CYBERSECURITY

Joseph Ellis

Quantum Computing for Humans

KEYS CONFERENCE

1

DISCLAIMER

- **This presentation is for information only.**
  Evaluate risks before acting based on ideas from this presentation.
- **This presentation contains the opinions of the presenters.**
  Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.**
  Unauthorized release of this information is prohibited.
  Original material is copyright © 2024 Tandem.

2

Joseph Ellis

CISM, CRISC, CISSP, Security+
Boost Consulting Manager, CoNetrix Security

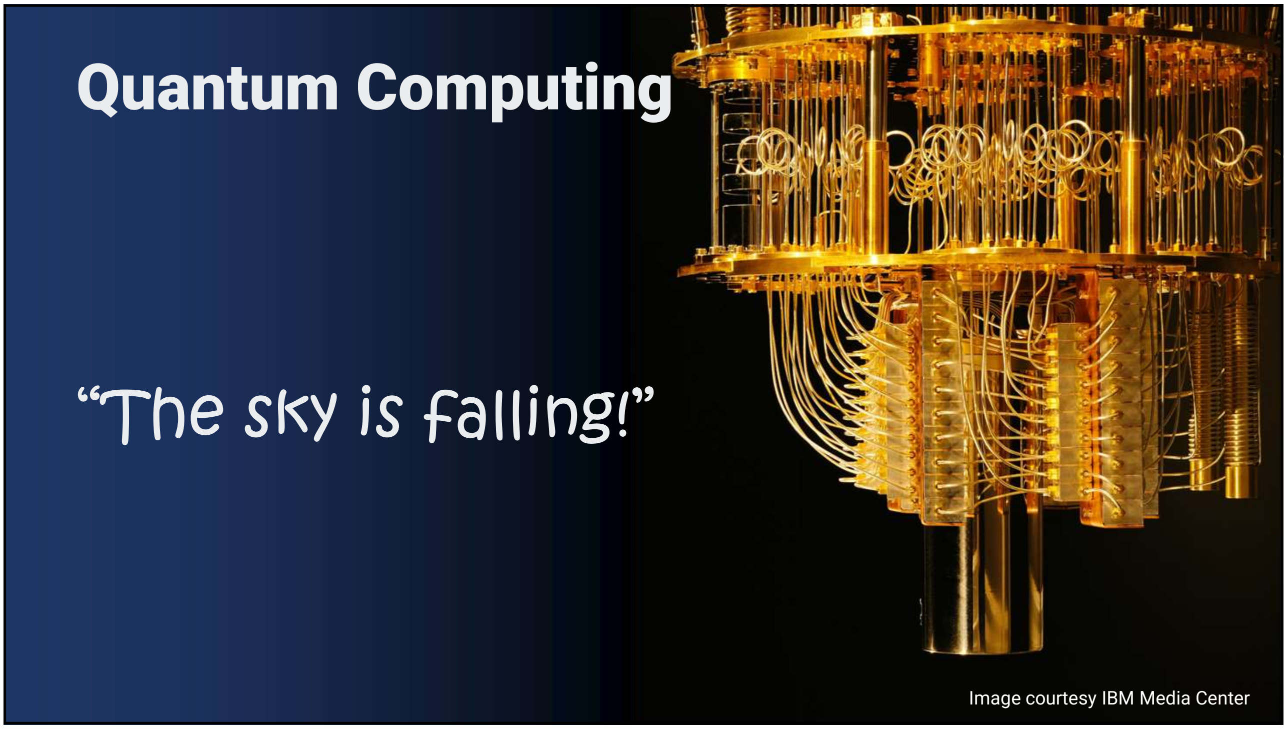
3

Agenda

Here's the Plan

- The Basics
- Security Considerations
- Take Action

4

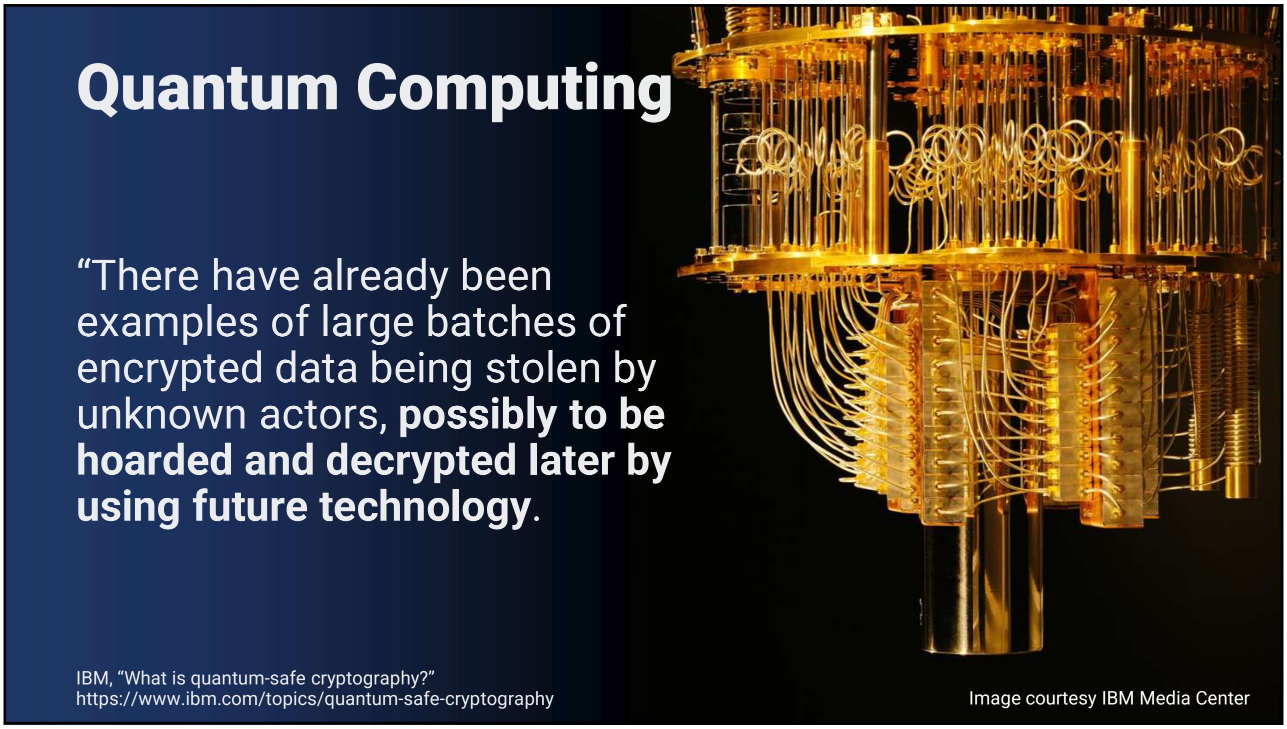


Quantum Computing

“The sky is falling!”

Image courtesy IBM Media Center

5



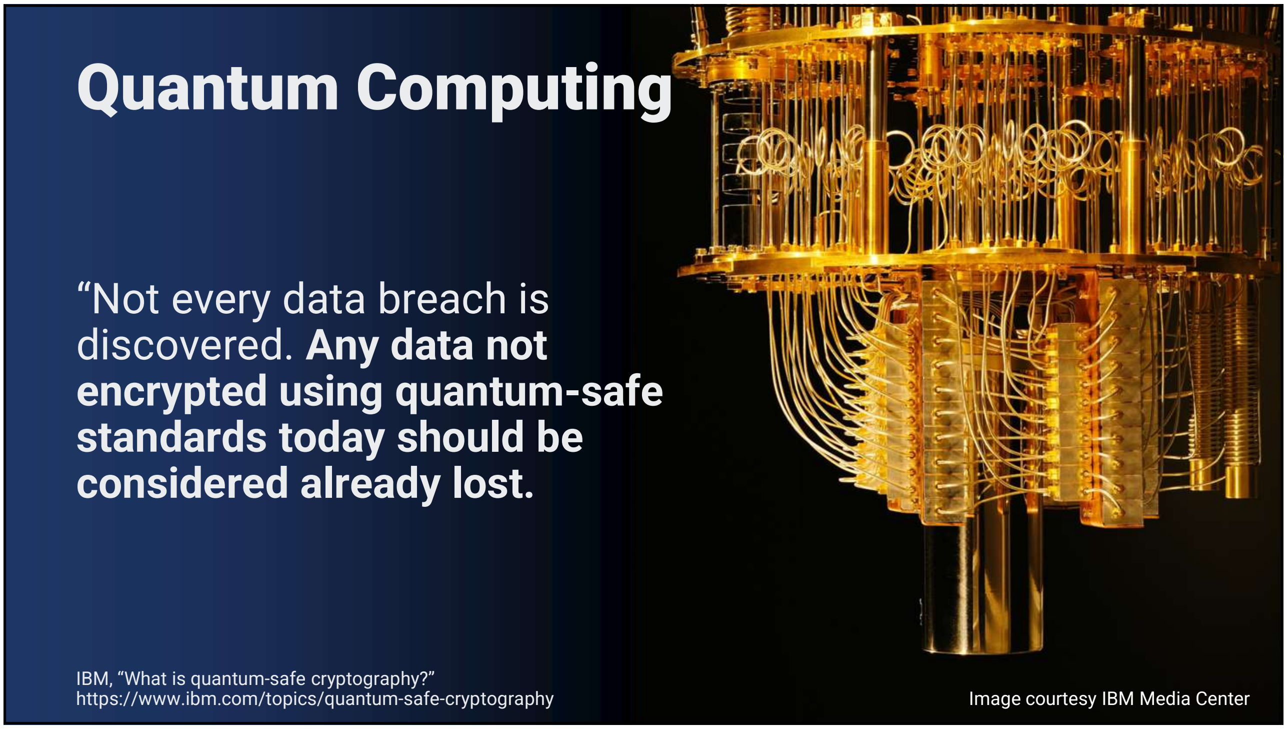
Quantum Computing

“There have already been examples of large batches of encrypted data being stolen by unknown actors, **possibly to be hoarded and decrypted later by using future technology**.

IBM, “What is quantum-safe cryptography?”
https://www.ibm.com/topics/quantum-safe-cryptography

Image courtesy IBM Media Center

6



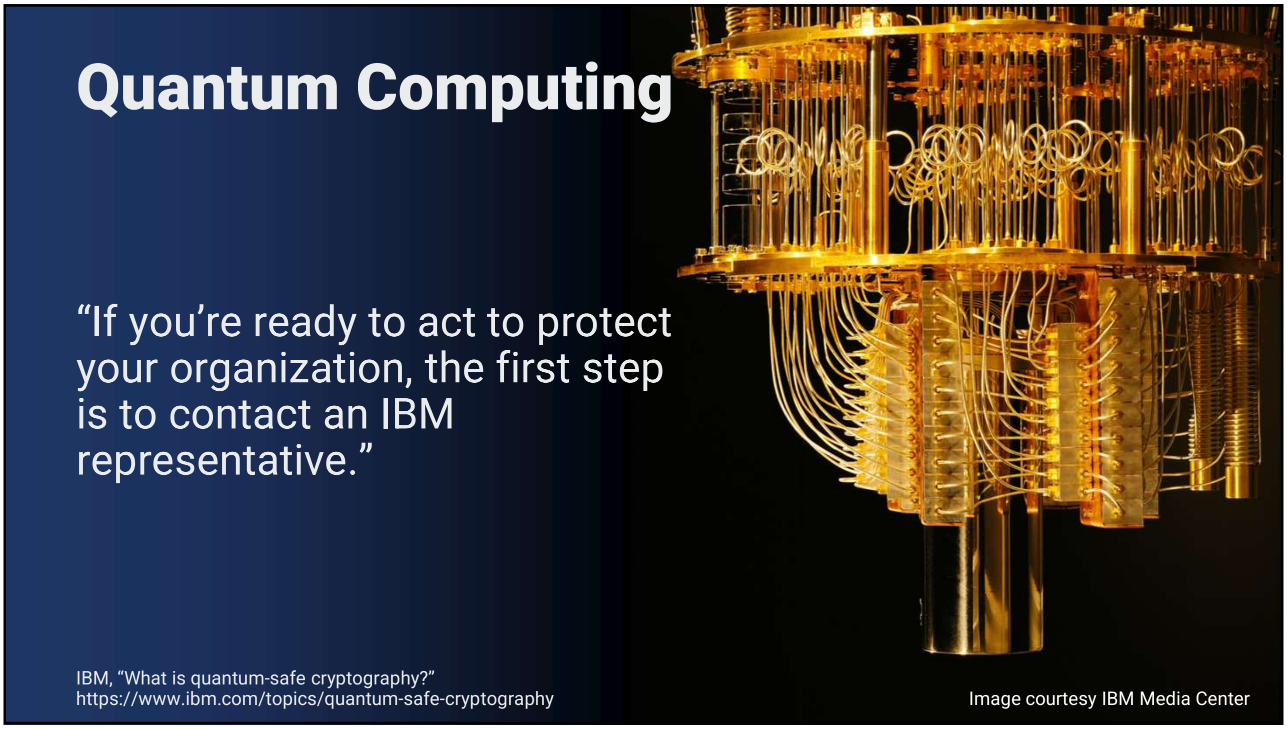
Quantum Computing

“Not every data breach is discovered. **Any data not encrypted using quantum-safe standards today should be considered already lost.**

IBM, “What is quantum-safe cryptography?”
https://www.ibm.com/topics/quantum-safe-cryptography

Image courtesy IBM Media Center

7



Quantum Computing

“If you’re ready to act to protect your organization, the first step is to contact an IBM representative.”

IBM, “What is quantum-safe cryptography?”
https://www.ibm.com/topics/quantum-safe-cryptography

Image courtesy IBM Media Center

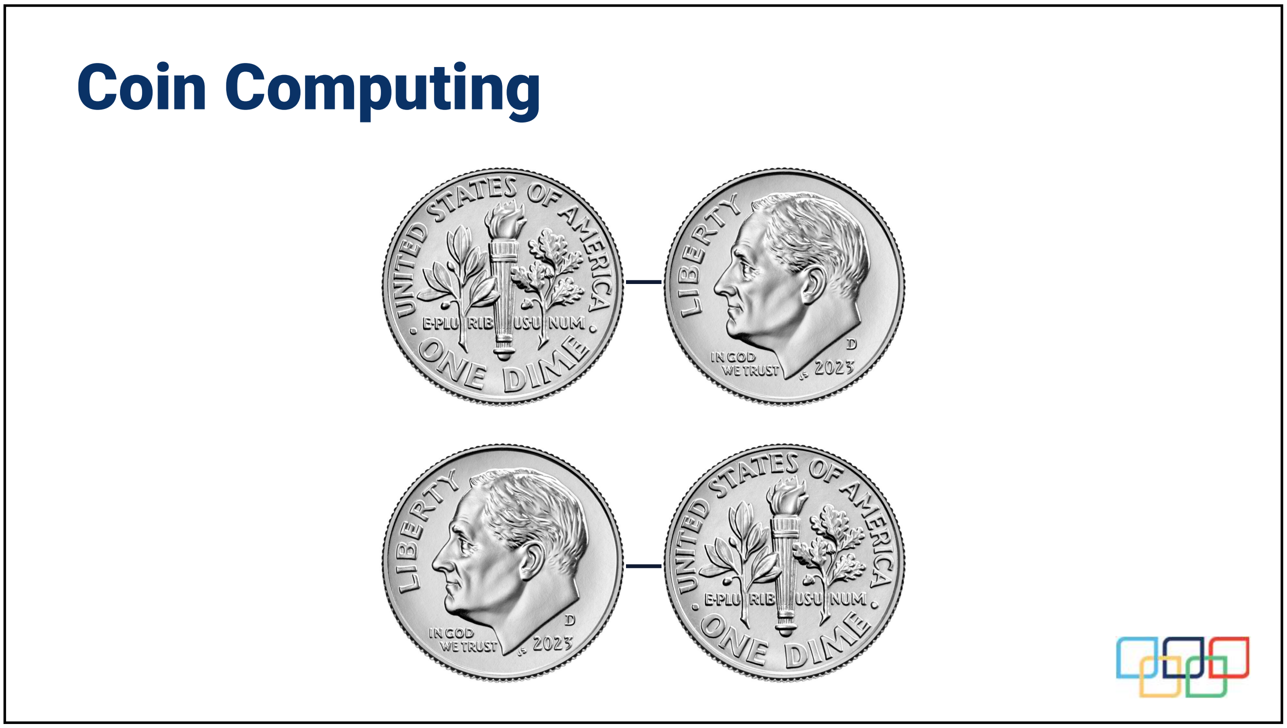
8

What is Quantum Computing, anyway?

9

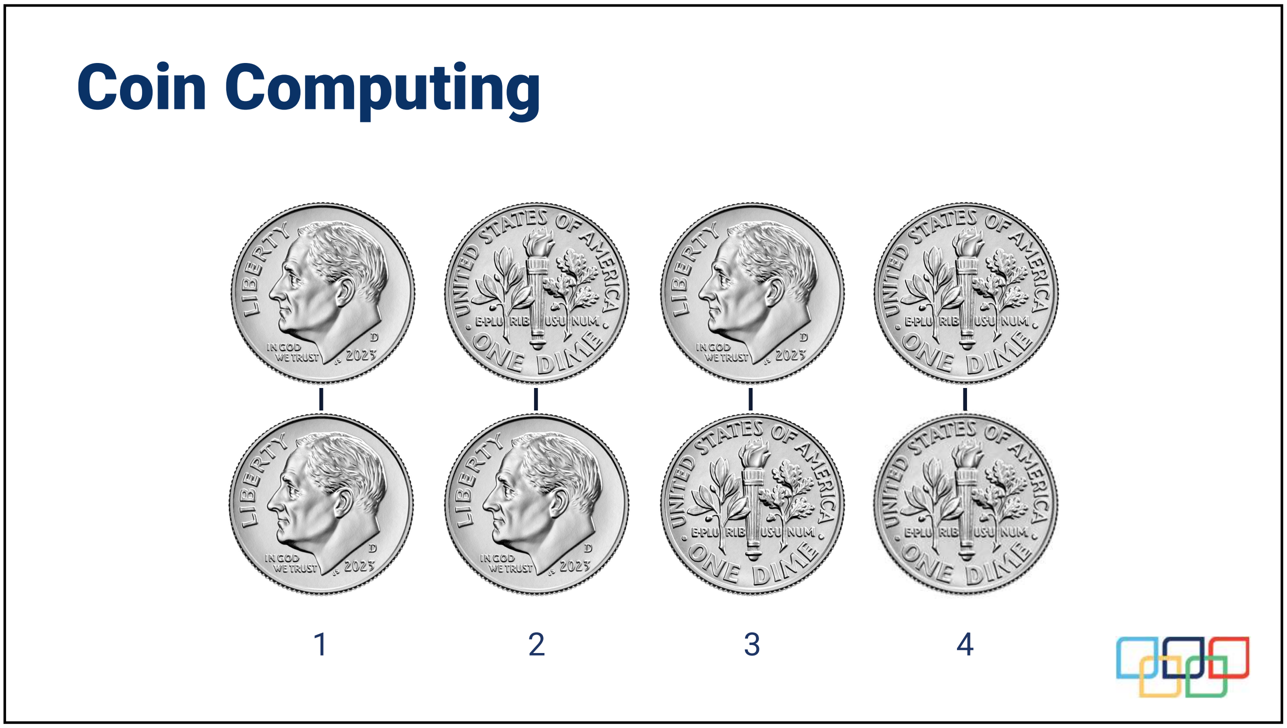
Coin Computing

10



Coin Computing

11



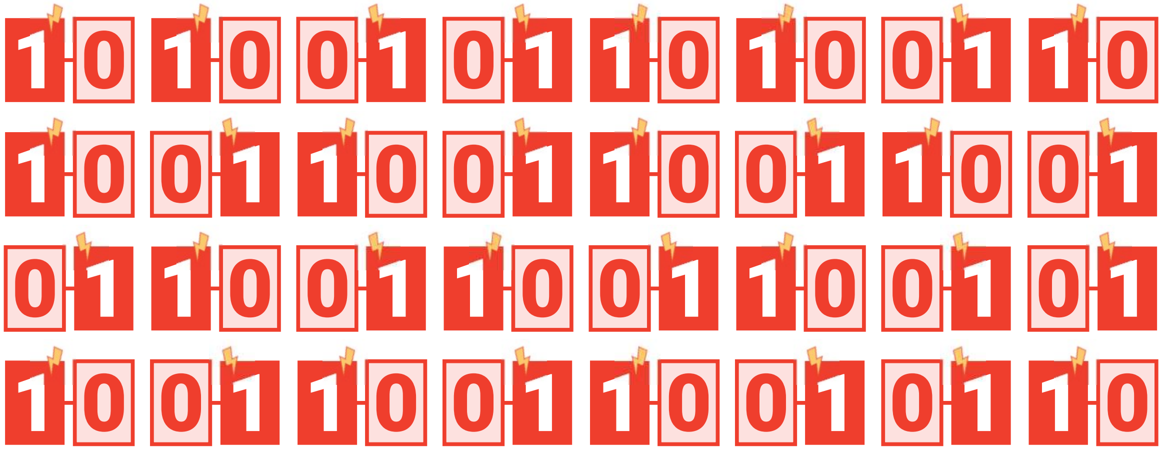
Coin Computing

12

Traditional Computing

13

Traditional Computing



1 0 1 0 0 1 0 1 1 0 1 0 0 1 1 0

1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1

0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 1

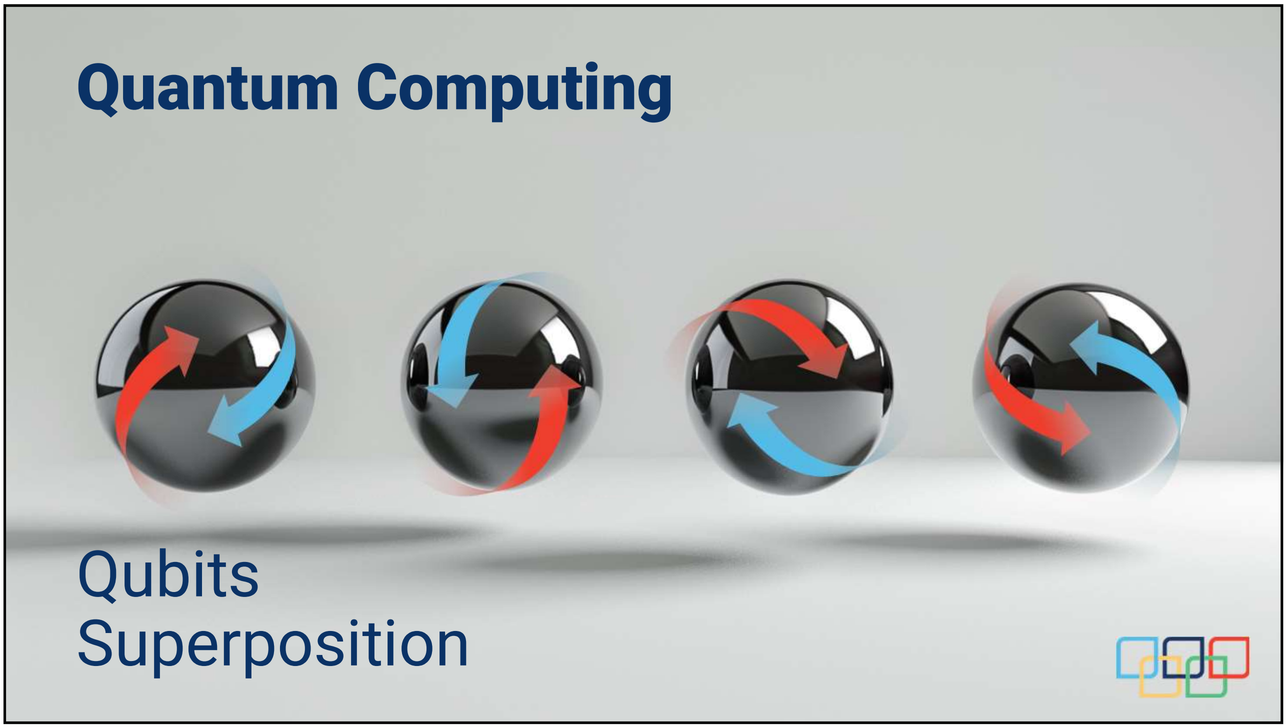
1 0 0 1 1 0 0 1 1 0 0 1 0 1 1 0

14

QUANTUM COMPUTING

15

16



Quantum Computing

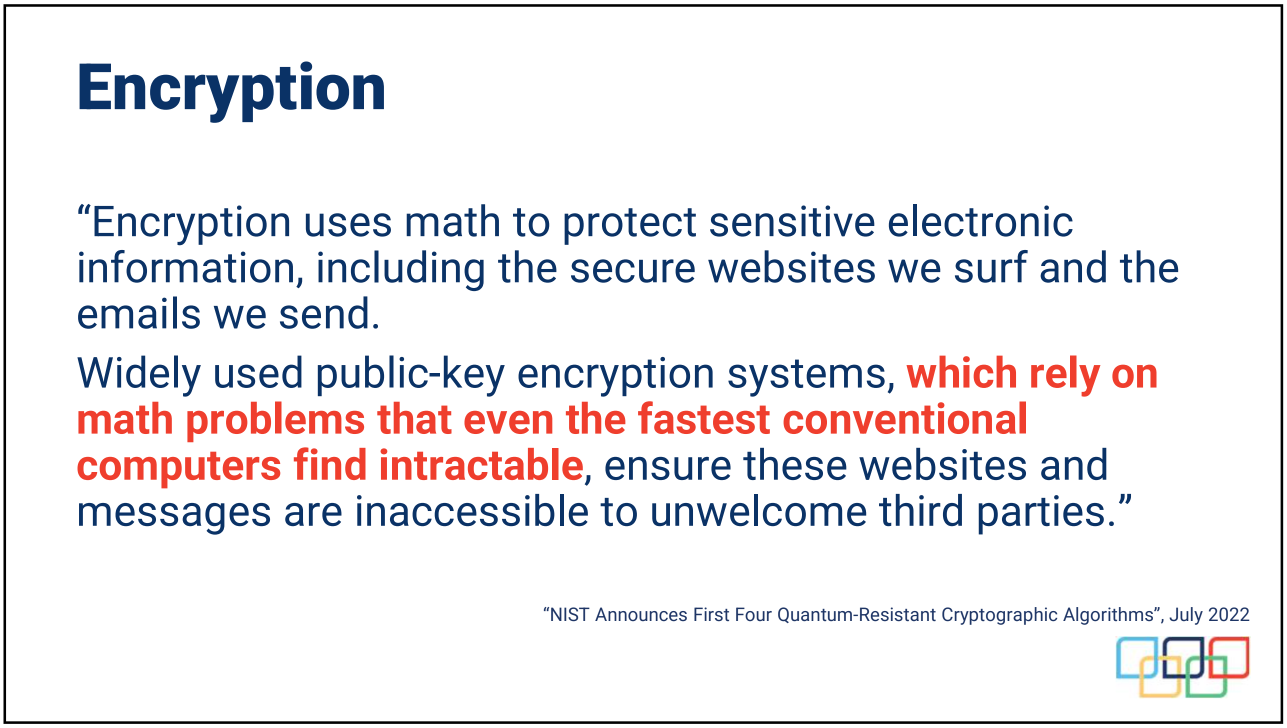
Qubits
Superposition

17

18

Security Considerations

19



Encryption

“Encryption uses math to protect sensitive electronic information, including the secure websites we surf and the emails we send.

Widely used public-key encryption systems, **which rely on math problems that even the fastest conventional computers find intractable**, ensure these websites and messages are inaccessible to unwelcome third parties.”

“NIST Announces First Four Quantum-Resistant Cryptographic Algorithms”, July 2022

20

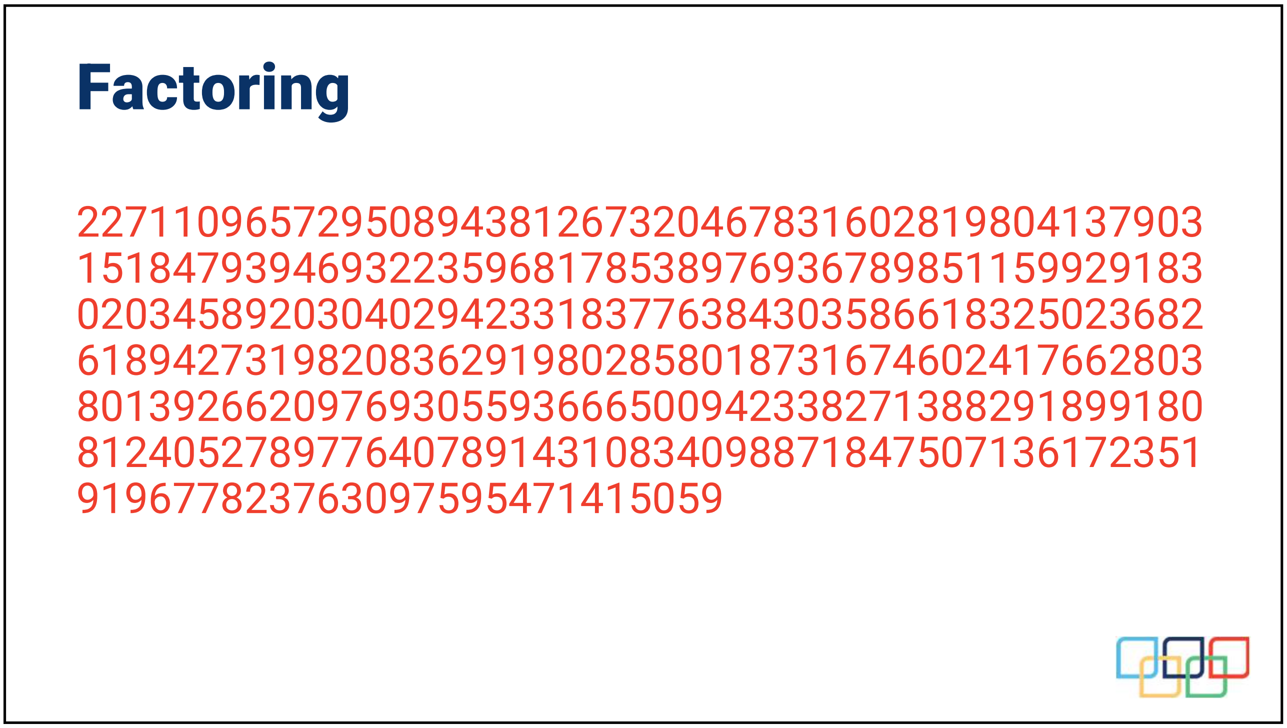
21

Factoring

21 = 7 x 3

589 = 19 x 31

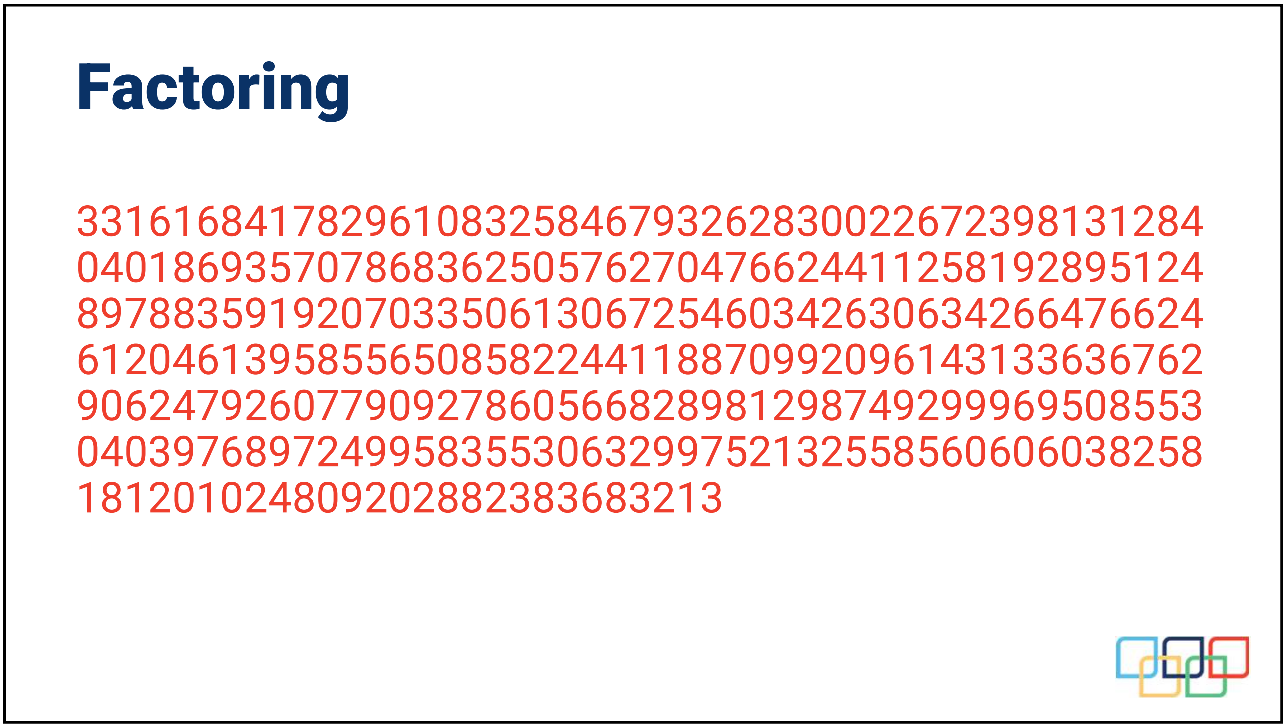
22



Factoring

22711096572950894381267320467831602819804137903
15184793946932235968178538976936789851159929183
02034589203040294233183776384303586618325023682
61894273198208362919802858018731674602417662803
80139266209769305593666500942338271388291899180
81240527897764078914310834098871847507136172351
919677823763097595471415059

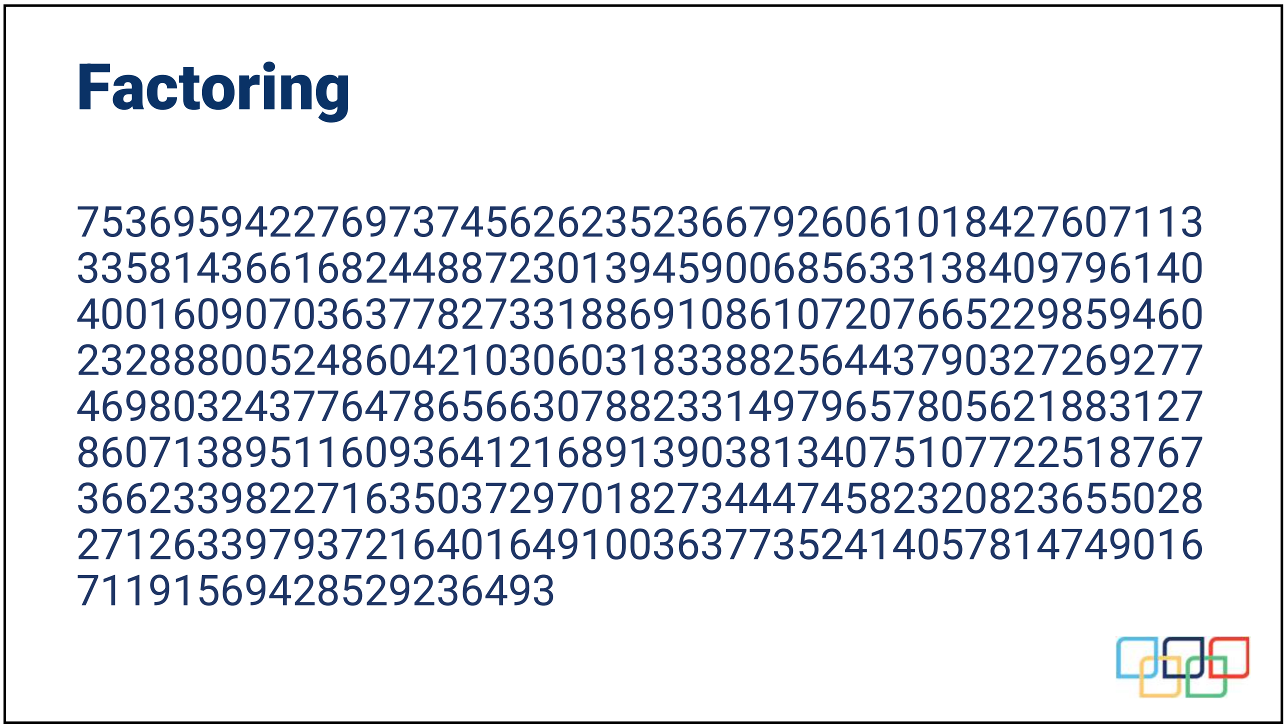
23



Factoring

33161684178296108325846793262830022672398131284
04018693570786836250576270476624411258192895124
89788359192070335061306725460342630634266476624
61204613958556508582244118870992096143133636762
90624792607790927860566828981298749299969508553
04039768972499583553063299752132558560606038258
181201024809202882383683213

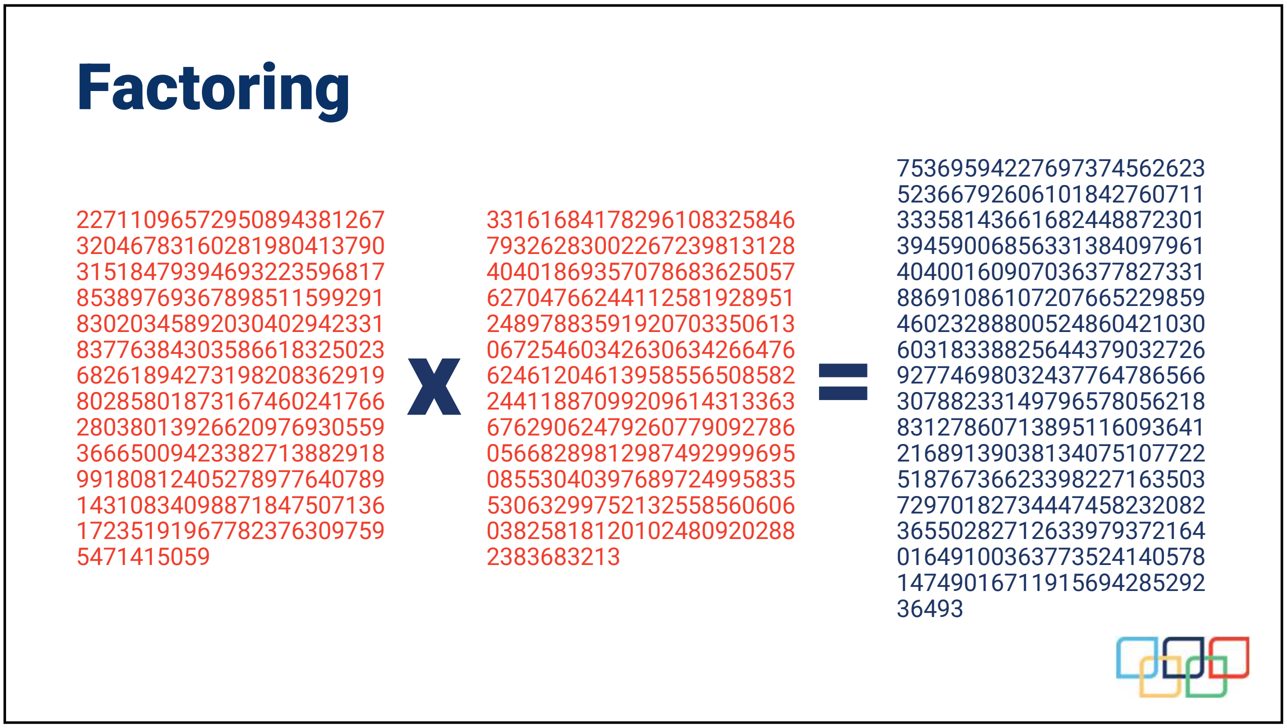
24



Factoring

75369594227697374562623523667926061018427607113
33581436616824488723013945900685633138409796140
40016090703637782733188691086107207665229859460
23288800524860421030603183388256443790327269277
46980324377647865663078823314979657805621883127
86071389511609364121689139038134075107722518767
36623398227163503729701827344474582320823655028
27126339793721640164910036377352414057814749016
71191569428529236493

25



Factoring

22711096572950894381267
32046783160281980413790
31518479394693223596817
85389769367898511599291
83020345892030402942331
83776384303586618325023
68261894273198208362919
80285801873167460241766
28038013926620976930559
36665009423382713882918
99180812405278977640789
14310834098871847507136
17235191967782376309759
5471415059

x

33161684178296108325846
79326283002267239813128
40401869357078683625057
62704766244112581928951
24897883591920703350613
06725460342630634266476
62461204613958556508582
24411887099209614313363
67629062479260779092786
05668289812987492999695
08553040397689724995835
53063299752132558560606
03825818120102480920288
2383683213

=

75369594227697374562623
52366792606101842760711
33358143661682448872301
39459006856331384097961
40400160907036377827331
88691086107207665229859
46023288800524860421030
60318338825644379032726
92774698032437764786566
30788233149796578056218
83127860713895116093641
21689139038134075107722
51876736623398227163503
72970182734447458232082
36550282712633979372164
01649100363773524140578
14749016711915694285292
36493

26

Factoring

"To give you an idea of the scale: **factoring a 500 digit number into its primes could take as long as the planet's formation**, and for huge numbers, the factoring process could take longer than the age of the universe itself."

Andreas Maier, "Prime numbers and their importance to modern life", CodeCoda, August 16, 2021, emphasis in the original

27

Solutions and Strategies

28

Quantum-Safe Cryptography

Quantum-resistant encryption algorithms:

CRYSTALS-Kyber
CRYSTALS-Dilithium
FALCON
SPHINCS+

"NIST Announces First Four Quantum-Resistant Cryptographic Algorithms", July 2022

29

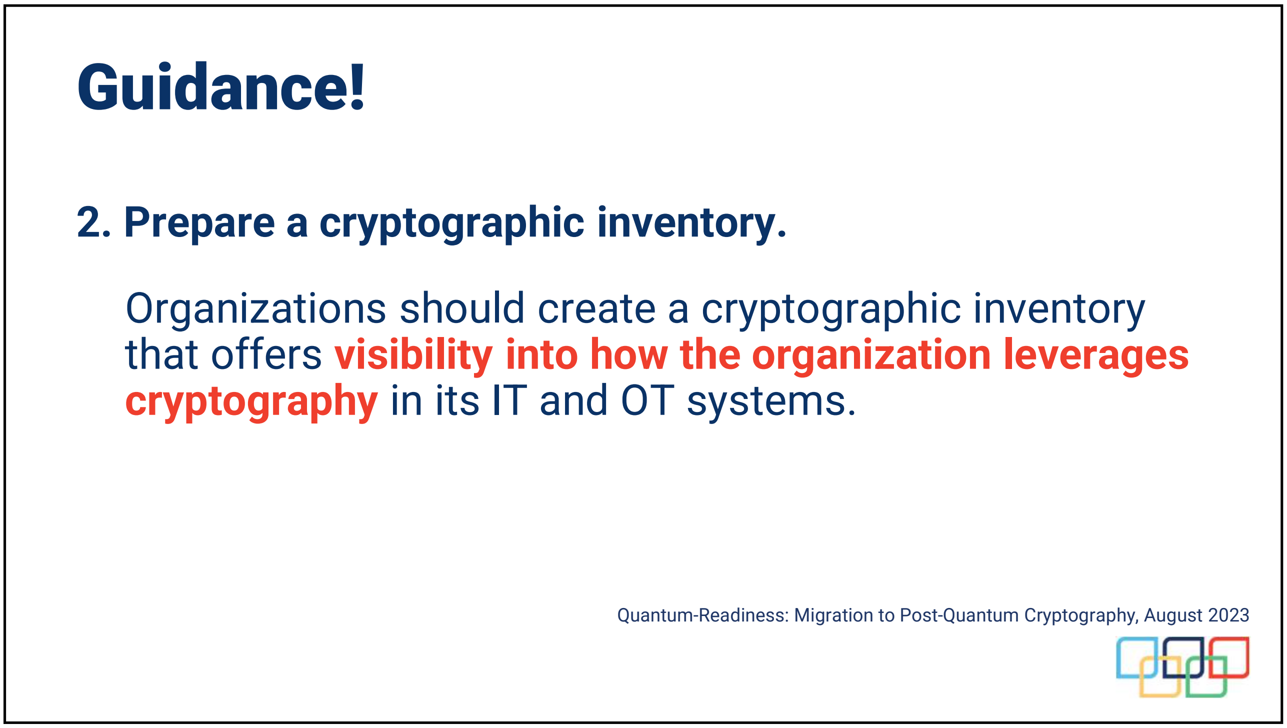
Guidance!

1. Establish a quantum-readiness roadmap.

[Establish] a project management team to plan and scope the organization's migration to PQC. Quantum-readiness project teams should initiate proactive cryptographic discovery activities that **identify the organization's current reliance on quantum-vulnerable cryptography**.

Quantum-Readiness: Migration to Post-Quantum Cryptography, August 2023

30



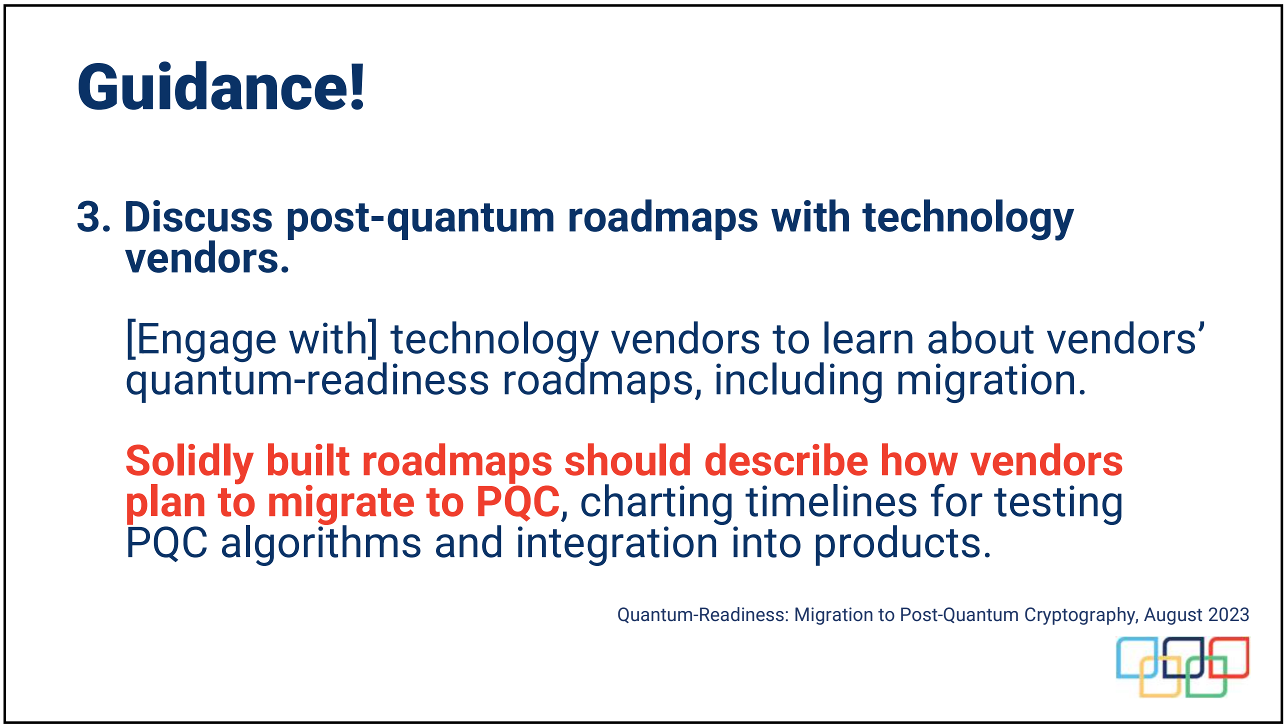
Guidance!

2. Prepare a cryptographic inventory.

Organizations should create a cryptographic inventory that offers **visibility into how the organization leverages cryptography** in its IT and OT systems.

Quantum-Readiness: Migration to Post-Quantum Cryptography, August 2023

31



Guidance!

3. Discuss post-quantum roadmaps with technology vendors.

[Engage with] technology vendors to learn about vendors' quantum-readiness roadmaps, including migration.

Solidly built roadmaps should describe how vendors plan to migrate to PQC, charting timelines for testing PQC algorithms and integration into products.

Quantum-Readiness: Migration to Post-Quantum Cryptography, August 2023

32

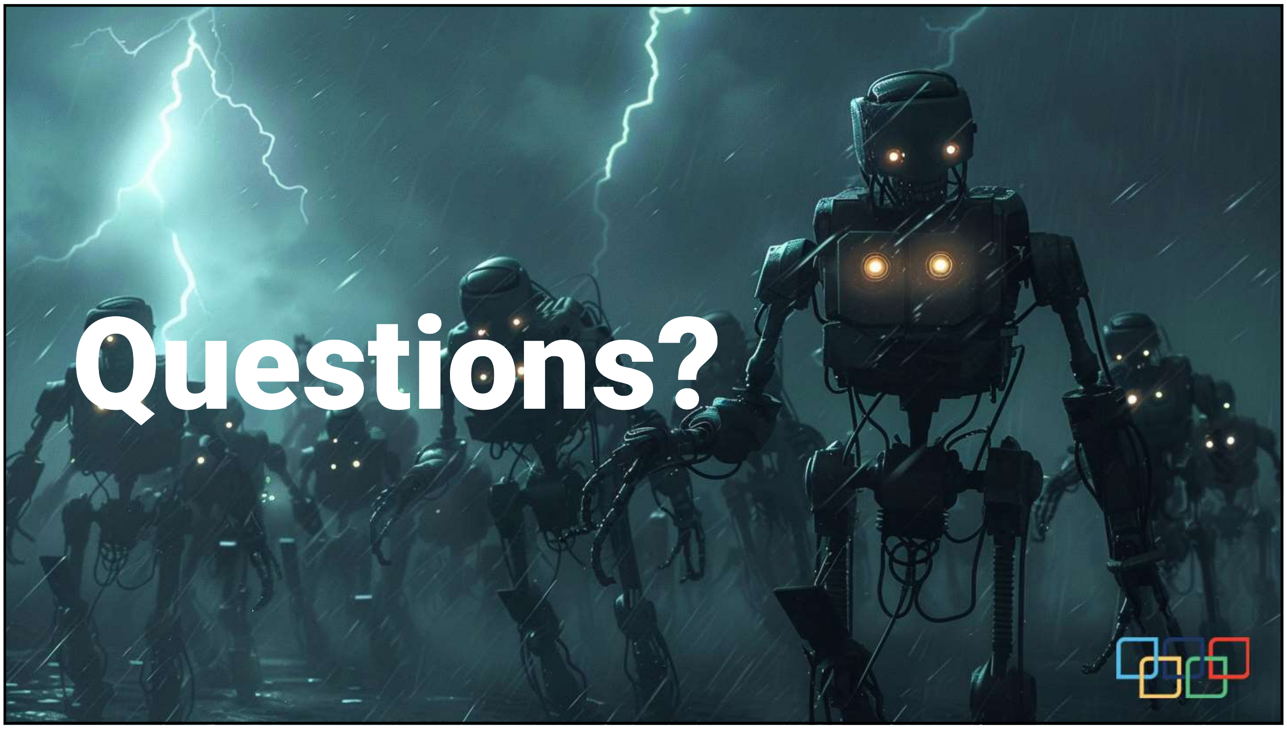
Guidance!

4. Supply chain quantum-readiness:

Organizations should develop an understanding of their reliance/dependencies on quantum-vulnerable cryptography in systems and assets, as well as **how the vendors in their supply chain will be migrating to PQC.**

Quantum-Readiness: Migration to Post-Quantum Cryptography, August 2023

33



Questions?

34

THANKS FOR JOINING!

Quantum Computing for Humans

Joseph Ellis

CISM, CRISC, CISSP, Security+
Boost Consulting Manager, CoNetrix Security

KEYS
CONFERENCE

35