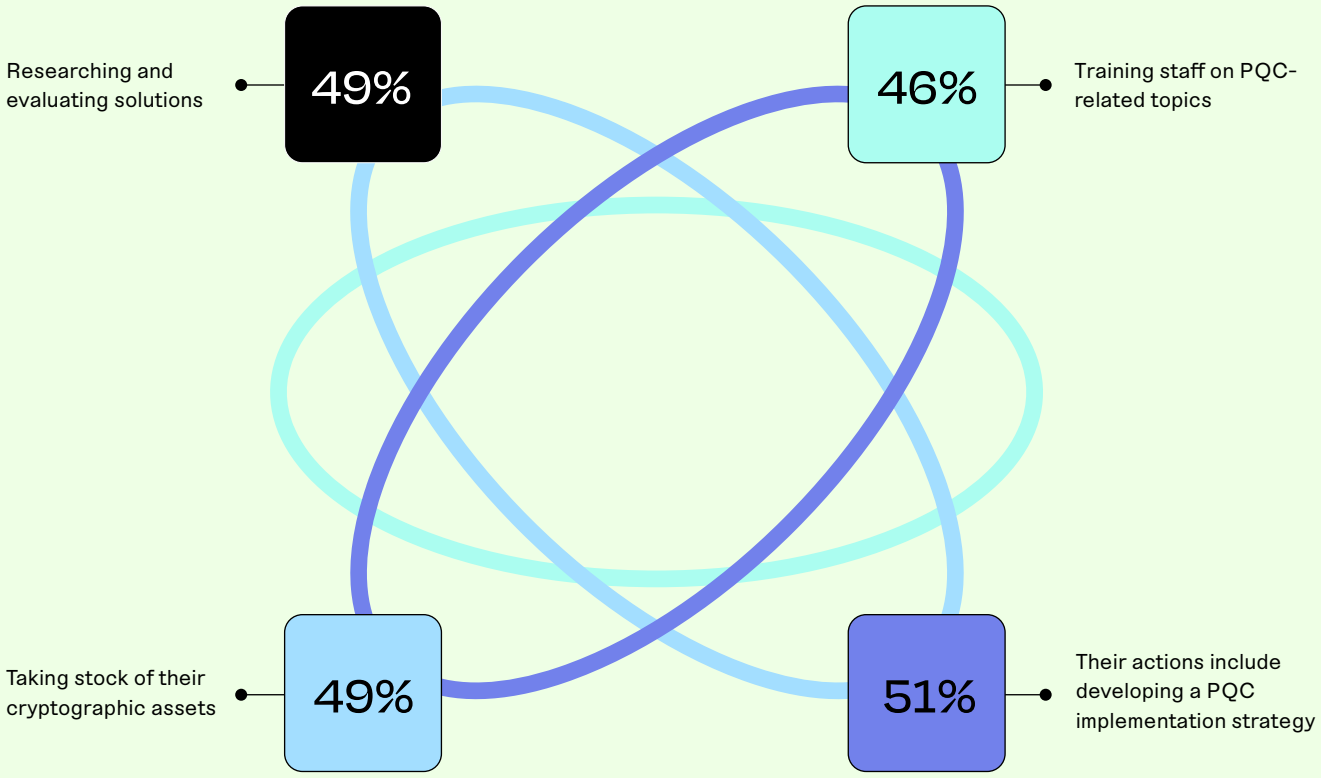
Key takeaway

The transition to quantum-ready security has only just begun. It will take years to accomplish. Think about the more than decade-long transition from SHA-1 to SHA-2. Many organizations still have SHA-1 in use in their environment, despite NIST announcing end of life in 2011. The transition to PQC will be on an entirely different scale.

04.

What actions is your organization taking, if any, to prepare for PQC?

As mentioned earlier, quantum-readiness isn't just a technology problem - it's a fundamental change in how businesses operate. So, it might be helpful for you to see the **top four things** that respondents are doing.



Key takeaway

These core activities will all help survey respondents prepare for PQC. The even better news? They're also activities that YOU can start doing too. For example, have you taken an inventory of all cryptographic assets, including keys, certificates, and algorithms? Have you considered how you'll train staff? Remember -- these new algorithms impact everything, which means that everyone is going to have to understand this.

Quantum Readiness: The Time to Prepare is Now

The PQC wave is on the horizon. While organizations have their sights set on what's coming, most aren't prepared to adapt – despite repeated warnings about "steal now, decrypt later" threats.

The biggest challenges that stand in their way are integration complexities, budget woes, a steep learning curve, and general uncertainty.

And the question of "when" to prepare is most certainly a challenge, as survey results indicate that global organizations across many industries are underestimating the scope and the timing for post-quantum readiness.

"NIST and other government agencies have repeatedly warned to take risk assessment and planning seriously," says **Chris Hickman**, **Chief Security Officer at Keyfactor**. "Regardless of whether we can estimate the arrival of the quantum computing era, we must prepare our information security systems to be able to resist quantum computing."

Despite these timeline snafus and delays, Hickman says it's promising to see that many organizations are beginning to take their first steps – planning, getting to know their environment, and better understanding these new algorithms and what they mean for their business.

> Shifting to new **quantum-era cryptographic algorithms** will take more than flipping a switch, and many are starting to realize it.

Hickman adds that when quantum computing becomes available, vulnerabilities will spring up quickly. Due to "steal now, decrypt later" risks, he says his goal is for everyone to start making changes as quickly as possible, because the risks go beyond integration and compatibility in their ecosystem.

"There are already hostile hackers and groups using exfiltration attacks to gather data today that could one day be valuable. On top of that, we have the challenge of skills shortages – that means finding people who understand this and upskilling personnel you already have. The reason why everyone has to 'get it' is because these new algorithms impact everything. Everyone must understand the changes coming."

Planning for Post-Quantum Starts Today

01.

Know what you have

Your first step is to build an inventory of all keys, certificates, protocols, and the applications that use them. This will help you prioritize where to focus first by the sensitivity of data and infrastructure.

02.

Build your plan

Next, you'll need to prioritize where to focus first, and map out a strategy for the transition. This is where testing begins, getting hands on with new PQC standards to test for compatibility, performance, and implementation.

03.

Begin the transition

This will take time and careful execution, but done right, and you'll be well on your way to quantum-readiness. Automation will be critical for this step, making it easier to migrate to new standards, such as re-issuing and deploying certificates from a new PQC-capable PKI.

Final Thoughts: Prepare Now or Panic Later

Ready or not, a new era is on the horizon. As you better understand, you can't wait for a quantum computer to pose a real threat. (If you did, you would be years behind!)

The biggest takeaway is that the transition to new quantum-resilient algorithms isn't just a technology problem. Rather, it's an organizational change and a fundamental shift in how we operate. It's not only upskilling and training your staff, it's also evaluating new tools and standards, and it's testing and working with these algorithms in a safe environment to begin understanding them.

Ready to learn more?	**Recommended exploring >** PQC Playground	**Recommended reading >** Whitepaper
	Explore **PQC Labs** and get hands-on with post-quantum cryptography so you can be PQC ready.	Learn more about what this means for your organization and how to take first steps: **Planning Ahead for Post-Quantum Cybersecurity**