

*The Cyber Breakfast Club*®

**Mr. Mike Charobee**

Founder of SaaS Security Outfitter CYBER BUYER®  
President and Founder of The Cyber Breakfast Club  
6 Regional Chapters and over 200 Members  
Nationwide  
<https://www.linkedin.com/in/mikecharobee/>



# PQC: A Short Primer

**Presented to Cyber Breakfast Club**

**Wednesday, November 4, 2025**

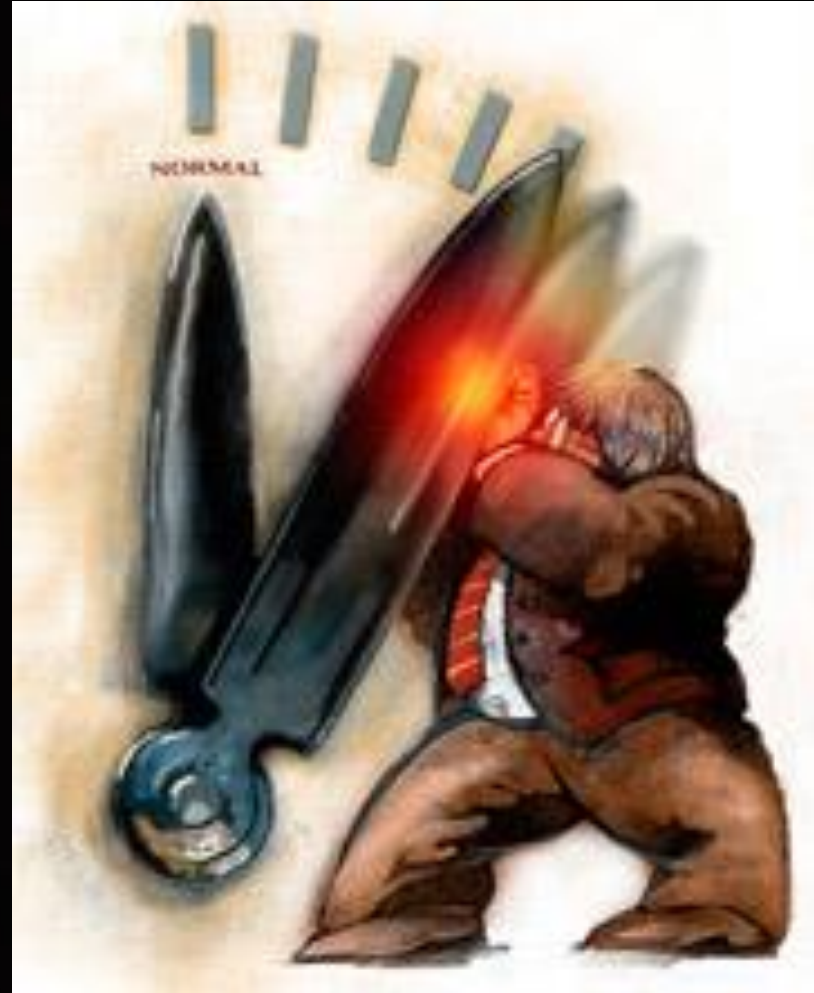
**From Chicago, (Wicker Park), Illinois, USA**

**William Slater  
President & CEO  
Slater Technologies, Inc.**

# PQC: A Short Primer

## Agenda

- Disclaimer
- Introduction
- What Is PQC?
- What is Q-Day?
- NIST PQC Standards
- Quantum Readiness
- Mosca's Theorem
- Cryptographic Agility
- Forget Q-Day Predictions
- PQC Timelines and Roadmap
- Dirty Secrets
- Conclusion
- Questions
- References
- About Me



# PQC: A Short Primer

## Disclaimer

This presentation will be delivered in September 2025 at the request of the organizers of the Australian Chapter of the Quantum Security Defence.

The content presentation is from William Favre Slater, III, a private U. S. Citizen, & President and CEO of Slater Technologies, Inc., and his research sources. It was prepared and presented with Good Will as a Service to Benefit the Good Citizens of Cyber Breakfast Club, and not as a representative of the U.S. Government or any other organization.

Mr. Slater only represents himself in his dealings with the Citizens of Cyber Breakfast Club and is solely responsible for his comments, content, and research.

# Enter the Quantum Zone



# PQC: A Short Primer

## Introduction

- **PQC, Post-Quantum Cryptography, has risen to the forefront as a crucial topic as people have realized the rapid advancement of Quantum Hardware Development is a reality and that the capabilities and impacts of Cryptographically Relevant Quantum Computers ( CRQC ) will be considerable.**
- **Shor's Algorithm, a cryptanalytical algorithm developed by Peter Shor at MIT in 1994 will easily break complex ciphers such RSA and ECC when Quantum Computers reach the capability to have the number of Qubits to run the program(s) that have implemented this algorithm. ( estimated to be approximately 1 million Qubits )**
- **NIIST ( National Institute of Standards and Technology – under the U.S. Department of Commerce) has developed Cryptographic Standards that are supposed to be Quantum Safe.**
- **The time to act on PQC Migration Projects is NOW, because the average Enterprise PQC Project takes 3 to 7 years to complete.**
- **We will briefly discuss HNDL and WHY it is a significant problem.**

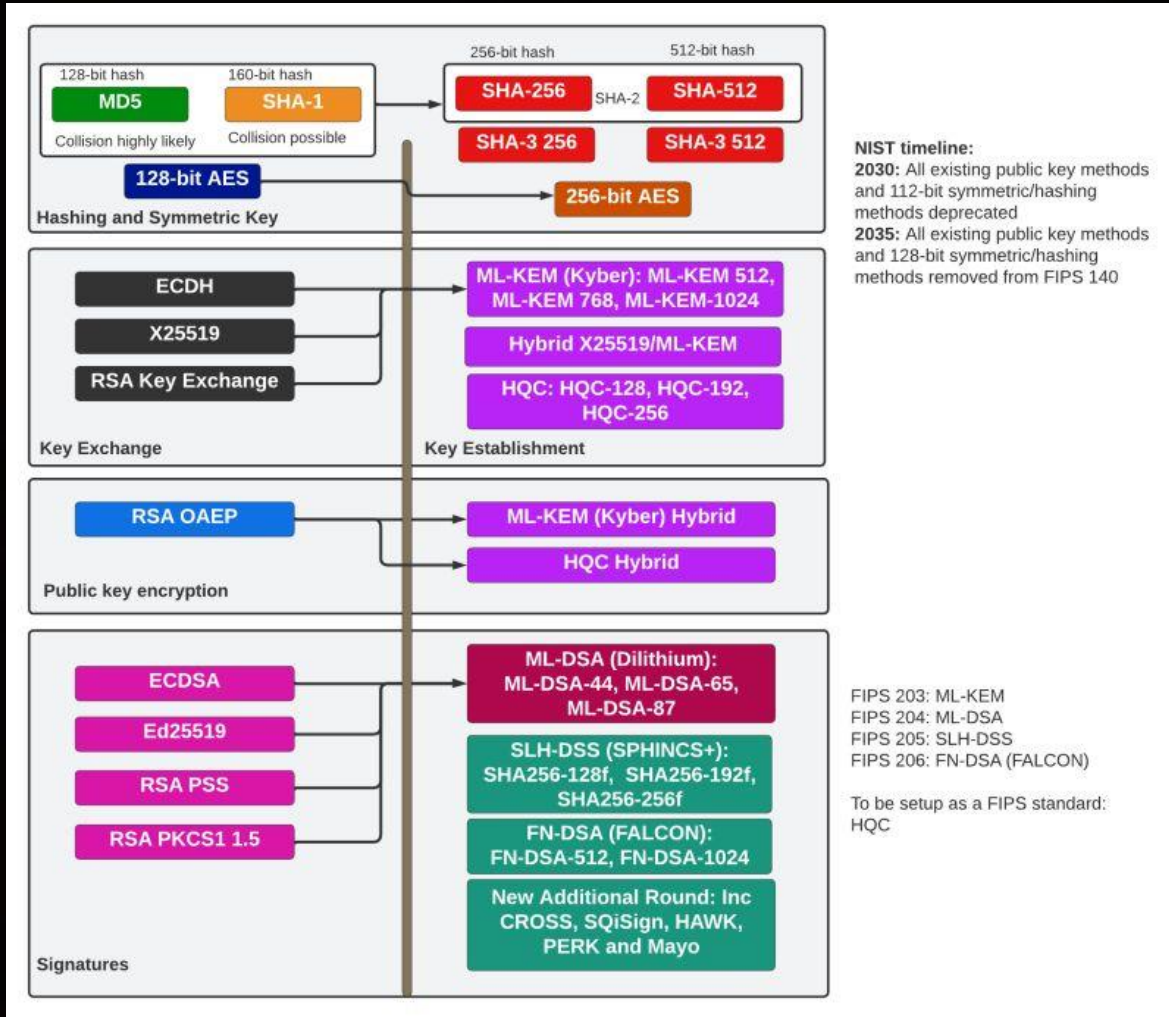
# PQC: A Short Primer

## What Is PQC?

- **PQC is Post-Quantum Cryptography.**
- **It is a standard that has been developed to withstand efforts by Quantum Computers to break standard cryptography. NIST is the most prevalent set of PQC Standards, but there are other standards available in Europe, Japan, China, etc.**

# PQC: A Short Primer

## What are we converting?



Source:  
Professor Bill Buchanan

# PQC: A Short Primer

## What is the PQC Migration Work Like?

It Is Hard to Do. Very, Very Hard!

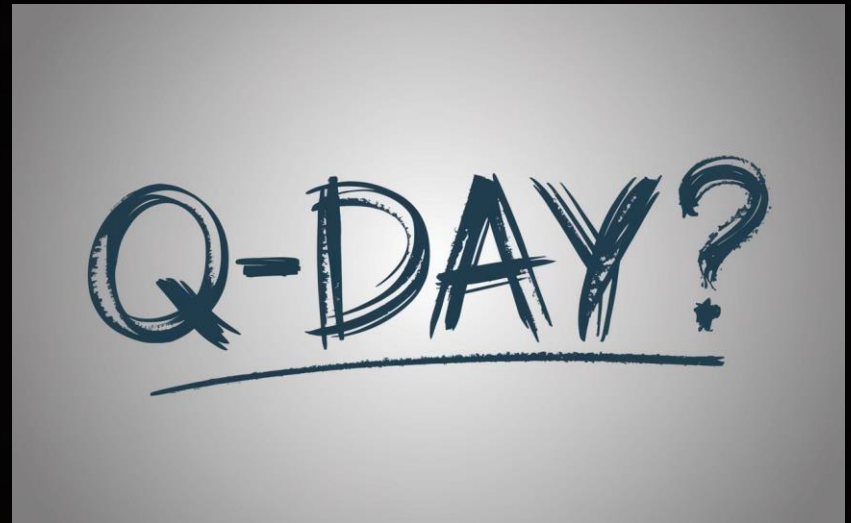
- **Not “Just Patch OpenSSL”:** PQC migration is an enterprise-wide overhaul, touching nearly every system using crypto
- **Analogy - Bigger than Y2K:** Far more complex than Y2K; we have millions of devices, apps, and cloud services all using cryptography
- **Crypto Everywhere:** No system is exempt - OS, apps, databases, IoT, communications, etc. all rely on encryption/authentication

Slide Source: Mr. Marin Ivezic, 2025.

# PQC: A Short Primer

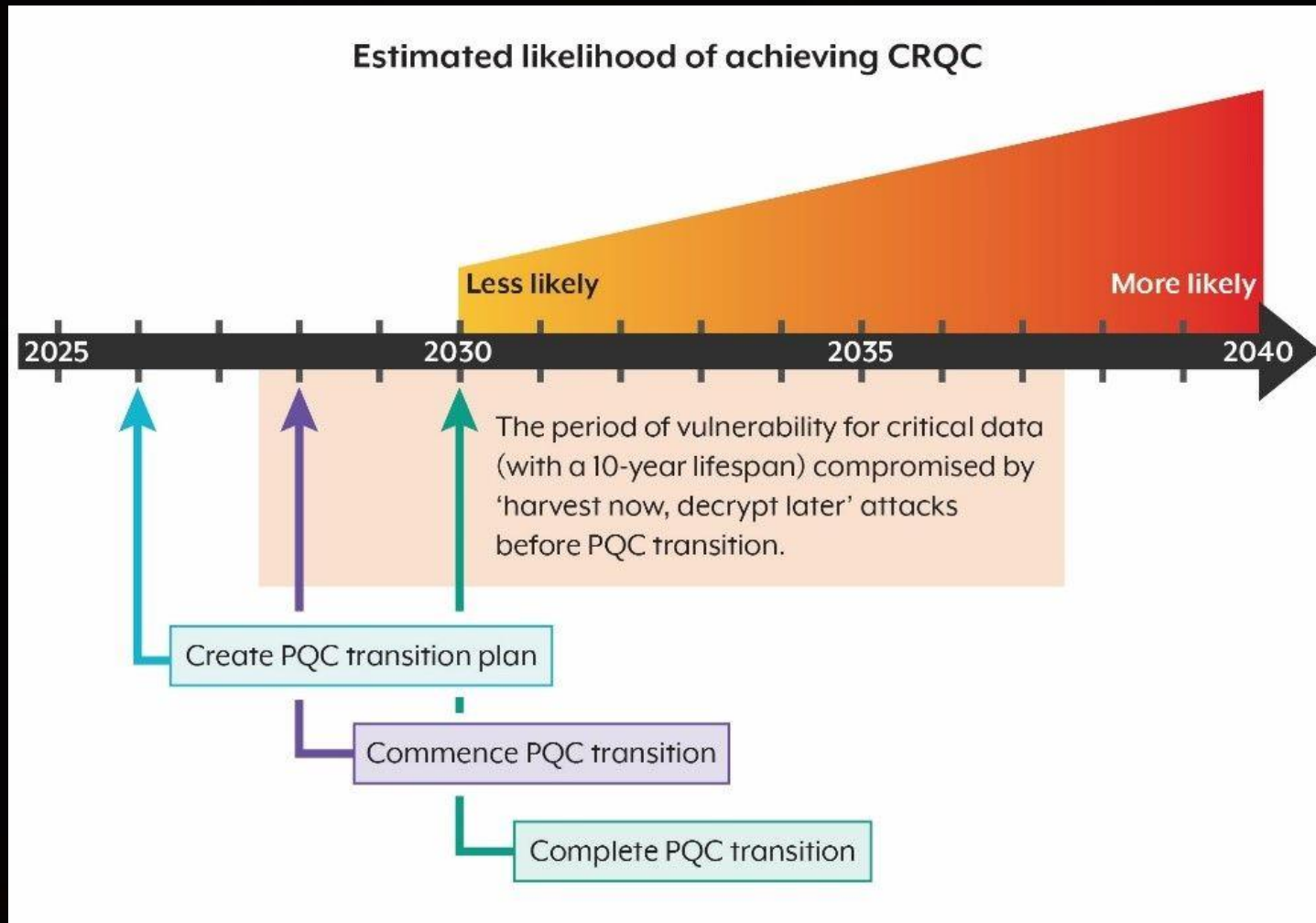
## What Is Q-Day?

- **Q-Day is the day when Quantum Computers reach the capacity to easily run programs that have implemented Cryptanalytic Algorithms such as Shor's Algorithm.**



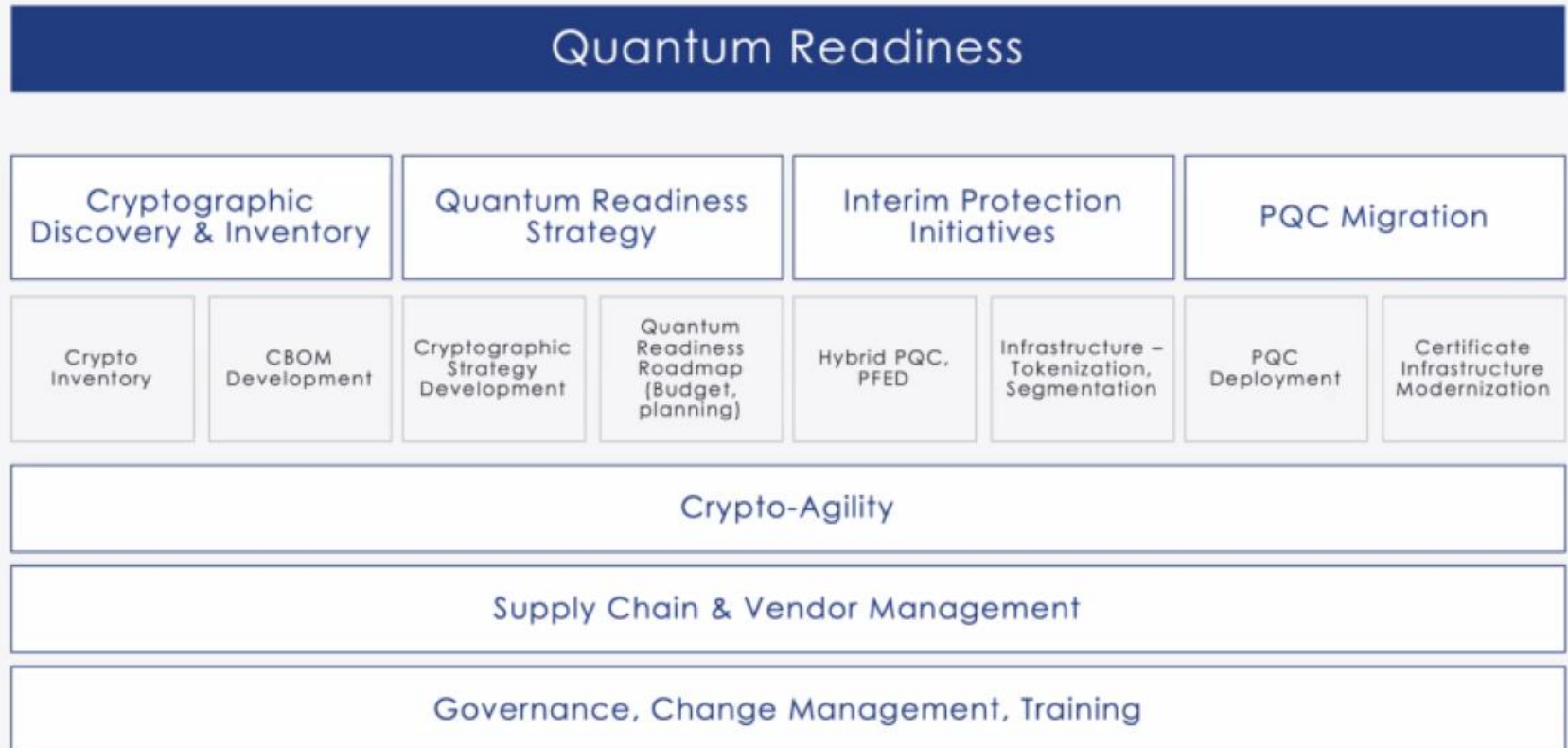
# PQC: A Short Primer

## Estimated Likelihood of Achieving CRQC



# PQC: A Short Primer

## Quantum Readiness



Slide Source: Mr. Marin Ivezic, 2025.

# PQC: A Short Primer

## Forget the Q-Day Predictions – Regulators, Stakeholders & Compliance People

### Forget Q-Day Predictions

- Regulators
- Clients
- Insurers
- Vendors
- Investors
- Analysts
- