Post Quantum World & Zero Trust

Presenter: Mamdouh Al-Gendy

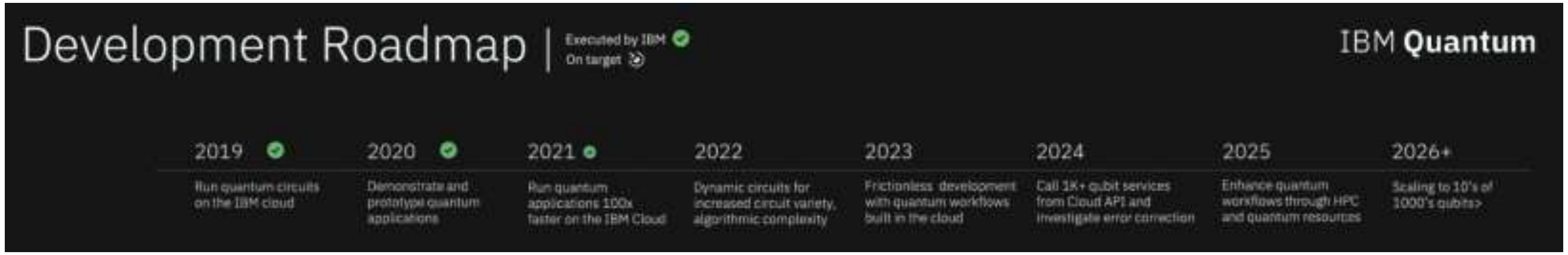
June 2023

ENTRUST

SECURING A WORLD IN MOTION

Quantum Computers: Richard Feynman (1959)

SCALED QUANTUM COMPUTERS ARE ON THE HORIZON



Development Roadmap | Executed by IBM ✓ On target

IBM **Quantum**

2019 ✓
Run quantum circuits on the IBM cloud

2020 ✓
Demonstrate and prototype quantum applications

2021 ●
Run quantum applications 100x faster on the IBM Cloud

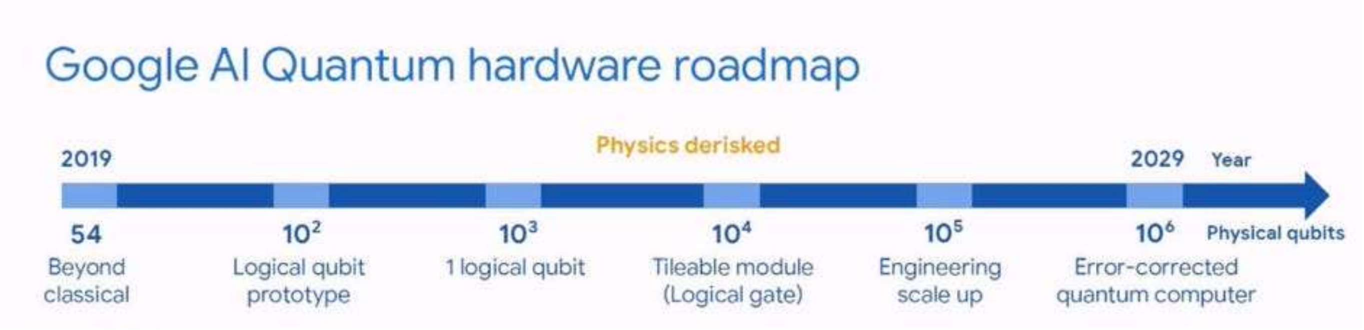
2022
Dynamic circuits for increased circuit variety, algorithmic complexity

