EXECUTIVE SUMMARY

2024 PKI and Post-Quantum Trends Study

Sponsored by Entrust

Independently conducted by Ponemon Institute LLC

Publication Date: October 2024

ENTRUST
SECURING A WORLD IN MOTION

Ponemon INSTITUTE

Contents

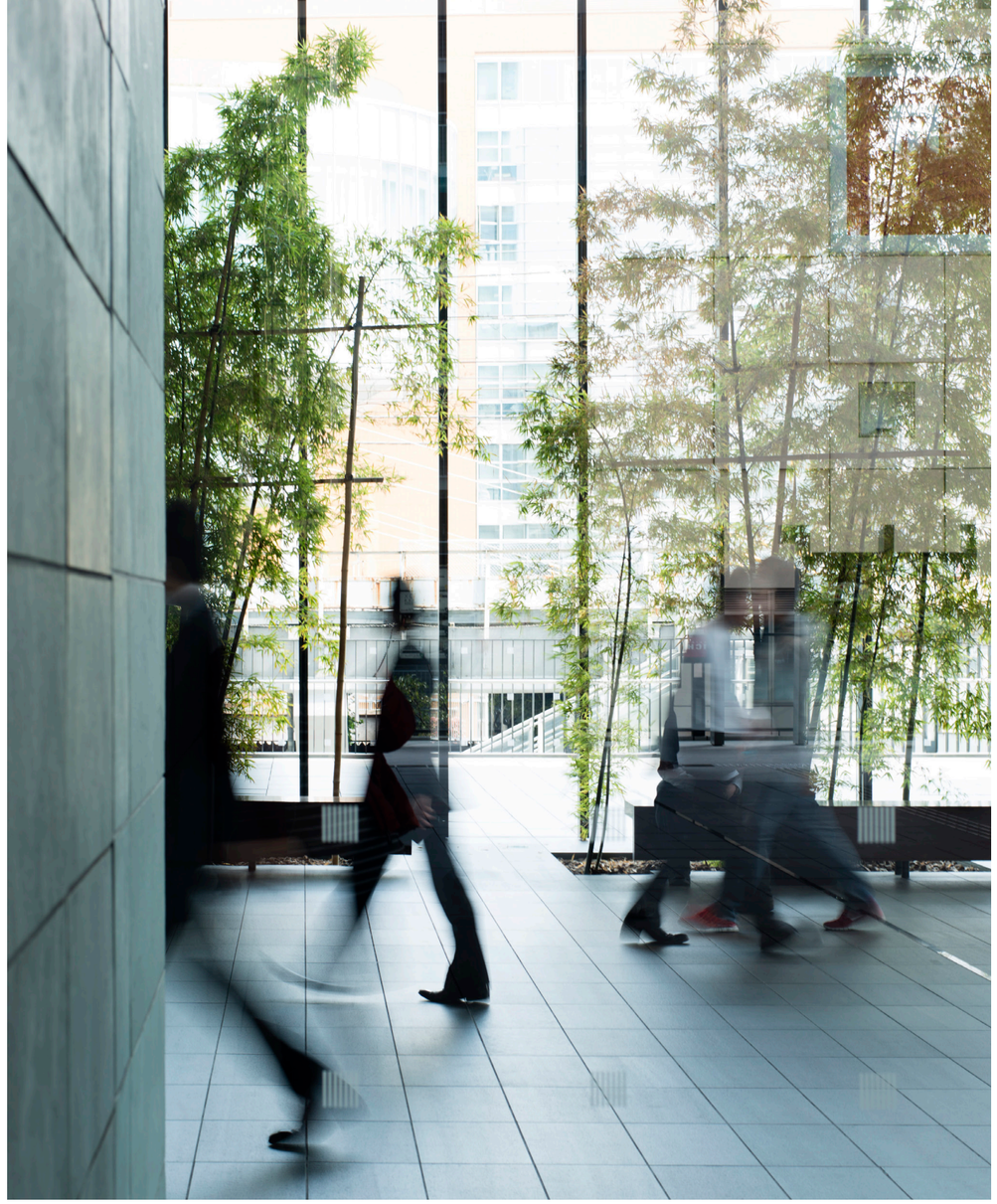
Minding Your Ps and Qs in the Post-Quantum Era

Quantum computing promises to revolutionize many industries – from healthcare and defense to finance and transportation. Yet it's also poised to disrupt conventional cryptography, threatening the world's economy, security, and even stability.

In many ways the post-quantum (PQ) era is already here with "Harvest Now, Decrypt Later" attacks that target long-life data like financial records and government intelligence. And the U.S. National Institute of Standards and Technology (NIST) has just released the first three post-quantum cryptography (PQC) standards to help organizations navigate their own PQC journey.

So, as the PQ era dawns, the conversation is quickly shifting from the "when" of PQ to the "hows" and "whats" of PQ. With that lens, the Entrust Cybersecurity Institute is pleased to highlight the results of our PKI and Post-Quantum Trends Study – conducted by Ponemon Institute – that delves into organizational PQ preparedness and the future of encryption.

For this study, the Ponemon Institute surveyed 2,176 IT and IT security practitioners across nine countries/regions: the United States, United Kingdom, Canada, Germany, United Arab Emirates, Australia/New Zealand, Japan, Singapore, and the Middle East.

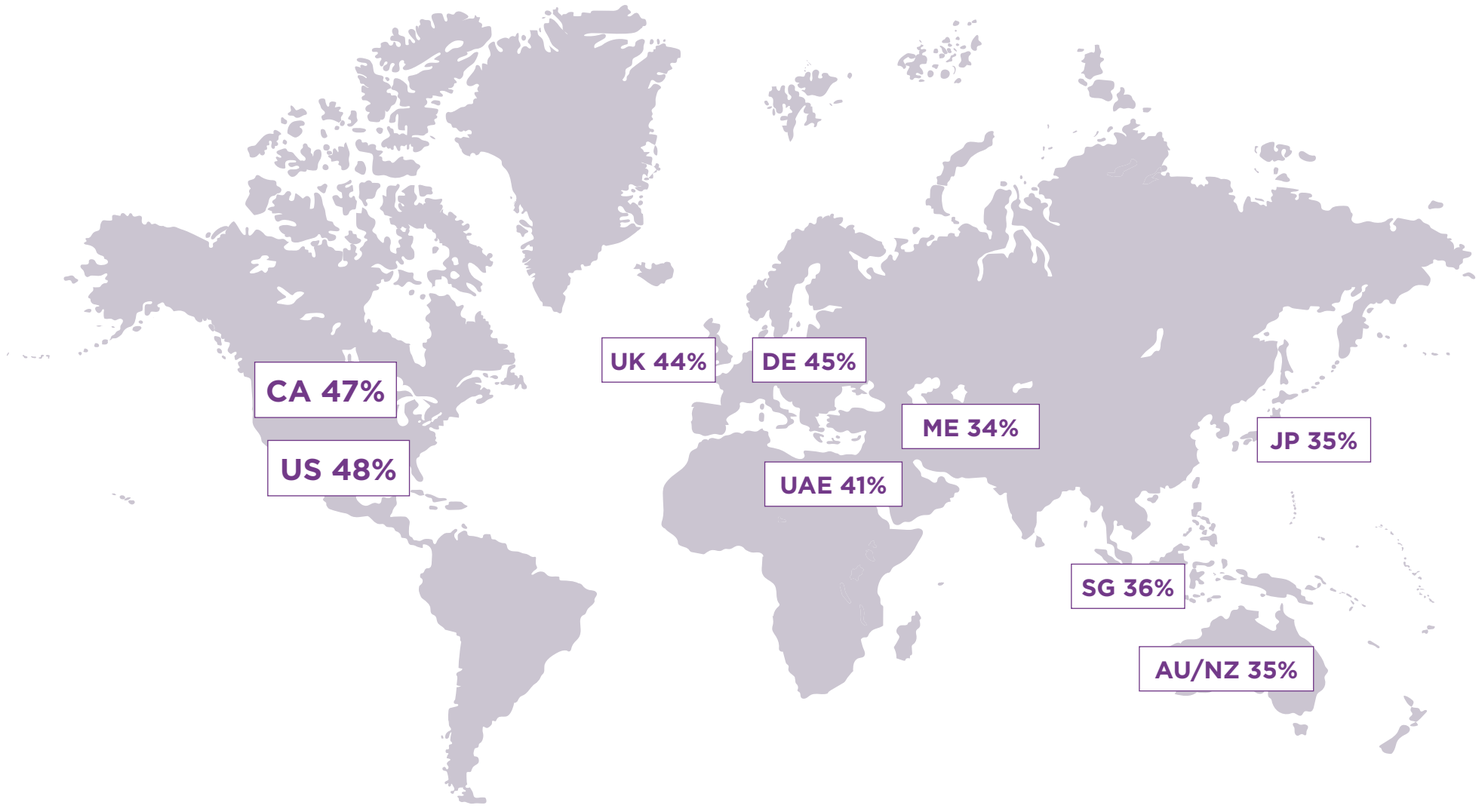


U.S. Leads in PQ Preparedness

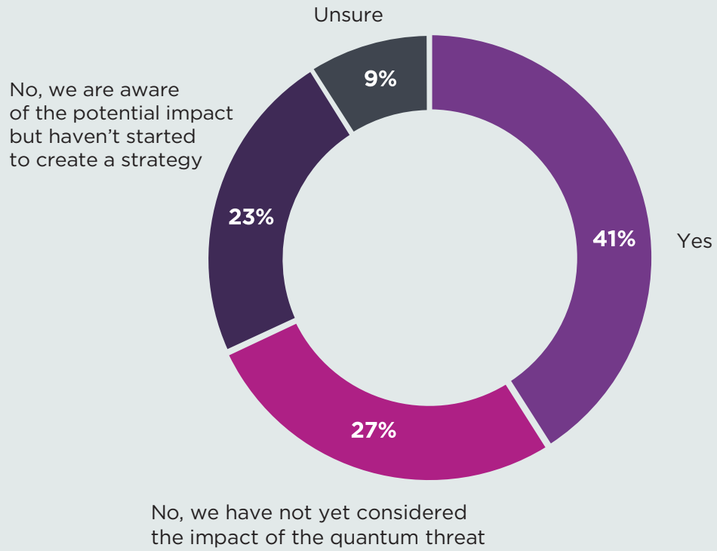
Post-quantum presents an almost existential threat with the potential for significant disruption, but also too big for many organizations to conceive – let alone prepare for.

Less than half of organizations globally (41%) are actively preparing for PQ, ranging from a high of 48% in the U.S. to just 34% in the Middle East. The quasi-good news is that another 23% have at least evaluated the potential impact – led by Canada (34%) and the U.S. (33%). However, it's disconcerting that 27% of organizations have not even considered the potential impact of the quantum threat, although that number is much lower in the U.S. (12%) and Canada (15%). It's also concerning that 9% of respondents are unsure if/what to even do regarding PQ.

The answers below represent a geographic breakout of who answered “Yes” to the question in the chart to the right sidebar.

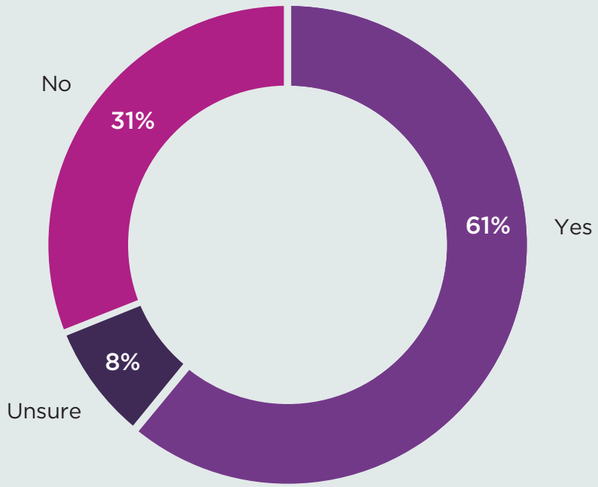


Is your organization preparing for the quantum threat?

