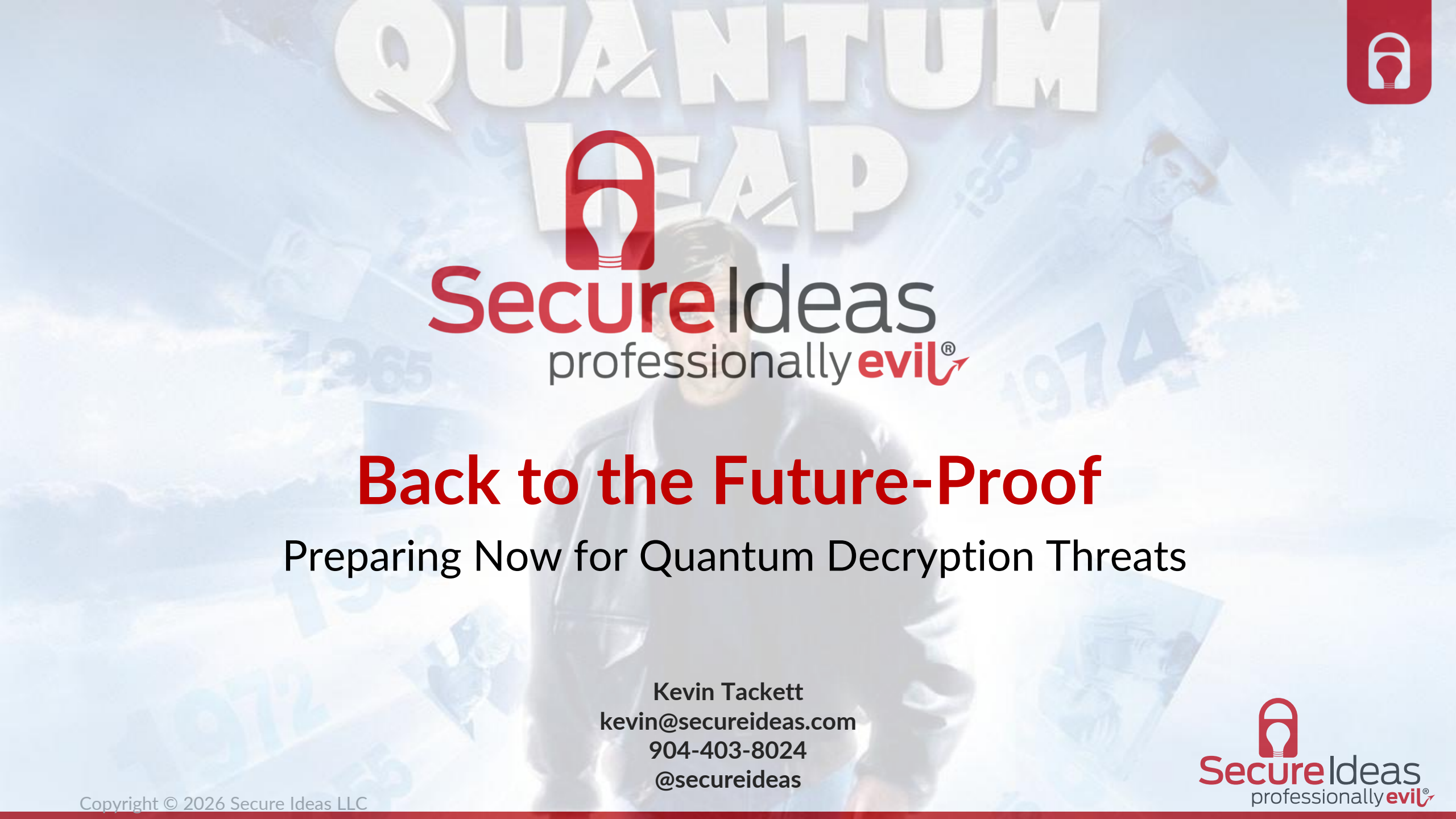


Back to the Future-Proof

Preparing Now for Quantum Decryption Threats

Kevin Tackett
kevin@secureideas.com
904-403-8024
@secureideas

Copyright © 2026 Secure Ideas LLC

Agenda

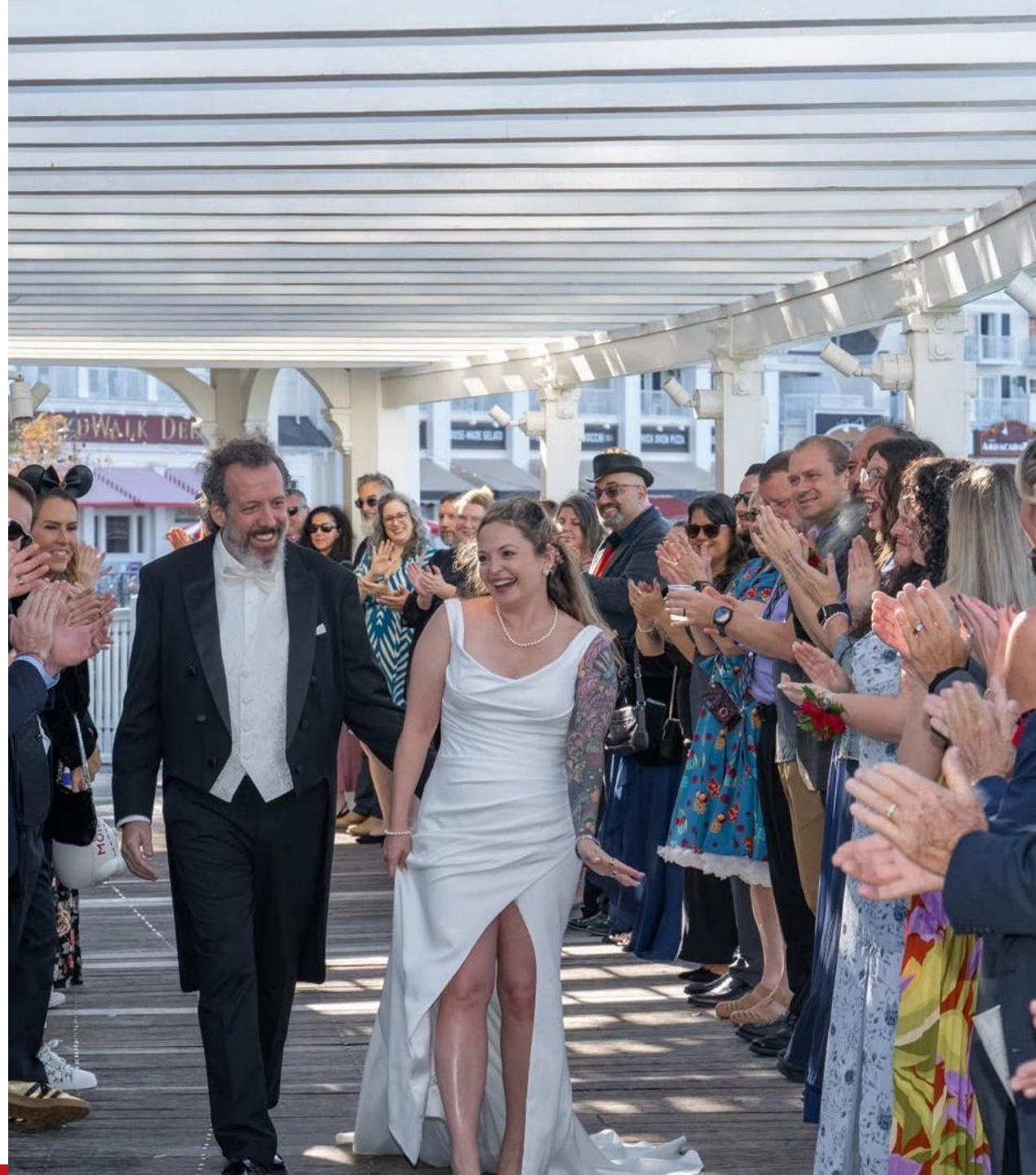
- Understanding the Threat
- What is the Risk
- Post-Quantum Standards
- Building your Transition
- Operational Challenges
- Communicating to Leadership

Copyright © 2026 Secure Ideas LLC

Kevin Tackett

- CEO - Secure Ideas, LLC
  - Founded in 2010
- IANS Faculty member
  - Since 2011
- Open-Source Fanatic
  - OWASP Leader
  - Project Builder and Founder
- Speaker, Course Instructor, Author
  - Since 1991
  - SANS, ISC2, OWASP, DEF CON, Blackhat, etc.
- Board Member
  - BSidesJax
  - President

- Other Interests
  - Warhammer (40K and AoS)
  - Woodworking
  - Husband and Father



Copyright © 2026 Secure Ideas LLC

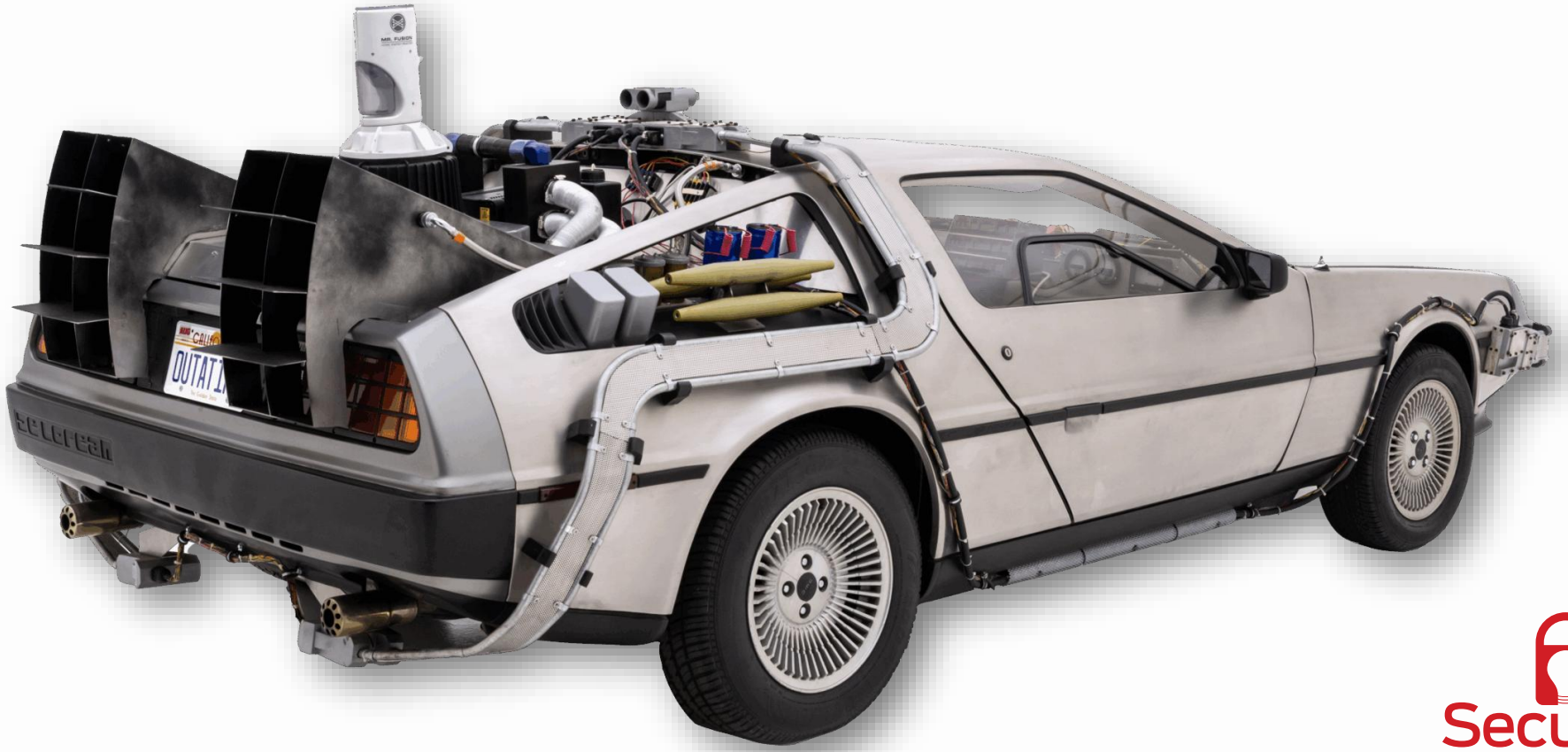


Understanding the Threat

Copyright © 2026 Secure Ideas LLC

The DeLorean Problem

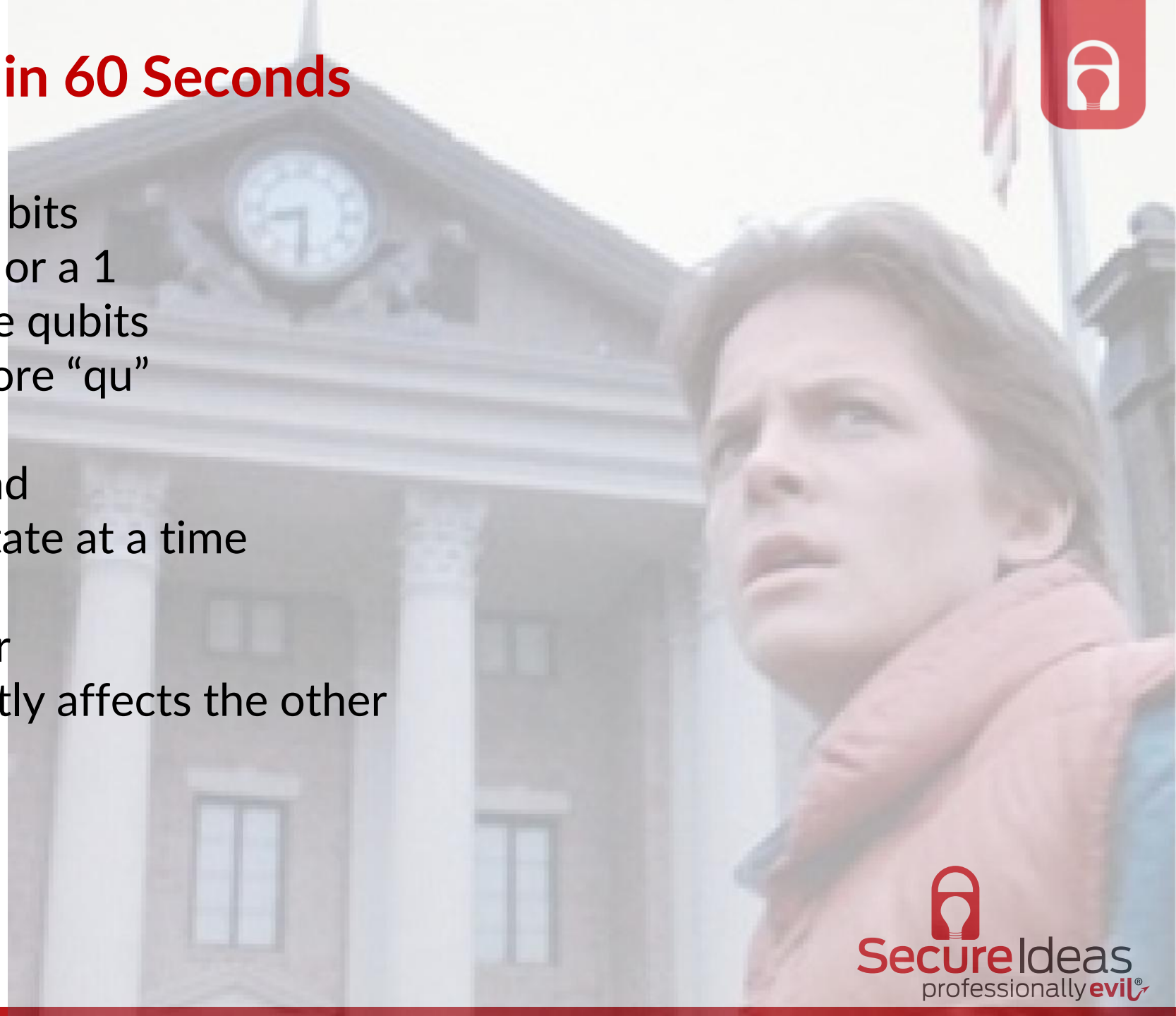
- Quantum computing WILL break encryption
  - When is the main question
- Preparing today is critical
  - Especially due to the *Harvest Now, Decrypt Later* issue



Copyright © 2026 Secure Ideas LLC

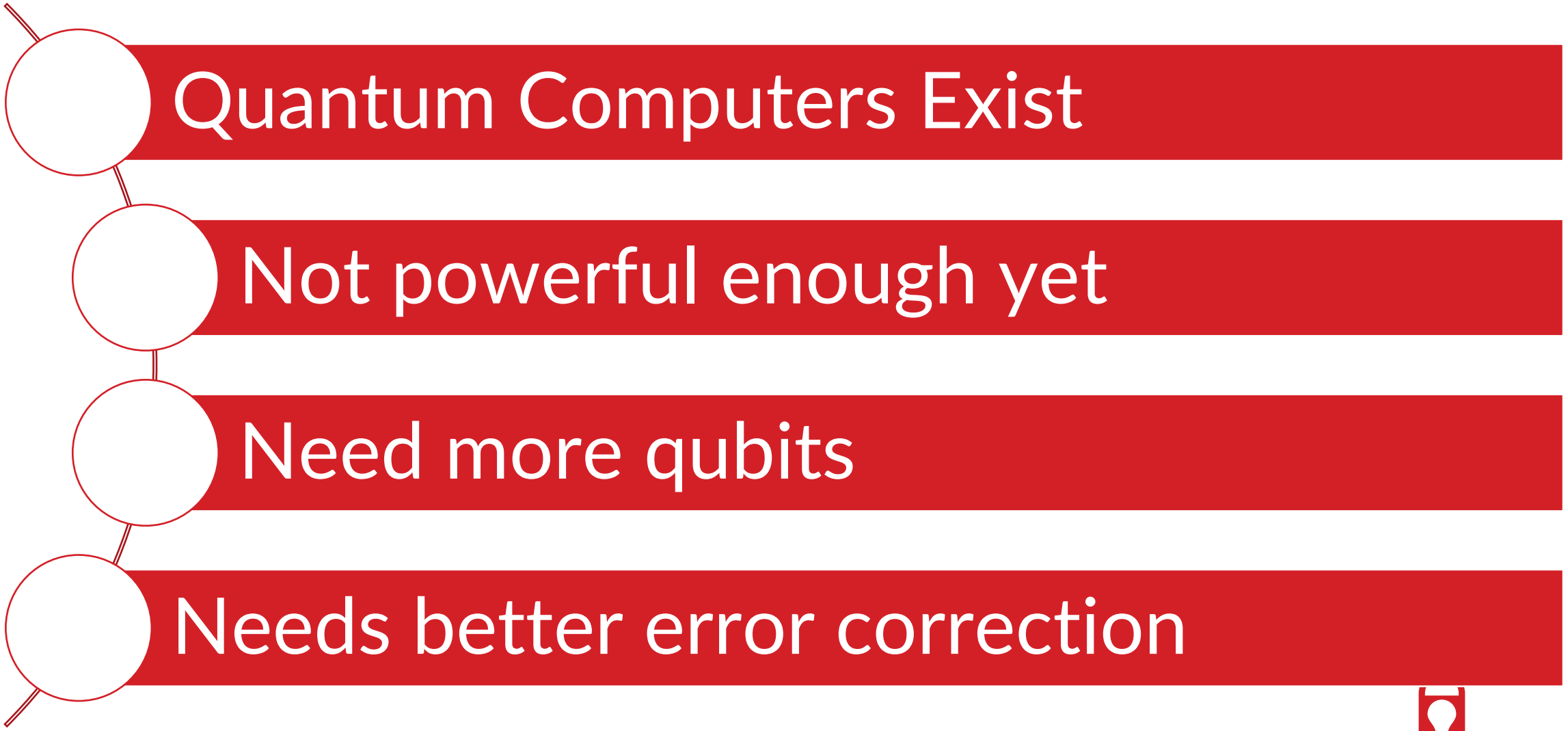
Quantum Computing in 60 Seconds

- Classical computers use bits
  - Each bit is either a 0 or a 1
- Quantum computers use qubits
  - Similar to bits but more “qu”
- Superposition
  - Is the bit alive or dead
  - Not limited to one state at a time
- Entanglement
  - Links qubits together
  - Changing one instantly affects the other



Copyright © 2026 Secure Ideas LLC

Current State



Copyright © 2026 Secure Ideas LLC



What is the Risk Actually?

Copyright © 2026 Secure Ideas LLC

Secure Ideas
professionally evil®

Risk Ratings are Hard

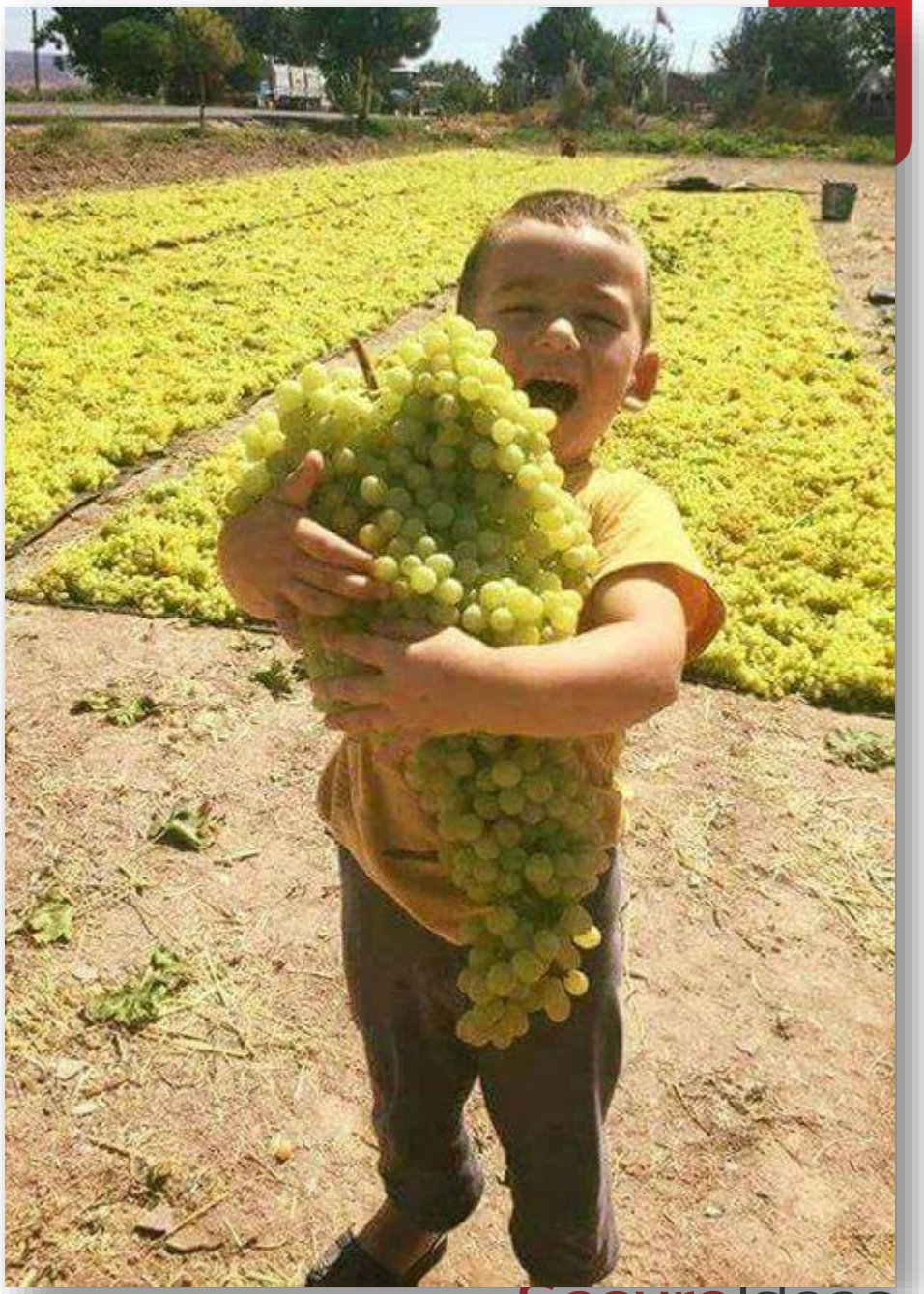
- Risk is a common word
  - Sadly, misunderstood way to often
- Business is key context
  - What are your worries?
  - Not what are others'



Copyright © 2026 Secure Ideas LLC

Harvest Now, Decrypt Later

- HNDL is the main concern today
  - Real-time decryption is coming
- Asymmetric encryption is completely broken
  - Shor's Algorithm (1994)
- Symmetric encryption is weakened
  - Grover's Algorithm(1996)
  - Halves the keyspace basically



Copyright © 2026 Secure Ideas LLC
Secure Ideas professionally evil®

Problematic Algorithms

- Some Examples
  - RSA in all forms
  - Elliptic curve cryptography
  - Diffie-Hellman key exchange
  - Most TLS implementations
- Where are these in use?
  - HTTPS
  - VPNs and remote access
  - Email transmission and digital signatures
  - Code signing
- More difficult examples
  - Embedded systems
  - Third-parties

Copyright © 2026 Secure Ideas LLC



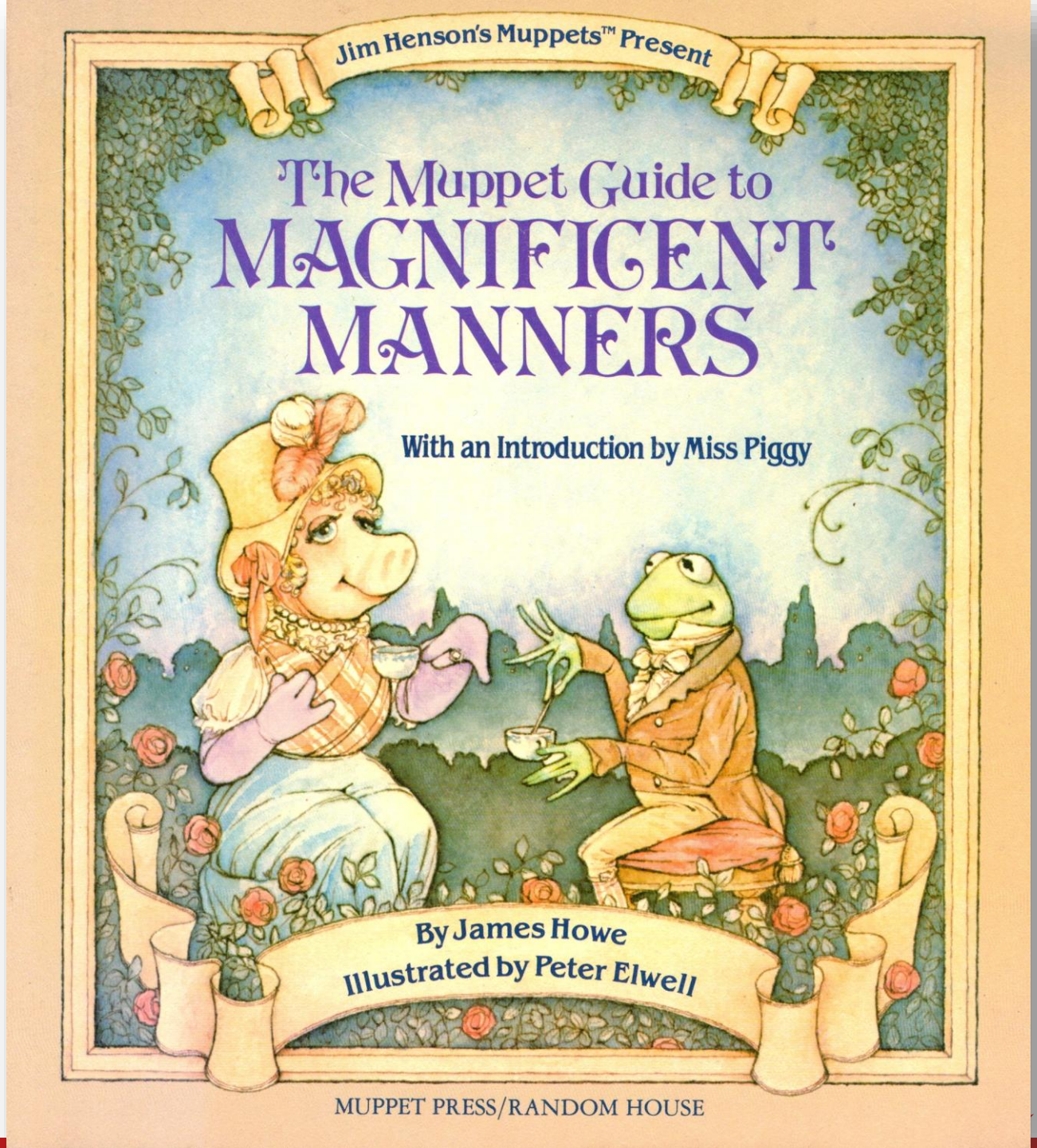
Post-Quantum Standards

Copyright © 2026 Secure Ideas LLC

Secure Ideas
professionally evil®

New Standards

- NIST is trying
  - Common purpose
- Standardized options released in 2024
  - One more coming in 2027
- Ready for use now
  - But be careful about traditional attacks
  - Hybrid mode to the rescue



Copyright © 2026 Secure Ideas LLC

Standards

- **FIPS 203: ML-KEM**
  - Module-Lattice-Based Key-Encapsulation Mechanism
  - Used for general encryption
  - Protects data in transit
- **FIPS 204: ML-DSA**
  - Module-Lattice-Based Digital Signature Algorithm
  - Primary standard for digital signatures
  - Verifies identity and authenticity
- **FIPS 205: SLH-DSA**
  - Stateless Hash-Based Digital Signature Algorithm
  - Backup signature method
  - Uses different math than ML-DSA

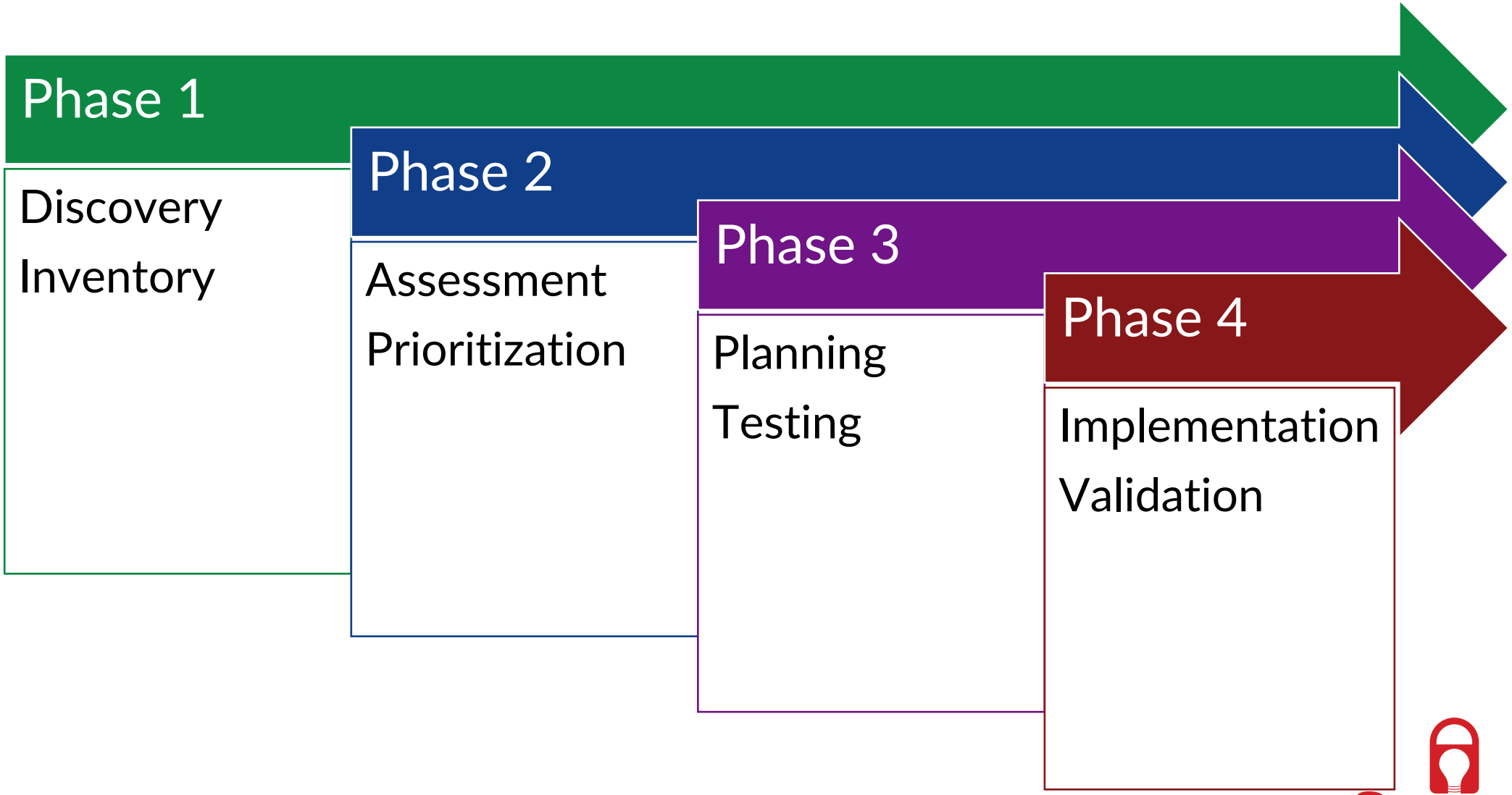
Copyright © 2026 Secure Ideas LLC
Secure Ideas professionally evil®



Building Your Transition

Copyright © 2026 Secure Ideas LLC

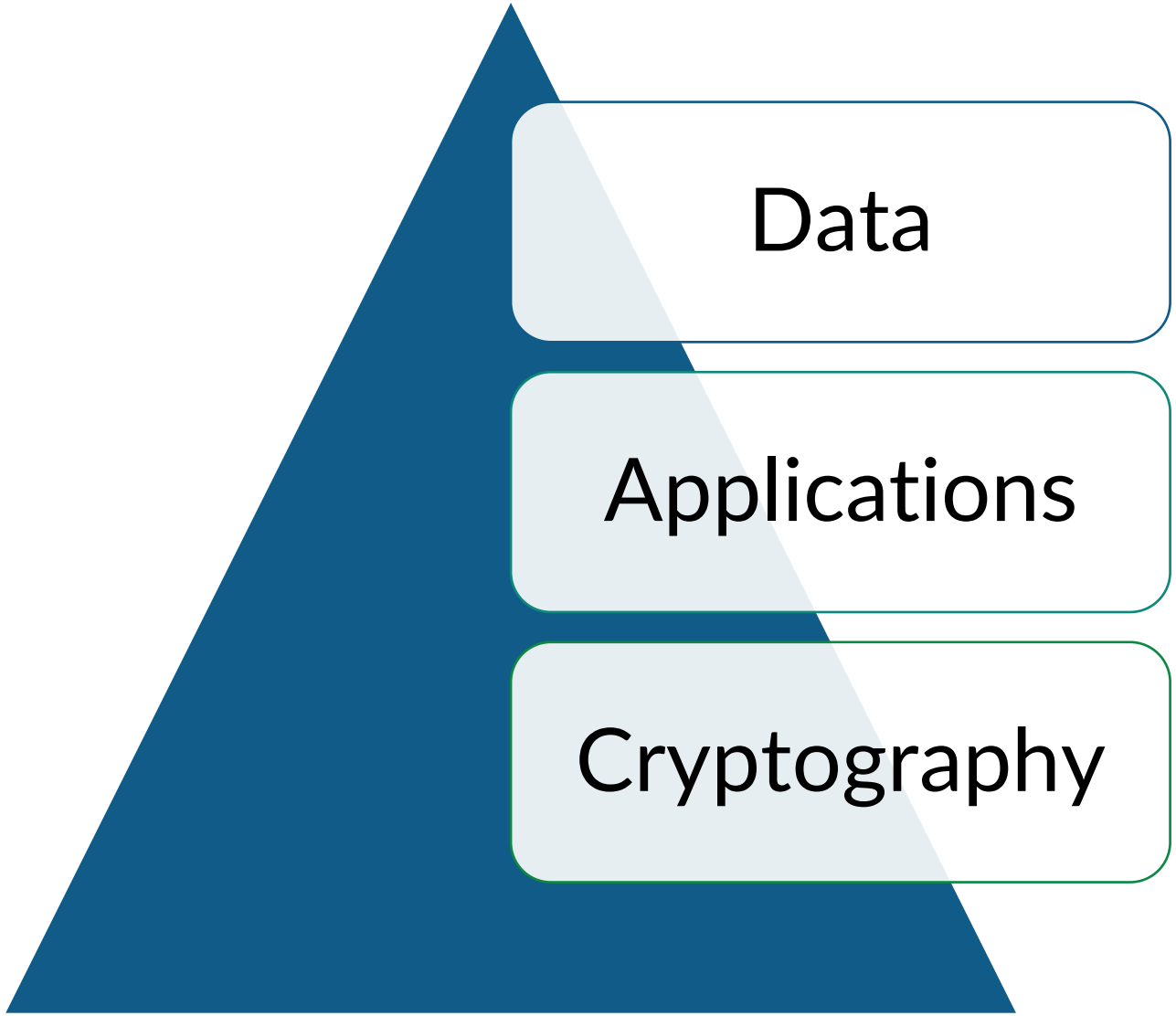
Transition Phases



Copyright © 2026 Secure Ideas LLC

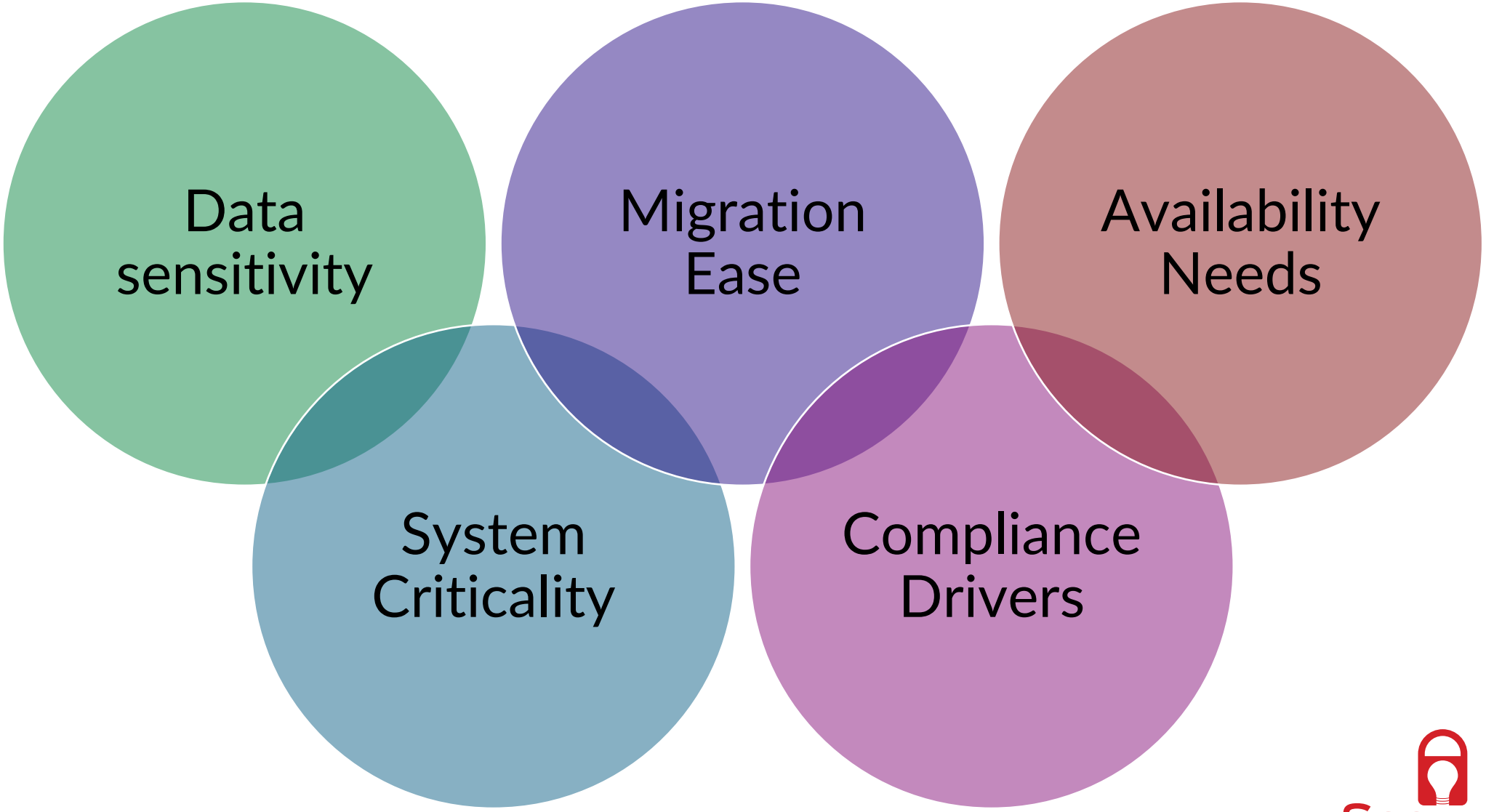
Secure Ideas
professionally evil®

Phase 1: Inventory



Copyright © 2026 Secure Ideas LLC

Phase 2: Prioritization



Copyright © 2026 Secure Ideas LLC

Phase 3: Planning and Testing



Testing Lab

Cooperation with Partners

Real-World Code

Consider Roll-back

Real Metrics

Copyright © 2026 Secure Ideas LLC

Secure Ideas professionally evil®

Phase 4: Implementation



Copyright © 2026 Secure Ideas LLC
Secure Ideas professionally evil®



Operational Challenges

Copyright © 2026 Secure Ideas LLC

Operational Challenges



Copyright © 2026 Secure Ideas LLC

Secure Ideas
professionally evil®



Communicating to Leadership

Copyright © 2026 Secure Ideas LLC

Secure Ideas
professionally evil®

Communicating to Leadership

Be Clear

- Don’t use jargon
- Analogies are good in moderation
- Don’t exaggerate

Understanding

- Focus on what we know
- Be open about projections and assumptions

Business Focus

- Understand OUR risks
- Know our systems
- Data sensitivity and longevity is key

Copyright © 2026 Secure Ideas LLC

Objections Answered

1. Quantum is decades away

- HNDL is happening

2. Vendors will handle it

- They are waiting on demand and need our requirements

3. This isn't a real threat yet

- CISA, NIST, and the NSA disagree with that. ☺

Copyright © 2026 Secure Ideas LLC

Manage Up and Down



Copyright © 2026 Secure Ideas LLC

Questions?



Kevin Tackett
kevin@secureideas.com
904-403-8024