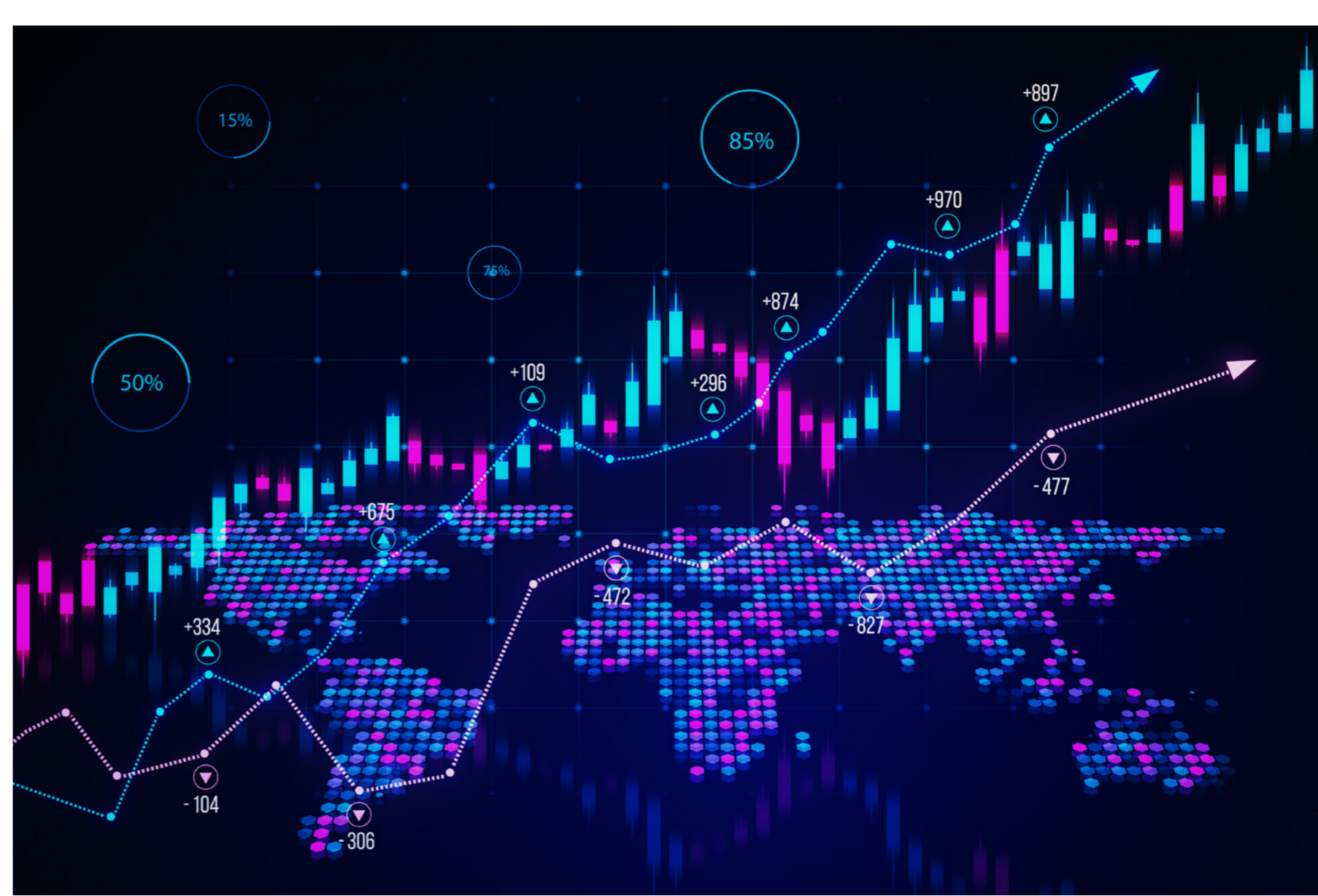


The Upcoming Cryptographic Transformation:



8 Important Facts about Post-Quantum Cryptography

With the release of the PQC algorithm standards from NIST, some organizations are starting to think about the upcoming overhaul to their cryptography. But when should one begin? Here are some key stats to help you assess when it's time to start.



2026 is the year that organizations in Code Signing, Secure Communications, and IoT need to be able to comply with regulations around **Post-Quantum Cryptography**.¹

Risk:

77% of organizations feel underprepared or completely unprepared for cybersecurity threats²

25% of bitcoins and **65%** of ether coins are currently vulnerable to a quantum attack, putting more than **\$40 billion** of value at risk³

4.35 M is the average cost to an organization if there is data breach³

Data that needs to be protected for **10 years** is susceptible today, including bank and financial data, private communications, personal health data, intellectual property, and much more³



Organizational Readiness:

55.5% rank PQC in their top 2 of greatest sources of emerging concern to their security program⁴

62% of enterprises have at least 5 enterprise key management systems adding to the complexity, presenting a serious challenge for establishing PQC and crypto agility⁵

73% recognize quantum is a threat, but only **39%** are working on a plan⁶

3.5 years: The average length of time for an organization to make changes to its cryptography⁷

At Thales, we believe the time to start getting ready is now.

But don't panic, prepare.

Take our free **5 minute PQC Risk Assessment** or learn more at <https://cpl.thalesgroup.com/encryption/post-quantum-crypto-agility>

¹ CSA_CNSA_2.0_ALGORITHMS_PDF (defense.gov)
² The State of Security Remediation 2024 | CSA (cloudsecurityalliance.org)
³ WEF_Translating to a Quantum Secure Economy_2022.pdf (weforum.org)
⁴ S&P Global Report for Thales for the 2024 Data Threat Report
⁵ 2023 Data Threat Report
⁶ 2024 Thales Post-Quantum Cryptography e-Book
⁷ Transitioning organizations to post-quantum cryptography | Nature