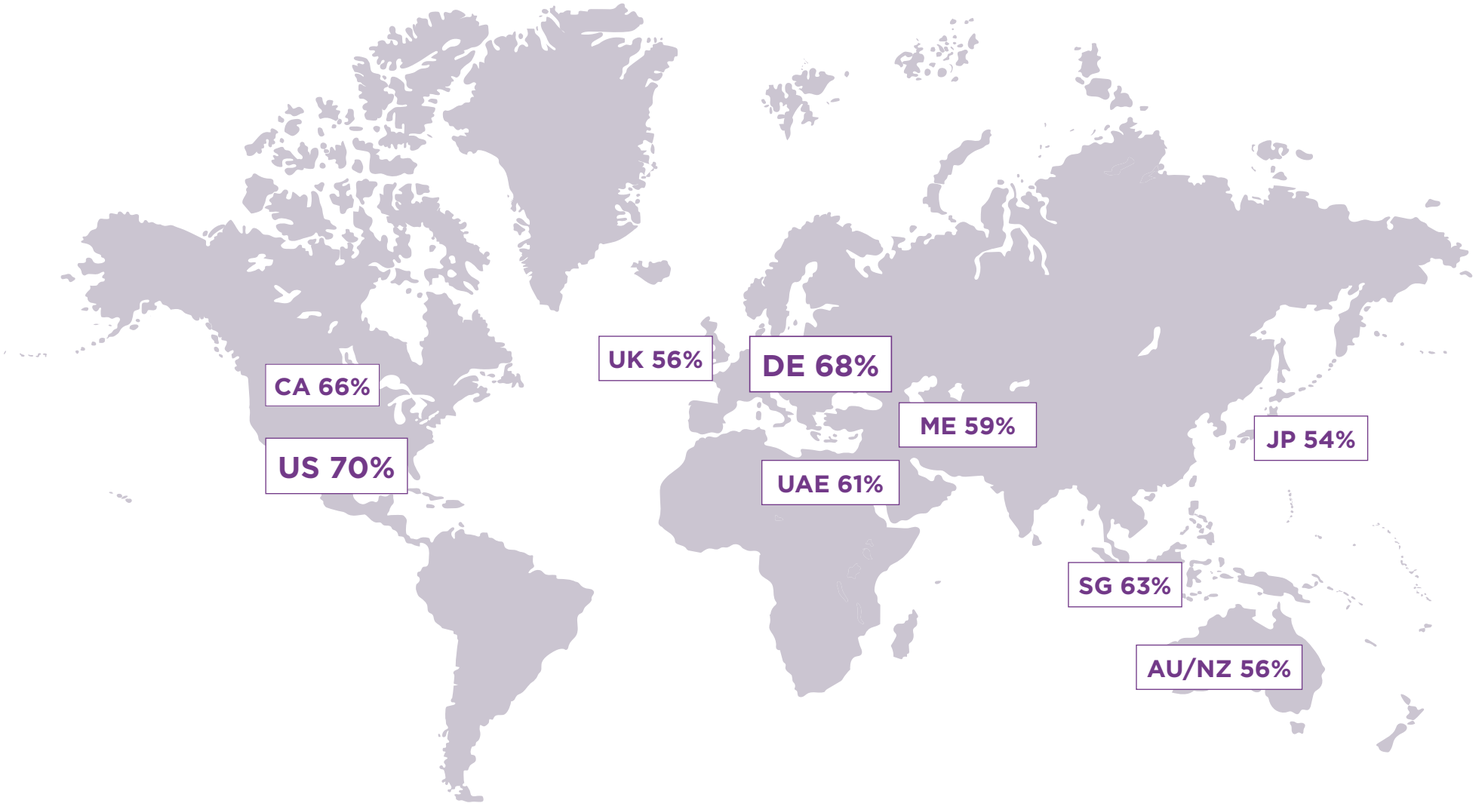


The majority of CISOs know PQ is on the horizon, with 61% of global organizations planning to migrate to PQC within the next five years. However, close to a third (31%) have no such plans. This trend is relatively consistent across the surveyed countries, with the U.S. being ahead of the curve with 70% citing PQC migration plans.

