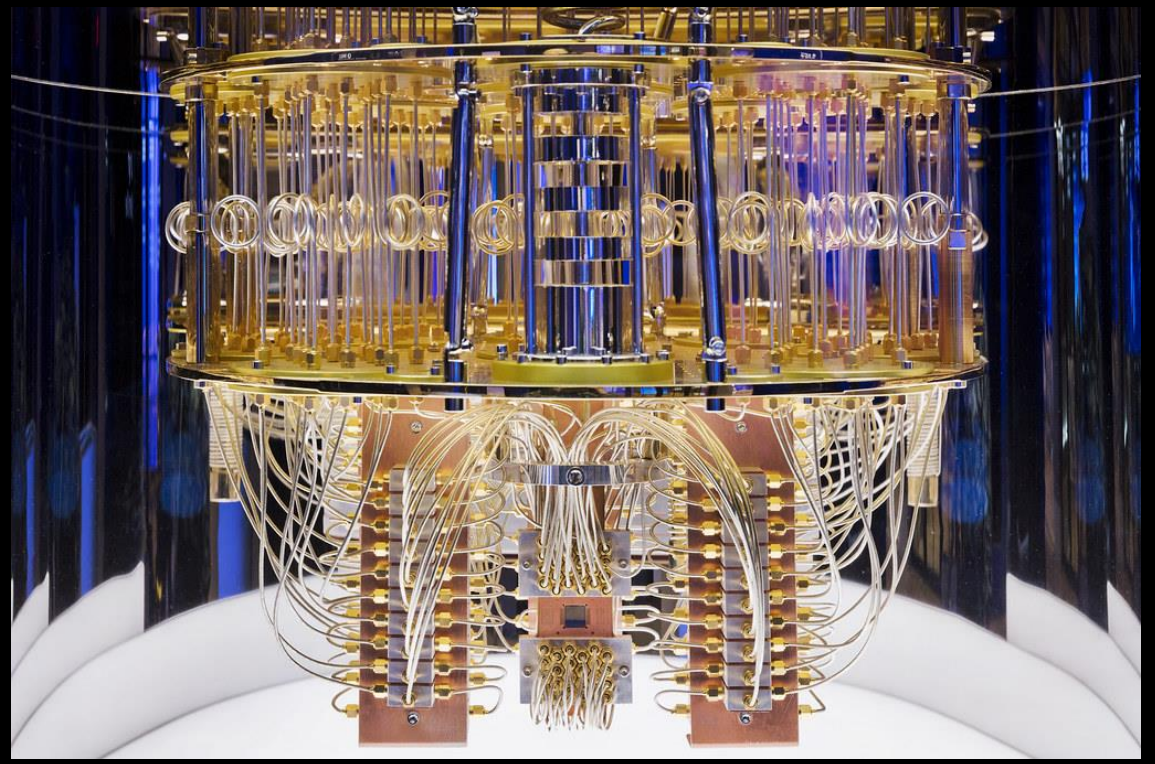
SECURING ASSETS IN THE POST QUANTUM ERA FOR TRAVELERS INSURANCE

Sam Oakes, Anthony Scardigno, Maniraj Chahal, Ryan Novara

WHAT IS QUANTUM COMPUTING ?

- What is it? Quantum computing is a computing that allows significantly faster processing in comparison to classical computing.
- How is it different? Regular computers use bits. Quantum computers use qubits with superposition and entanglement instead.
- Importance? Quantum computing allows us to solve problems that regular computers can't, such as being able to brute force secure facilities with significantly less resources, time, and energy.
- Challenges? The physical aspect of qubits make them difficult to use in quantum computers.



HARVEST NOW DECRYPT LATER

Adversaries will collect encrypted data

Personal information, policy details, claims information, payment information, etc.

Once quantum computers become available, they will decrypt

Information stolen holds its value

How an HNDL Attack Works (A 2-Pronged Approach)

Nation-State Actor

Your Data

Data Storage

Step 1: An attacker steals your cryptographically secured data and stores it on a server they control.

Step 2: An attacker uses quantum computing capabilities to decrypt your stolen data, which they can then use, barter, or sell to other cybercriminals for nefarious purposes.

Decrypted Data

Quantum Computer

POST QUANTUM CRYPTOGRAPHY ALGORITHMS

Crystals-Kyber

Crystals-Dilithium

AES (larger key sizes)

HOW TO IMPLEMENT PQC METHODS

1. Understand the Need
2. Recognize Key Areas
3. Choose PQC Method
4. Train Staff
5. Maintenance

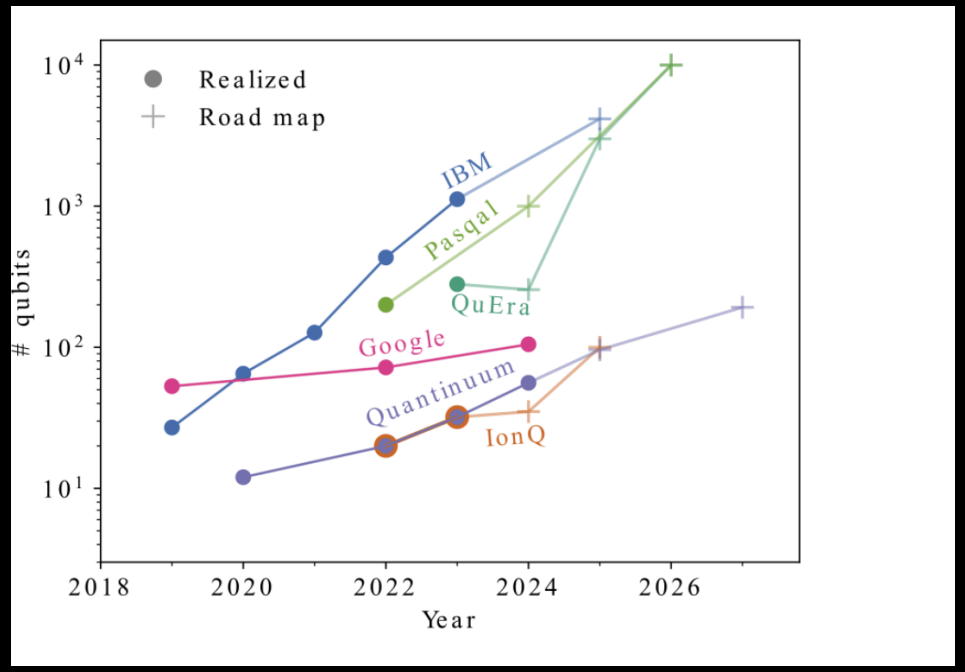
"DEFEND DIAMONDS LIKE DIAMONDS AND PENCILS LIKE PENCILS"

- DAVID PALMBACH
CYBER SECURITY ADVISOR (CSA) FOR CONNECTICUT
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)

IMPACT ON BUSINESS

- Protection against identity theft, identity fraud, and corporate espionage
- Even with a quantum computer, adversaries will not be able to decrypt data
- Boosts client trust
- Secure transactions for processing claims, managing policies, and client communications.
- Mitigates risk from attacks that could halt business and lead to profit loss

QUANTUM OVER TIME



- According to NIST, quantum computing devices with encryption-breaking capabilities could be developed within the next decade, posing a threat to the "security and privacy of individuals, organizations, and entire nations." (Source: "US unveils new tools to withstand encryption-breaking quantum")

BUSINESS CONTINUITY

- If unprepared adversarial attacks in the PQE could cripple or completely halt business for lengthy periods of time
- Ensuring an applicable BCP is in place as well as proper standards and regulations that align with secure quantum practices is vital
- Could lead to detrimental consequences and massive profit loss

LOSS OF DATA

- Vulnerabilities in the classical cryptography could lead to severe data loss for clients and the business
- Loss of customer data could lead to lack of trust from consumers
- Data loss could also lead to heightened ransomware attacks thus having to pay out money to adversaries to ensure business continuity

CHEAPER NOW VS. LATER (COMPETITIVE ADVANTAGE)

- Open-source methods (Open Quantum Safe, and OpenSSL library)
- No risk now, only gain
- Costs now include, licensing fees, development costs, or consulting fees from cybersecurity providers such as AWS(Amazon Web Services)
- Costs later will include all listed above including a charge for the encryption method itself
- As quantum becomes more powerful prices will increase for encryption implementation through supply and demand
-

REGULATIONS

- Complying with *Goverenence Risk & Compliance regulations* to avoid legal complications
- Avoiding lawsuits and class actions by customers over privacy violations and data loss
- Getting ahead of *PQC* allows *Goverenece Risk & Compliance* and legal departments time to learn about the area and be prepared

CUSTOMER TRUST AND REPUTATION

- Unmatched data security
- Trust through transparency
- Customer loyalty
- Distinguishing brand value
- “81 percent of respondents agreed that the way an organization treats personal data is indicative of how it views and respects its customers.” – 2022 Cisco Customer Privacy Survey

CALL TO ACTION

- Advancements in Cyberattacks
- Sensitive Data in the insurance sector
- Data protection
- Competitive advantage

WHY YOU SHOULD CARE

We don't know exactly when quantum systems might be powerful enough to crack 2048-bit cryptography, but some experts have sketched out timelines based on what we know so far.

The National Institute of Standards and Technology (NIST)'s *Report on Post-Quantum Cryptography* found that the first breaches might come as soon as 2030.[1]

"I have estimated a one in seven chances that some of the fundamental public-key cryptography tools upon which we rely today will be broken by 2026," wrote Dr. Michele Mosca, an expert from the University of Waterloo, "and a 50% chance by 2031."[2]

- WHILE QUANTUM COMPUTERS ARE NOT YET READILY AVAILABLE THE DEVELOPMENT AND USE OF THEM WILL BECOME MORE PREVALENT IN THE NEXT DECADE

- PREPARING AND BEING KNOWLEDGEABLE ON THE SUBJECT NOW CAN SAVE TIME, MONEY AND RESOURCES AS WELL AS MINIMIZING THE POTENTIAL THREAT LANDSCAPE FOR YOUR BUSINESS

Thank you!

Questions?