2023
Frictionless development with quantum workflows built in the cloud

2024
Call 1K+ qubit services from Cloud API and investigate error correction

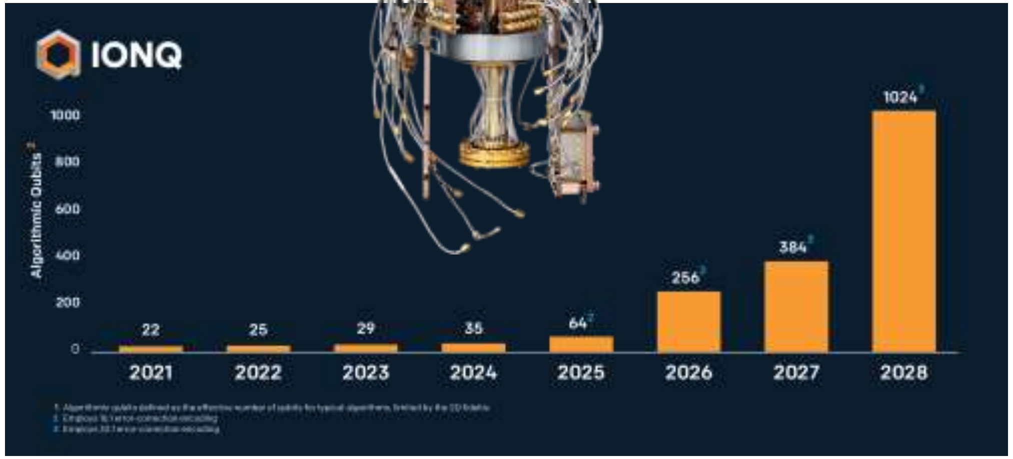
2025
Enhance quantum workflows through HPC and quantum resources

2026+
Scaling to 10's of 1000's qubits>



Google AI Quantum hardware roadmap

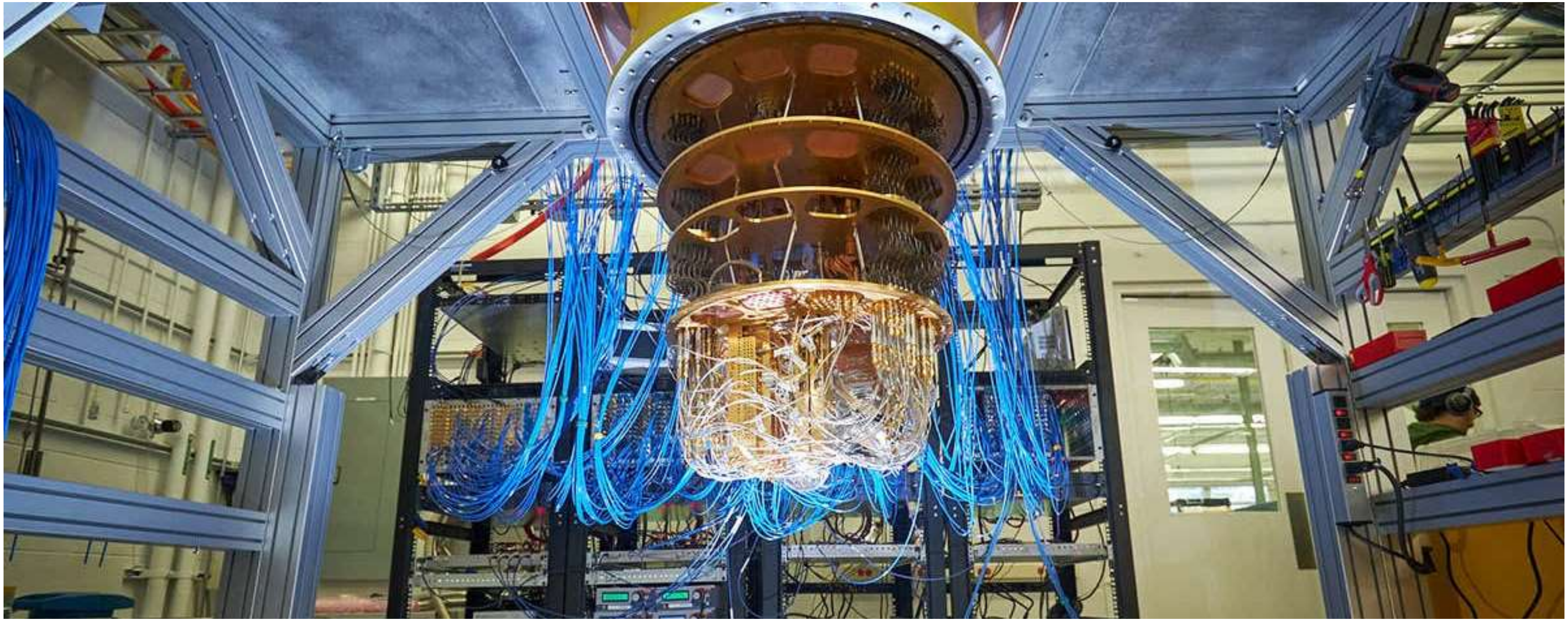
Rigetti Aspen-11



1. Algorithmic qubits defined as the effective number of qubits for typical algorithms, limited by the 2Q fidelity
2. Employs 16:1 error-correction encoding
3. Employs 32:1 error-correction encoding

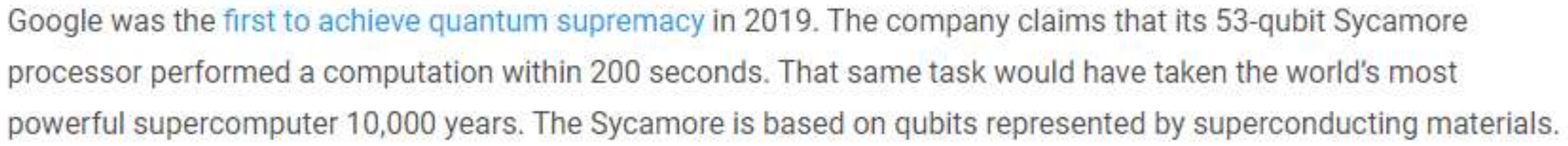
ENTRUST

Sycamore Quantum Computer

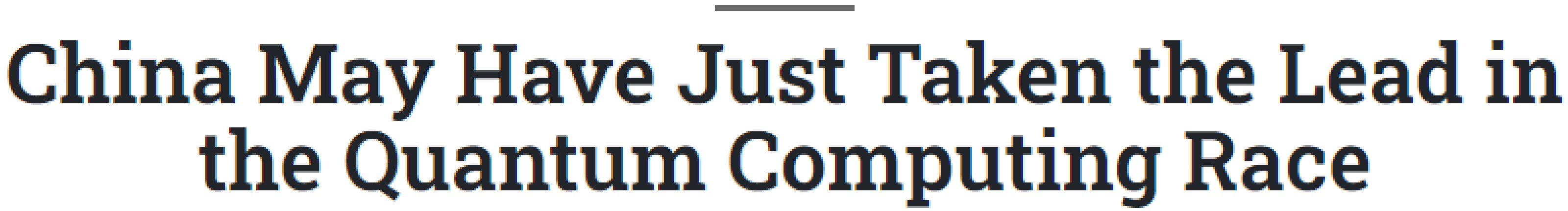


100,000 Billion Times Faster Than Today's Best Supercomputers.

Quantum Computers? What’s Going On!!!



Google was the first to achieve quantum supremacy in 2019. The company claims that its 53-qubit Sycamore processor performed a computation within 200 seconds. That same task would have taken the world’s most powerful supercomputer 10,000 years. The Sycamore is based on qubits represented by superconducting materials.



China May Have Just Taken the Lead in the Quantum Computing Race

China’s 66-qubit quantum computer reportedly completed the same task 1 million times faster.

How Much Does a Quantum Computer Cost?

A quantum computer cost billions to build.

However, China-based Shenzhen SpinQ Technology plans to sell a $5,000 desktop quantum computer to consumers for schools and colleges. Last year, it started selling a quantum computer for $50,000.

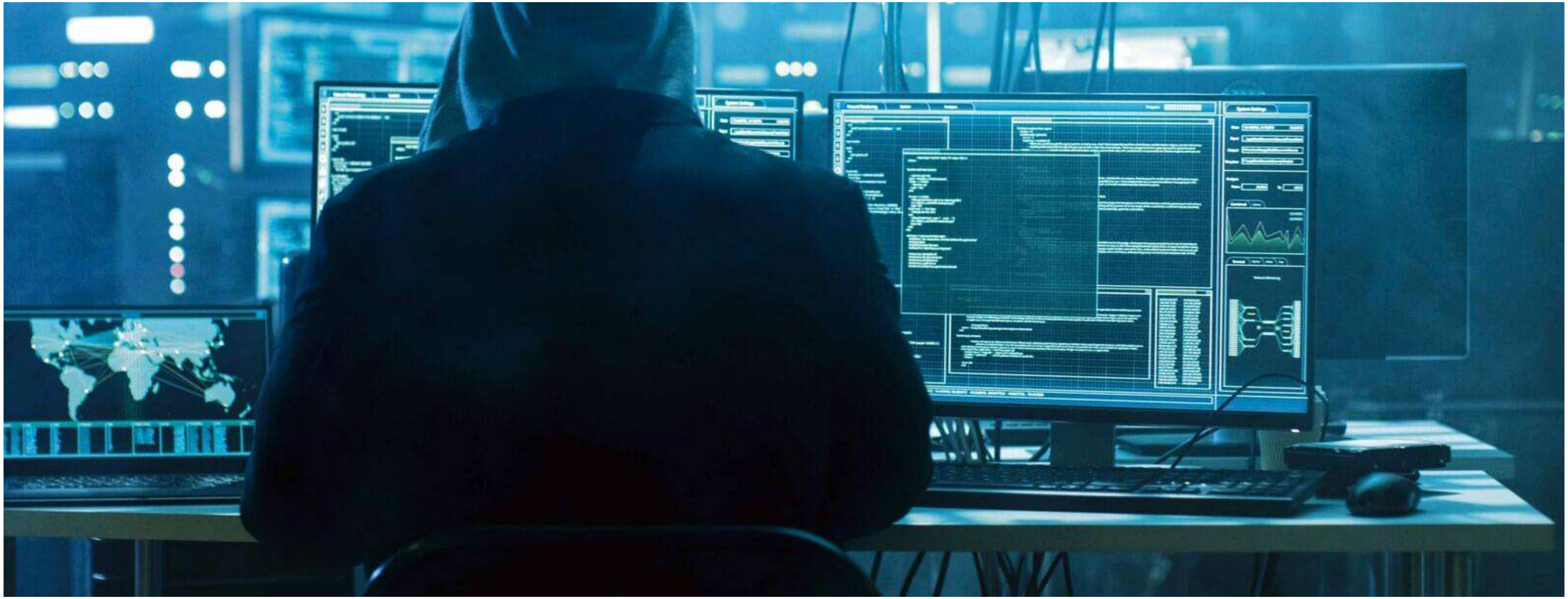
ENTRUST

The Potential Of A Better Future

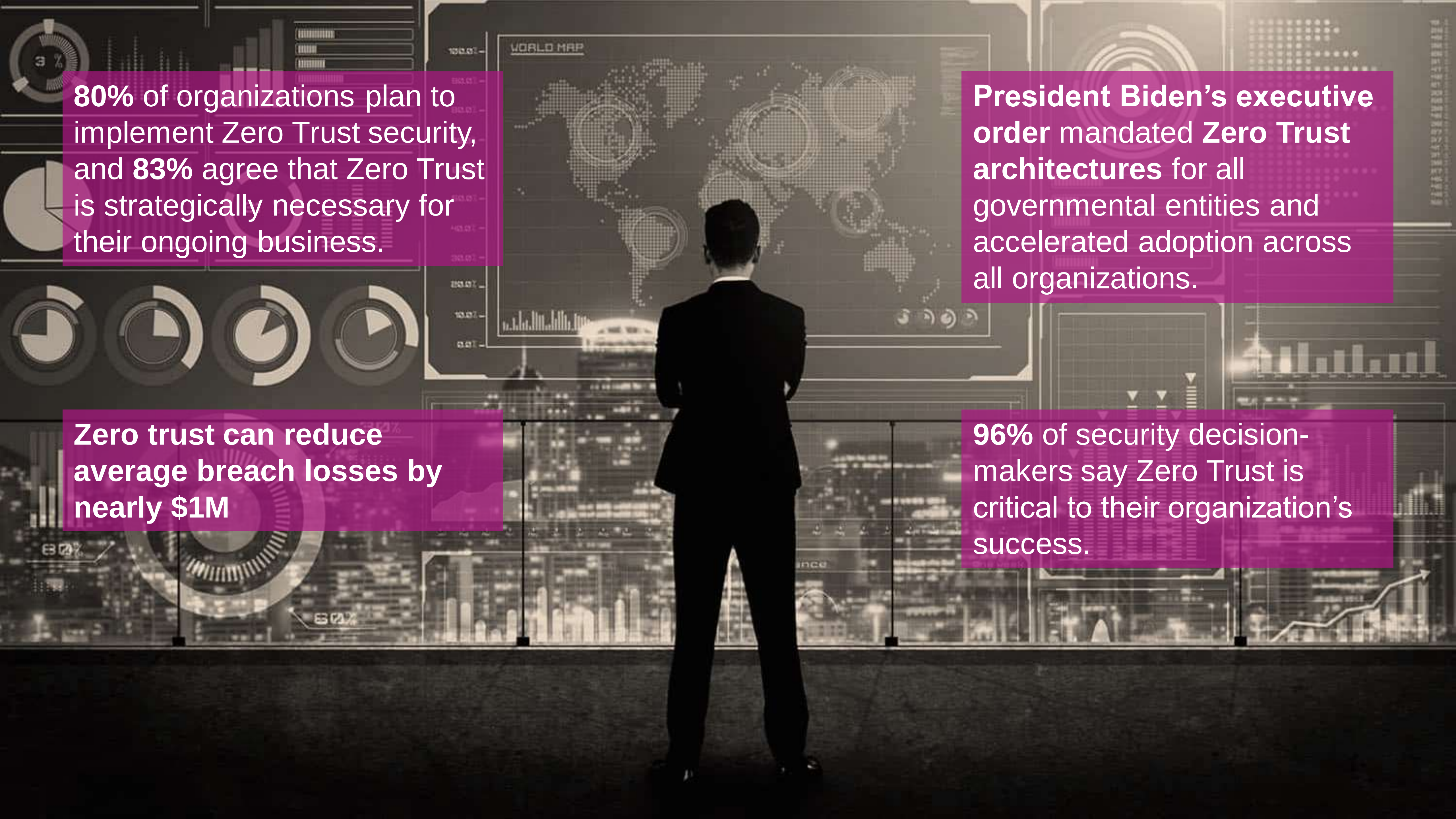
```
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
```

ENTRUST

What Are The Cyber Risks In The Future?



ENTRUST



80% of organizations plan to implement Zero Trust security, and **83%** agree that Zero Trust is strategically necessary for their ongoing business.

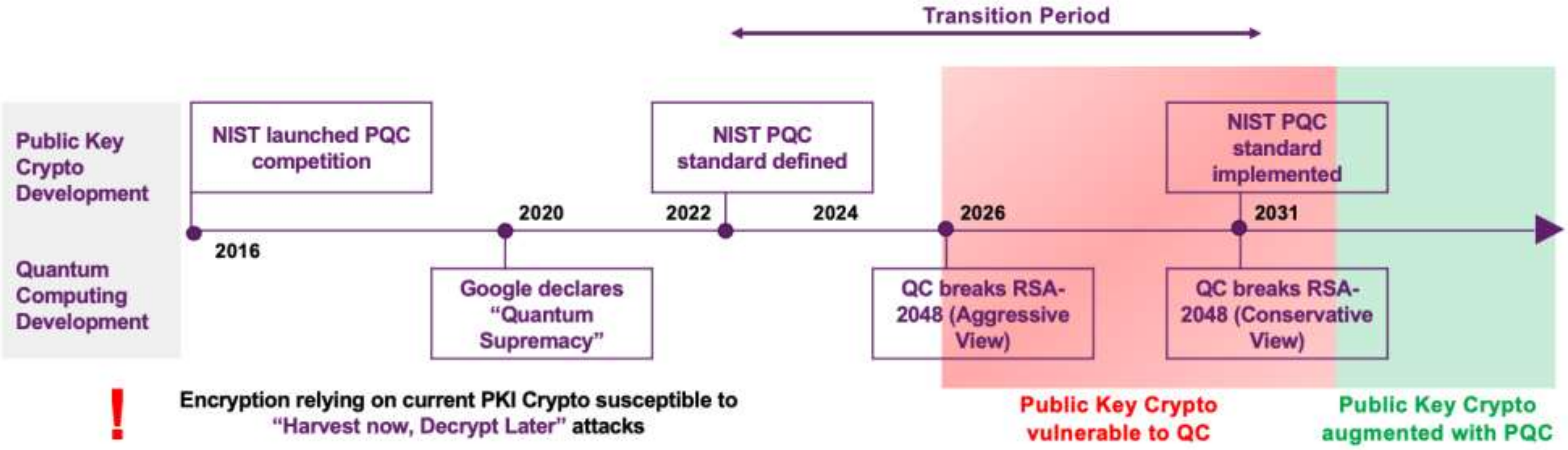
President Biden's executive order mandated **Zero Trust architectures** for all governmental entities and accelerated adoption across all organizations.

Zero trust can reduce average breach losses by nearly $1M

96% of security decision-makers say Zero Trust is critical to their organization's success.

QUANTUM THREAT AND EXPECTED TIMELINE

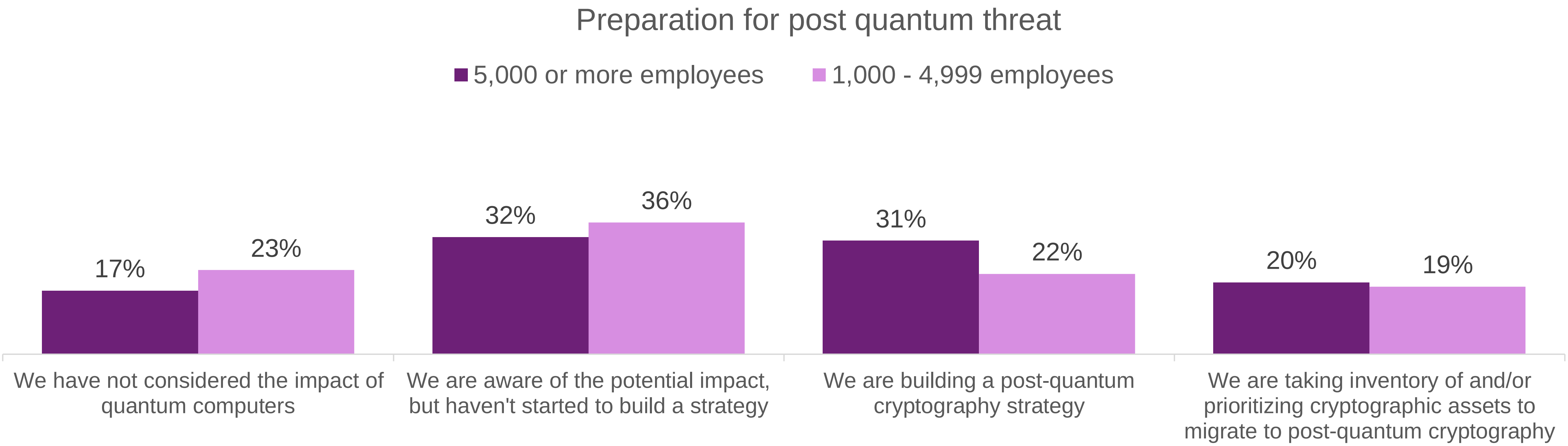
- Quantum computers will be able to break current public key encryption
- Accurate crypto inventory & mitigation strategies are required
- Long term data needs to be protected not then, but now
- Failure to migrate leaves applications and data at risk of compromise.



Transition Period
Public Key Crypto Development
Quantum Computing Development
NIST launched PQC competition
2016
2020
Google declares "Quantum Supremacy"
2022
NIST PQC standard defined
2024
2026
QC breaks RSA-2048 (Aggressive View)
2031
NIST PQC standard implemented
QC breaks RSA-2048 (Conservative View)
!
Encryption relying on current PKI Crypto susceptible to "Harvest now, Decrypt Later" attacks
Public Key Crypto vulnerable to QC
Public Key Crypto augmented with PQC

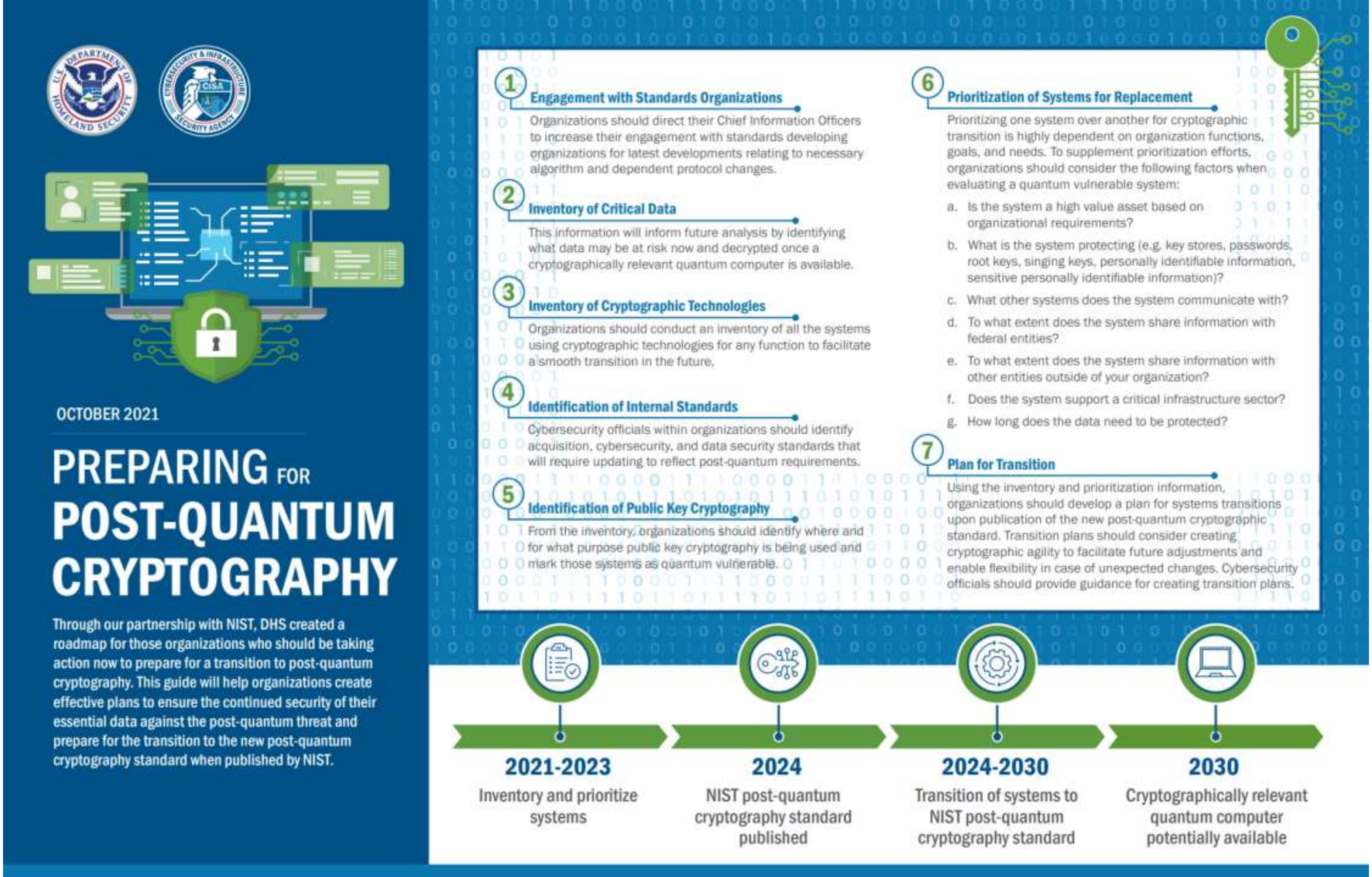
PQ PREPAREDNESS – MARKET INFORMATION

Quantum computers are in development and experts predict that they will be able to crack standard encryption methods within the decade. How if at all is your organization preparing for post quantum threat?



The majority of organizations have not yet started taking steps to prepare for PQ, they need to

ENTRUST



OCTOBER 2021

PREPARING FOR POST-QUANTUM CRYPTOGRAPHY

Through our partnership with NIST, DHS created a roadmap for those organizations who should be taking action now to prepare for a transition to post-quantum cryptography. This guide will help organizations create effective plans to ensure the continued security of their essential data against the post-quantum threat and prepare for the transition to the new post-quantum cryptography standard when published by NIST.

1 Engagement with Standards Organizations

Organizations should direct their Chief Information Officers to increase their engagement with standards developing organizations for latest developments relating to necessary algorithm and dependent protocol changes.

2 Inventory of Critical Data

This information will inform future analysis by identifying what data may be at risk now and decrypted once a cryptographically relevant quantum computer is available.

3 Inventory of Cryptographic Technologies

Organizations should conduct an inventory of all the systems using cryptographic technologies for any function to facilitate a smooth transition in the future.

4 Identification of Internal Standards

Cybersecurity officials within organizations should identify acquisition, cybersecurity, and data security standards that will require updating to reflect post-quantum requirements.

5 Identification of Public Key Cryptography

From the inventory, organizations should identify where and for what purpose public key cryptography is being used and mark those systems as quantum vulnerable.

6 Prioritization of Systems for Replacement

Prioritizing one system over another for cryptographic transition is highly dependent on organization functions, goals, and needs. To supplement prioritization efforts, organizations should consider the following factors when evaluating a quantum vulnerable system:

a. Is the system a high value asset based on organizational requirements?

b. What is the system protecting (e.g. key stores, passwords, root keys, singing keys, personally identifiable information, sensitive personally identifiable information)?

c. What other systems does the system communicate with?

d. To what extent does the system share information with federal entities?

e. To what extent does the system share information with other entities outside of your organization?

f. Does the system support a critical infrastructure sector?

g. How long does the data need to be protected?

7 Plan for Transition

Using the inventory and prioritization information, organizations should develop a plan for systems transitions upon publication of the new post-quantum cryptographic standard. Transition plans should consider creating cryptographic agility to facilitate future adjustments and enable flexibility in case of unexpected changes. Cybersecurity officials should provide guidance for creating transition plans.

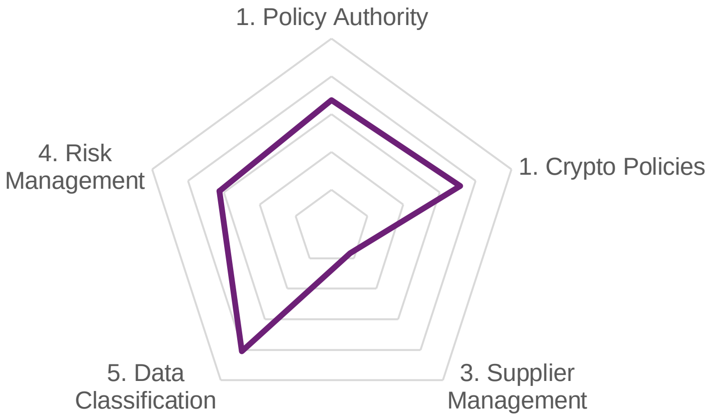
2021-2023
Inventory and prioritize systems

2024
NIST post-quantum cryptography standard published

2024-2030
Transition of systems to NIST post-quantum cryptography standard

2030
Cryptographically relevant quantum computer potentially available

POST QUANTUM READINESS ASSESSMENT



- Maturity level assessed across:
  - Process, People & Technology
- Recommendations documented
- Roadmap mutually agreed and tracked

Unknown

- **Highly reactive**
- Lack of ownership
- No centralized policy
- No inventory of assets
- Silo and segmented organization
- **No roadmap**

Awareness

- **Reactive**
- Decentralized crypto; ad hoc tools
- Evaluates regulations and understands **crypto landscape**
- Risk mitigation plan in place, but **lacks planning** and visibility of critical issues

Management

- **Moderately proactive**
- Policy established
- Crypto policy and staffing in place
- Exposed to vulnerabilities
- **InfoSec oversight**
- Backlog of issues and improvements
- **Short-term vision**

Optimization

- **Proactive**
- Central policy widely enforced
- Crypto management and discovery tools
- Cross functional team
- Modern, cloud-based technologies
- Lacks dedicated resources; competing priorities
- **3-year crypto roadmap**

Excellence

- **Highly proactive**
- Centralized crypto centre established
- Full set of tools and best practices in place
- Board support
- Fast response to fix vulnerabilities and comply with new standards with **Crypto Agility**
- Manage investments in timely matter
- Monitors emerging threats
- **5-year crypto roadmap**

Risk **Maturity**

Thank You!

ENTRUST