Does your organization plan to migrate to PQC within the next five years?



The answers below represent a geographic breakout of who answered "Yes" to the question in the chart in the left sidebar.



PQ Headwinds

For those preparing for the quantum threat, the majority are focused on building their cryptographic strategy (44%) and agility (37%). But there are some significant headwinds, with 43% of organizations globally concerned about their inability to improve the discovery/inventory of their crypto assets – let alone manage them. In fact, this was a top-three concern for seven of the nine countries/regions in this study. Plus, 40% of organizations globally expressed considerable concern around the security of proposed new PQC algorithms.

Another recurring concern for 38% of global respondents is not having the right scale and technology to support the extra computing power required for PQC, with this being the top concern in Australia/New Zealand, Japan, and Singapore. Also, 37% globally cited the inability to have an enterprise-wide strategy as a key concern – even higher for organizations in the U.S., UK, UAE, Singapore, and Australia/New Zealand.

Somewhat surprising, "Harvest Now, Decrypt Later" attacks are at the bottom of the global list of concerns at 24%, which is relatively consistent across countries.

Top concerns about the quantum threat and migration to PQC

1. Inability to improve the discovery/inventory of our cryptographic assets
2. Newly proposed PQ cryptographic algorithms may not be secure after deployment
3. Inability to support the extra computing power required for PQC
4. Inability to have an enterprise-wide strategy

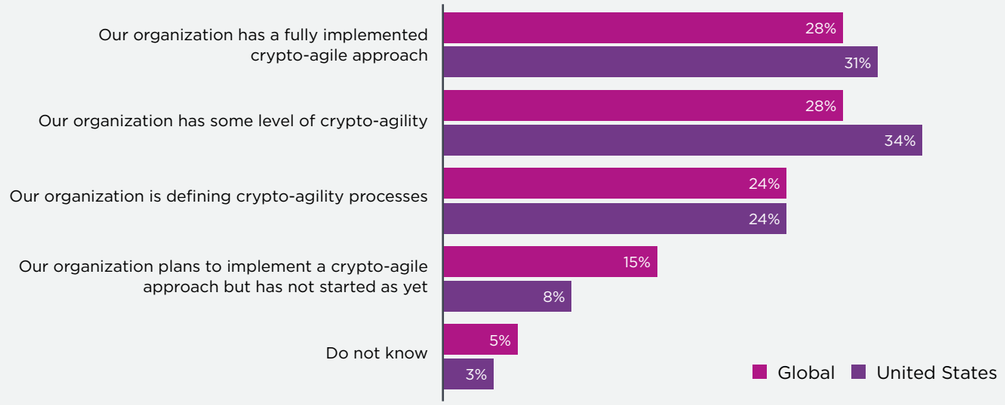
Getting Crypto-Agile

Preparing for PQC starts with taking an inventory of your cryptographic assets and ensuring they are crypto-agile. But you can't manage what you can't see! So, it's a little concerning that less than half (45%) of organizations report having full visibility into their entire cryptographic estate across environments.

The good news is that 80% of organizations are doing "something" to improve crypto-agility, with a relatively even global split between a fully implemented crypto-agile approach (28%), some level of crypto-agility (28%), and those defining crypto-agility processes (24%).

In general, U.S. organizations are the most prepared, with 89% doing something, including 34% with some level of crypto-agility and 31% fully implemented.

What is the current state of your organization's crypto-agility?



Get the Full Report

Thank you for reading the executive summary. Download the full Ponemon PKI and Post-Quantum Trends Study for a deeper dive into the survey results.

Download Report

ABOUT ENTRUST

Entrust is an innovative leader in identity-centric security solutions, providing an integrated platform of scalable, AI-enabled security offerings. We enable organizations to safeguard their operations, evolve without compromise, and protect their interactions in an interconnected world – so they can transform their businesses with confidence. Entrust supports customers in 150+ countries and works with a global partner network. We are trusted by the world's most trusted organizations.

entrust.com | Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION