Cambridge Quantum

PRESS RELEASE

Cambridge, United Kingdom
Thursday, February 3rd 2022

IN GLOBAL SURVEY, CYBERSECURITY PROS FEAR A SURPRISE QUANTUM ATTACK

yet only 1 in 5 are prepared

(origin)CQ

In a report issued by Dimensional Research for Cambridge Quantum, 75% acknowledge quantum attacks will defeat current encryption but only 13% have purchased products to fight the threat

PRESS RELEASE
Cambridge, United Kingdom
Thursday, February 3rd 2022

A global research survey of information security professionals released today found that most believe advancing technologies will break longstanding encryption standards within the next two years. Professionals said most organizations are currently unprepared to defend against encryption attacks but plan to be by 2023.

Conducted in October 2021 by Dimensional Research for Cambridge Quantum (now part of the newly formed company Quantinuum), the report evaluated the opinions of more than 600 cybersecurity professionals across industry and government.

Key highlights include

- 70% of respondents expect new and evolving technologies will compromise existing encryption approaches
- 75% acknowledged that quantum-enabled attacks will defeat current encryption techniques
- 80% of respondents are worried that a quantum-enabled attack could occur "without warning"
- 49% plan to purchase quantum security solutions as part of their strategic plan.

PRESS RELEASE
Cambridge, United Kingdom
Thursday, February 3rd 2022

The report found that only 21 percent of security professionals surveyed feel prepared for advancing encryption attacks while another 38 percent say their organizations will be ready within the next two years. However, just one in five indicate any budget allocation to address the issue and even fewer have started researching quantum threats and possible solutions.

With nearly half indicating they are quantum security knowledgeable, the key challenges cited in building a quantum defense include lack of in-house expertise, immature solutions, and undefined post-quantum encryption algorithms. Just 13 percent have purchased a solution to start enabling a quantum defense.

"Cybersecurity professionals appear to appreciate the advancing threat to current encryption standards and say they will be ready in time. However, there appears to be little real movement within organizations towards preventing a potentially catastrophic loss of critical data, despite the associated financial and legal consequences," said Duncan Jones, head of quantum cybersecurity for Cambridge Quantum.

Jones said the strategy being implemented by adversarial nations and other bad actors to steal encrypted communications today for later decryption with quantum computers should especially concern those organizations required to protect critical data over several years or more. 86% of respondents confirm they adhere to regulations requiring critical data protection for an extended period with nearly half needing to protect data for five years or more.

"Organizations with data in the cloud or IoT devices in the field should move quickly to strengthen encryption against existing threats as well as those posed by quantum attackers in the future," Jones said. "Financial institutions, healthcare, governments and other entities protecting critical data should ensure their security foundation is as strong as possible today, as well as future-proofed for tomorrow."

Jones said organizations can move towards using post-quantum algorithms, such as those being standardized by the NIST post-quantum cryptography process, as well as consider bolstering current encryption defenses by leveraging quantum-enhanced cryptography.

To review the full report, click here.

dimensional research

ABOUT DIMENSIONAL RESEARCH

Dimensional Research® provides practical market research for technology companies. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and provides business growth. Our researchers are experts in the applications, devices, and infrastructure used by modern businesses and their customers.

FOR MORE INFORMATION

DimensionalResearch.com

ABOUT CAMBRIDGE QUANTUM

Founded in 2014, Cambridge Quantum is a global leader in quantum software and quantum algorithms, enabling clients to achieve the most out of rapidly evolving quantum computing hardware. It is part of the newly formed Quantinuum, the world's largest, integrated quantum computing company.
Cambridge Quantum has offices in Europe, USA, and Japan.

FOR MORE INFORMATION

CambridgeQuantum.com
LinkedIn
Access the source code for lambeq, TKET, Python bindings and utilities on GitHub