digicert®

POST-QUANTUM CRYPTOGRAPHY

RESULTS FROM PONEMON'S GLOBAL STUDY ON QUANTUM PREPAREDNESS

As quantum computing advances, IT professionals face the challenge of preparing for attacks that can easily break today's strongest encryption technologies. Post-Quantum Cryptography (PQC) can protect data and assets from quantum threats, but as Ponemon found, IT professionals around the world are looking for solutions to issues like awareness, resources, and organizational policy gaps.

BIG PICTURE

1,426 Total IT and IT security practitioners surveyed

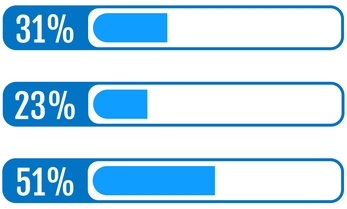
61%

61% concerned their org won't be prepared to address quantum threats

74% concerned about "Harvest Now, Decrypt Later"

ROADBLOCKS

Most IT professionals are aware of the dangers of quantum threats, but the process of building and running quantum security is challenged by organizational awareness and buy-in.



31% say their org isn't taking any steps to prepare for quantum attacks

Only **23%** say their org currently has a strategy for addressing quantum threats

51% say the biggest roadblock to implementing PQC is a lack of resources (time, money, knowledgeable personnel)

CRYPTO-ASSET VISIBILITY & MANAGEMENT

Cybersecurity experts agree the first step in implementing effective PQC is inventorying all crypto-assets in the organization.

65% say the increase in the use of cryptographic keys and certs has increased operational burdens

61% say their org is deploying more keys and certificates

58% say their org doesn't know how many keys and certificates it has in use

TAKEAWAYS

1. Now is the time to define your transition to quantum-safe.
2. Organizations need to assign clear ownership of PQC implementation.
3. Investing in cryptographic agility today is critical.

[See the full study here.]

digicert®

WANT TO LEARN MORE ABOUT HOW TO PREPARE FOR THE QUANTUM-SAFE TRANSITION?

READ STUDY

Statistics and findings are the result of a Ponemon Institute study, sponsored by DigiCert.