Q-Day Cometh: PQC Attack Protection Is Here

This Summer, the U.S. National Institute of Standards & Technology (NIST) will publish its first set of Post-Quantum Computing (PQC) standards. The time is now to do your due diligence on the most trusted PQC attack prevention and protection tools and solutions. Many corporations, such as Honeywell, have partnered with Quantinuum to fortify their critical infrastructure against PQC attacks. We are proud to connect with Quantinuum to offer the very best quantum-resistant CyberCloak™ capabilities to guard against the inevitable Q-Day onslaught.

"Quantum science suggests the existence of many possible futures for each moment of our lives. Each future lies in a state of rest until it is awakened by choices made in the present."

Gregg Braden

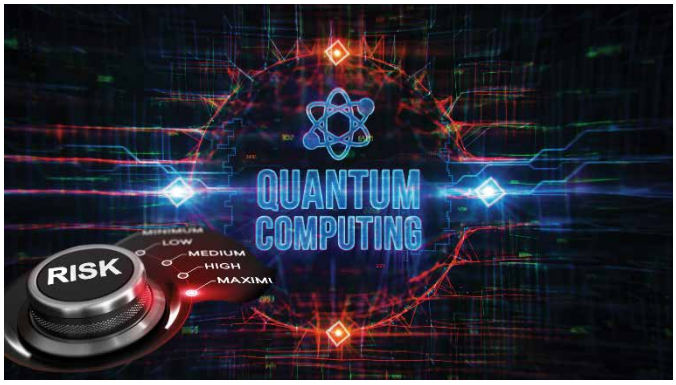
First – What is it?

Quantum computing harnesses the principles of quantum mechanics to process information in fundamentally different ways compared to traditional computing. Unlike classic computers, which use bits to represent data as 0s or 1s, quantum computers use quantum bits, or qubits, that can exist simultaneously in multiple states (0, 1, or both 0 and 1) thanks to a property called superposition. Additionally, qubits can be entangled, allowing them to be interconnected in ways that provide exponential increases in processing power. This enables quantum computers to solve complex problems much more efficiently than their traditional counterparts, potentially revolutionizing fields such as cryptography, material science, and artificial intelligence.

For those of us in the cybersecurity industry, this means that cyber criminal can do more harm faster. ***BEWARE***: the data they are harvesting now will be corrupted on Q-Day.

What and When is Q-Day?

Q-Day refers to the moment when sufficiently large quantum computers become capable of breaking modern encryption algorithms by utilizing multi-state qubits to execute Shor's algorithm. This event poses significant implications for data security, as many current cryptographic schemes could be rendered obsolete, necessitating the development of new quantum-resistant encryption methods.



Estimates regarding the timing of an actual Q-Day attack range from 5 to 20 years, depending on which source or expert you're consulting. It also depends largely on when quantum computers can crack the challenge of factoring a 2048-bit key.

Perspective for TODAY

Amidst the justifiable alarmism surrounding the growth of quantum computing, there are measures that organizations can take today to protect their critical infrastructure against the inevitable PQC attacks.

- Deploy quantum resistant solutions that have overlay architectures to protect your critical assets and data NOW! The goal of quantum cyber attackers is to steal and compromise massive amounts of personal and corporate data all at once. They're working to this end every day/minute.

- Secure your networks and data using quantum-resistant cryptography TODAY. Proper protection now is insurance. It builds trust within customers and the general public.

> ***"Unless companies are securing their networks and data using quantum-resistant cryptography, they will be opening themselves and their customers up to compromise."***
> Michael McLaughlin (Interview w/Dan Lohrman – GovernmentTechnolgy –

Blue Ridge Networks, Inc. & Quantinuum

Quantinuum brings impressively effective quantum-safe encryption with the highest quality entropy to guarantee that keys are truly unpredictable. Our collaboration enables us to enhance the encryption security of our CyberCloak™ capabilities with near-perfect randomness. This ensures quantum resistance and secure remote access. In short, your data today and tomorrow are protected against PQC attacks. Continued innovations in partnership with Quantinuum yield solutions that are bolstered with cryptographic keys that offer protection for personal identifiable information (PII), financial records, patient/healthcare data, and government/military technical assets.

Learn more about our quantum-resistant LinkGuard™ solution.

About Us

Blue Ridge Networks, Inc., is a proven and trusted provider of effective CPS/OT/IT cybersecurity solutions. Our zero-trust quantum resistant "CyberCloak™" capabilities are protocol agnostic, compatible with legacy systems, and deploy quickly with minimal overhead. We protect continuous operations by enabling secure remote access while preventing external network infiltration and mission-critical data exfiltration.

Regulated, Commercial, and Industrial organizations have trusted Blue Ridge Networks for over 20 years to prevent exploits and receive continuous returns on their investments while achieving uninterrupted operational efficiency.

BLUERIDGE® NETWORKS

1-800-704-5234
sales@blueridgenetworks.com
BlueRidgeNetworks.com