Building Quantum Resistant Organizations and Securing Your Data in the Future

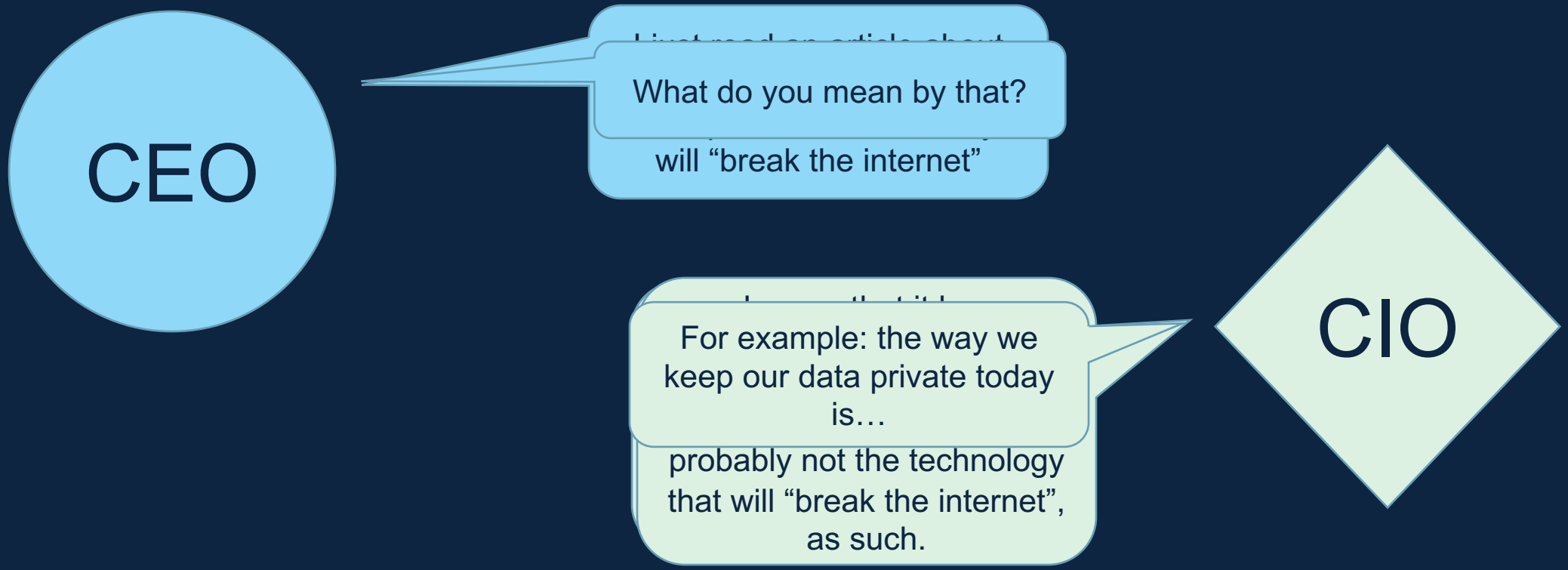
Presented at MNSEC2022 by Michael Willburn

October 6, 2022

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

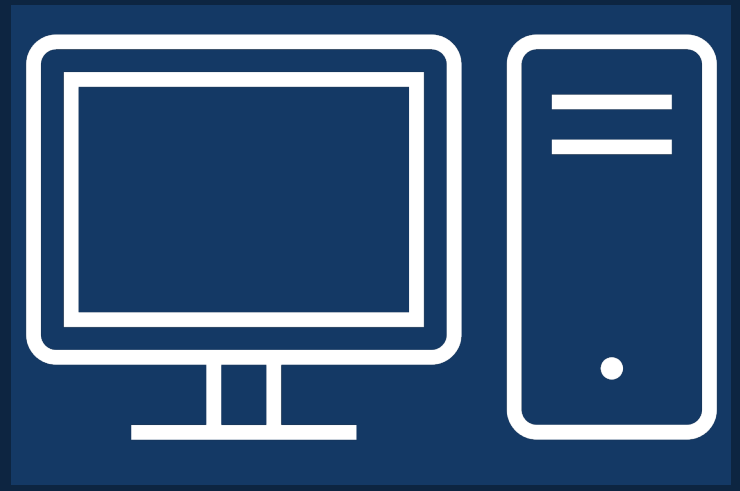
Agenda

- Review of Public Key Infrastructure and Encryption
- Quick Introduction to Quantum Computing
- Why is it a Cybersecurity concern?
- What can we do about it?
- Questions and Discussion



Review of Public Key Infrastructure and Encryption

Protecting Data Today

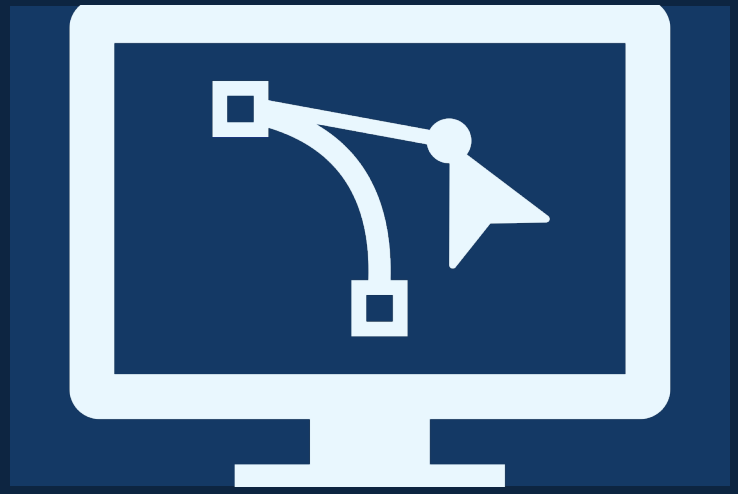


Data at Rest

- Full Disk Encryption
- Access Management
- Storage Federation

Data in Transit

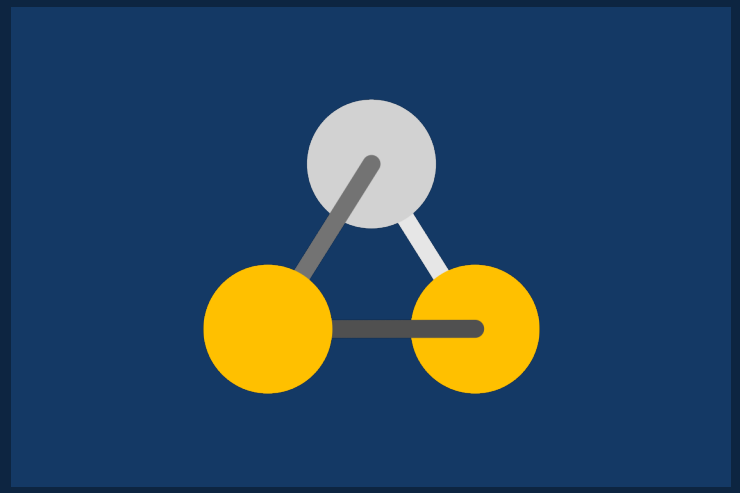
- Encrypted Tunnels
- Air-Gapped Networks
- Traffic Obfuscation



Data in Use

- Encryption
- User Awareness
- Policy

Encryption Techniques

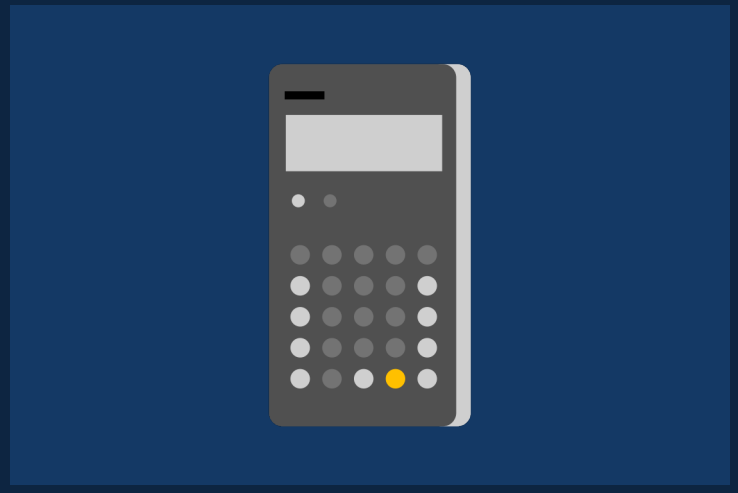


Public Key Infrastructure

- Public and Private Keys
- Multifactor Authentication
- Encryption Protocols

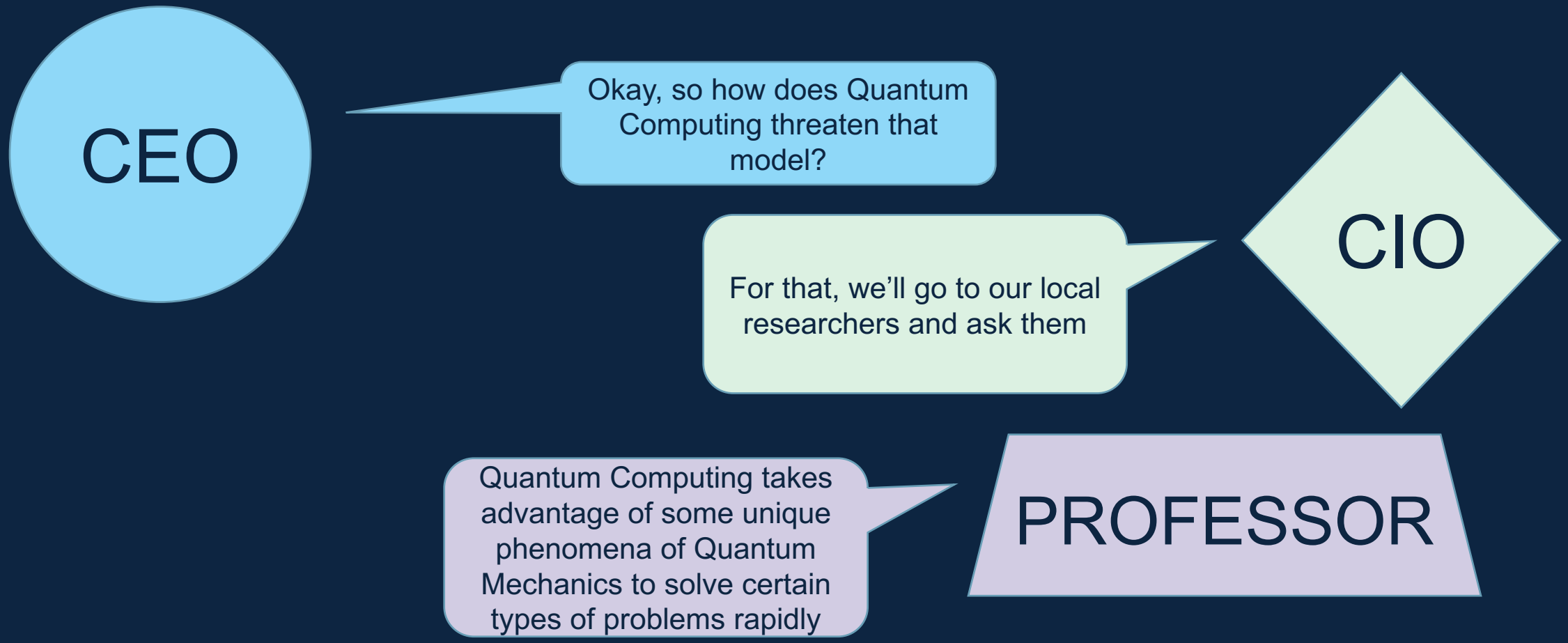
Encrypted Tunnels

- VPN
- End-to-End
- Encryption Protocols



Cryptography

- Historical Techniques
- Mathematically Based
- Large Prime Numbers



Quick Introduction to Quantum Computing

There's No Quick Way to Explain it Thoroughly

Classical Computing

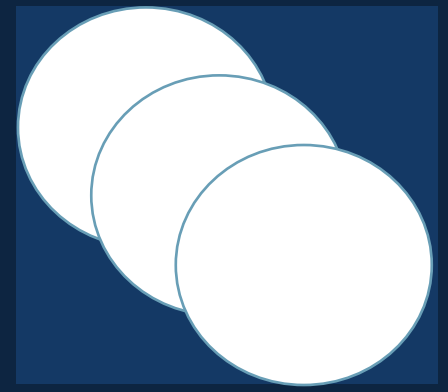
- Binary Information
- Logic Gates
- Serial or Parallel Processing

Quantum Computing

- Qubits
- Programming Languages
- Some types of Computer

Quantum Logic Gates

- Entanglement
- Measurement of Entangled Particles



Decoherence

- Non-binary
- Sensitive to subtle changes
- This is part of the power of Quantum Computing

There’s Nothing Easy About It

Precise Conditions

- Extreme Low Temperatures
- Tightly Controlled Vacuum Conditions

Hardware/Software

- Huge
- Interface with Classical Computer
- Programming is not trivial

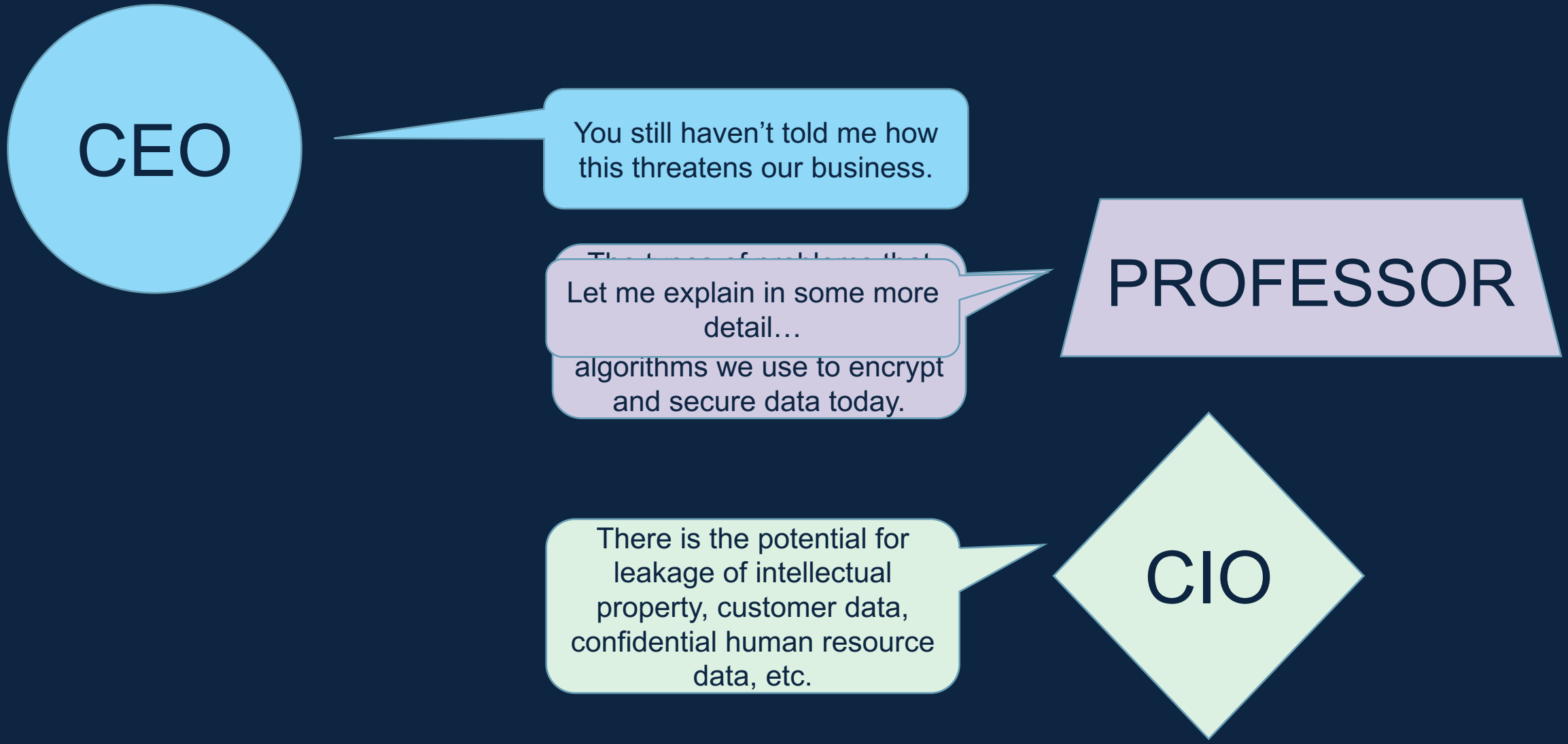
Black Box

- Don’t know exactly what happens internally
- The “Oracle”

Decoherence

- Quantum Error Correction
- Inevitable?

MITRE



Why is Quantum Computing a Cybersecurity Concern?

Qubits, Superpostion, and Quantum Factoring…Oh My!

Quantum Factoring: Shor's Algorithm

- Hybrid Implementation of classical factoring and the Quantum Fourier Transform
- Changes the time to factor a large number from exponential time (classical factoring) to polynomial time (Shor's Algorithm)

- Factoring the large prime numbers used in Cryptography is computationally intractable on classical computers
  - Or at least takes so long that it doesn't matter in the end
  - Example: Brute Forcing RSA-2048 encryption
    - ~300 trillion years
    - That's a LONG Time
- Ultimately it means that factoring is faster on a Quantum Computer
  - Example: Brute Forcing RSA-2048 encryption
    - ~ 8 hours
    - Oh my…

We use RSA in our organization! We better change now if we don't want our confidential information leaked.

That said, there is credible evidence that some organizations are collecting encrypted data now to decrypt in the future. So sooner is better.

That is not to say that we should not start taking steps. Better cryptographic practices in our organization should only enhance our security.

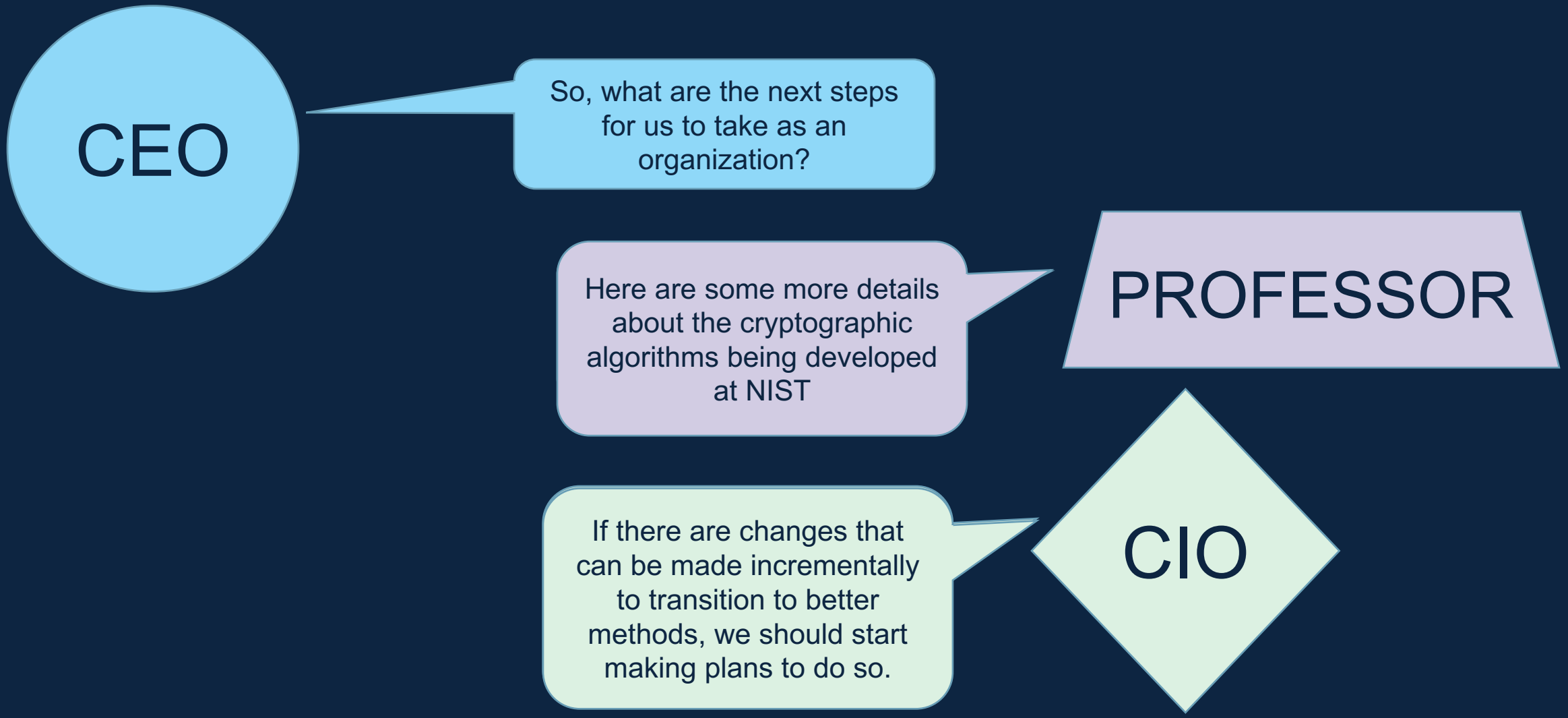
MITRE

Quantum Computing is Still Developing

- Quantum Computers are finding many uses in science and technology
- The Technology to crack cryptography seems to always be “about 10 years away”
  - The reason: Quantum Systems are difficult to work with
    - Quantum Decoherence: an inevitability?
    - Hardware costs and scalability
  - There are vocal critics that argue that it will never be usefully achieved
- The Best “Quantum” Computers today generally work with around 100 Qubits
  - To factor RSA-2048 as discussed would take about 20 million Qubits with our current understanding of error correction

So, Should We Really Worry?

- Not today, but maybe tomorrow
  - Something is impossible right up to the moment that it becomes possible
  - The next breakthrough in Quantum Computing could take place tomorrow
- The implications of a leap in Quantum Computing that breaks current cryptographic standards is not something to be ignored
  - Much of our current PKI and encrypted tunneling protocols would be available in clear text to entities that have capable Quantum Computers
  - It has taken over 20 years to implement PKI as it is today
  - It will take a long time to transition systems to a new cryptographic standard
- Developing more secure cryptographic algorithms improves overall security



What Can We Do About it?

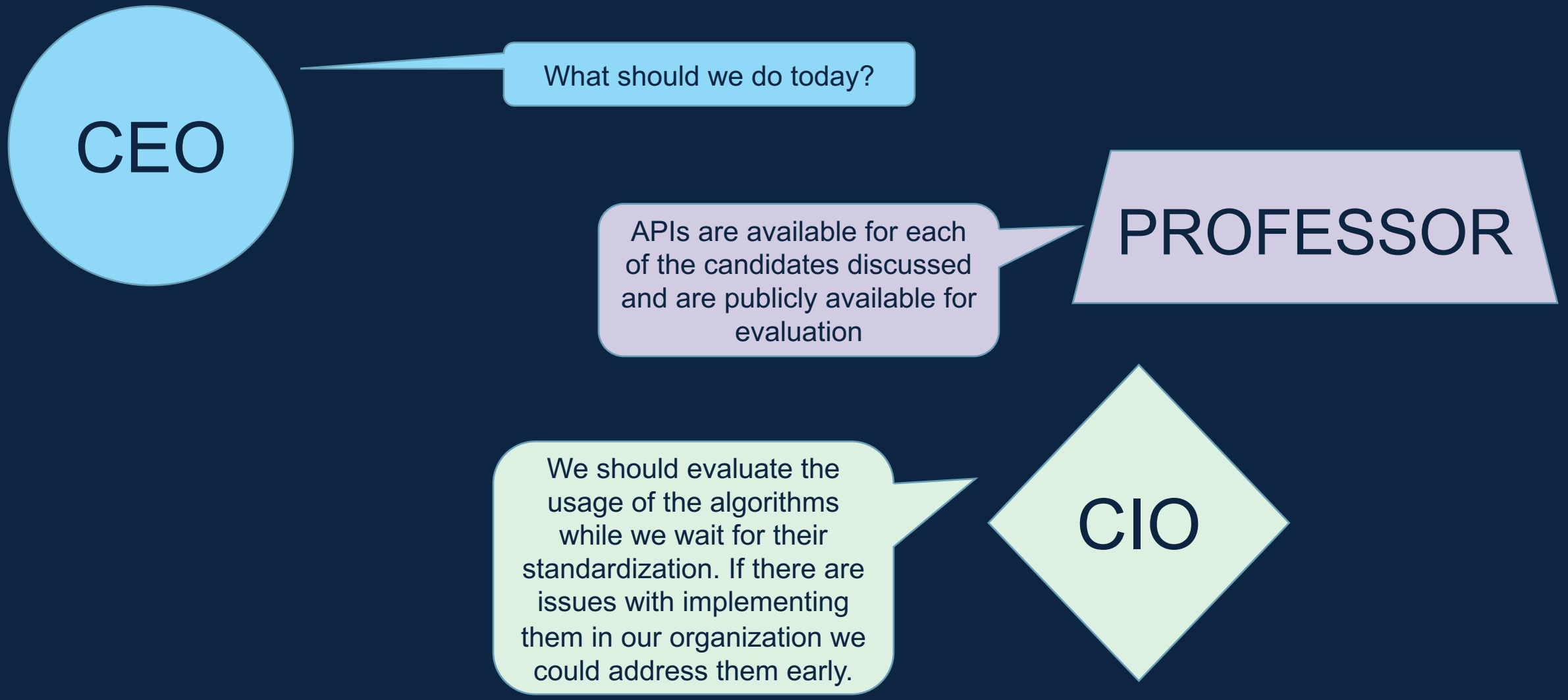
NIST Call for Post Quantum Cryptography Candidates

- Feb 24-26, 2016 NIST Presentation at PQCrypto 2016: Announcement and outline of NIST's Call for Submissions (Fall 2016) by Dustin Moody
- Dec 21, 2017 Round 1 algorithms announced (69 submissions accepted as "complete and proper")
- January 30, 2019 Second Round Candidates announced (26 algorithms)
- July 22, 2020 Third Round Candidates announced (7 Finalists and 8 Alternates)
- July 5, 2022 Announcement of Candidates to be Standardized and Fourth Round Candidates (Total of 4)
  - Shortly thereafter another article was published about one of the candidates (SIKE) that showed it could be broken with a single CPU and one hour using some very interesting math
  - Takeaway here: creating new cryptographic algorithms is difficult at best, cybersecurity professionals will need to pay attention moving forward

The Candidates to be Standardized

	CRYSTALS- KYBER	CRYSTALS- DILITHIUM	FALCON	SPHINCS+
Type of Algorithm	**Public-key Encryption (PKE) and Key-establishment Algorithm**	**Digital Signature Algorithm**	**Digital Signature Algorithm**	**Digital Signature Algorithm**
Description	• Only candidate for PKE • Early adoption by organizations like Cloudflare, Amazon, and IBM • Case Studies are available • Relatively Low Computational Costs	• Integrates easily with Kyber • Case Studies are available • Relatively Low Computational Costs	• Most scalable • Designed to be implemented soonest • Lowest Computational Cost	• Possibly the most secure • Highest Computational Cost

MITRE



What is Cloudflare Doing?

- Their team sees evidence that Quantum Computing is inevitable and therefore has significant privacy concerns
- Cloudflare is therefore already taking steps to implement Post Quantum Cryptography
  - In 2019 Cloudflare and Google performed the “TLS Post-Quantum Experiment”, which involved implementing and supporting new key exchange mechanisms based on post-quantum cryptography for all Cloudflare customers for a period of a few months
  - Began to use Post Quantum Cryptography for most of their internal services by the end of 2021
  - Positioning themselves to be among the first services to offer post-quantum cipher suites to customers as standards emerge.
  - Integrating the candidate standards into their Cloudflare Interoperable, Reusable Cryptographic Library (CIRCL)

What is Amazon Doing?

- The AWS Key Management Service now supports a hybrid TLS Post Quantum Key Exchange algorithm
  - Post Quantum security available for the Cloud, at least if it is hosted by AWS
- Example of how this Hybrid Key Exchange works:
  - The negotiated post-quantum key is appended to the ECDHE (standard TLS) key before being used as the hash-based message authentication code (HMAC) key
  - The text hybrid in its ASCII representation is prepended to the beginning of the HMAC message.
  - The entire client key exchange message from the TLS handshake is appended to the end of the HMAC message
  - Small increase in computing overhead (~0.3 milliseconds) when using the hybrid model vs. the purely standard TLS handshake

What is IBM Doing?

- Created a tape drive using the CRYSTALS algorithms (both KYBER and DILITHIUM) and asymmetric AES-256 encryption
  - The new IBM quantum computing-safe tape drive prototype is based on a state-of-the-art IBM TS1160 tape drive and uses both Kyber and Dilithium in combination with symmetric AES-256 encryption to enable the world's first quantum computing-safe tape drive. The new algorithms are implemented as part of the tape drive's firmware and could be provided to customers as a firmware upgrade for existing tape drives and/or included in the firmware of future generations of tape drives.
- This is in addition to their work to develop Quantum Computing Capability
  - In November 2021 they announced a 127 Qubit chip named the "Eagle"
- And a whole lot more!

Questions and Discussion

Michael Willburn

mwillburn@mitre.org

@aluthis

linkedin.com/in/mikewillburn

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

References

Moody, D. "Post-Quantum Cryptography: NIST's Plan for the Future". Presented at PQCrypto 2016, February 24-26, 2016 (Fukuoka, Japan). Accessed on September 14, 2022.

Chen, L., et al. "Report on Post Quantum Cryptography". NIST Publication 8105. 2016. Accessed on September 16, 2022.

Cooper, D., et al. "Recommendation for Stateful Hash-Based Signature Schemes". NIST Publication SP 800-208. 2020. Accessed on September 16, 2022.

Ross, W., et al. "Digital Signature Standard (DSS)". NIST Publication FIPS 186-5. 2019. Accessed on September 15, 2022.

NIST. "Post Quantum Cryptography: Workshops and Timeline". https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline. Accessed on September 16, 2022.

Aumasson, J. et al. "SPHINCS+" . https://sphincs.org/. Accessed on September 16, 2022.

Bernstein, A., et al. "The SPHINCS+ Signature Framework". The SPHINCS Project. 2019. Accessed on September 17, 2022.

Avanzi, R., et al. "The CRYSTALS Project". https://pq-crystals.org/kyber/index.shtml. Accessed on September 16, 2022

Lantz, M., et al. "World's First Quantum Computing Safe Tape Drive". IBM. 2019. Accessed on September 18, 2022.

Celi, S., et al. "The post-quantum future: challenges and opportunities". Coudflare. 2022. Accessed on September 15, 2022.

Weibel, A. "Round 2 post-quantum TLS is now supported in AWS KMS". AWS Security Blog. 2020. Accessed on September 16, 2022.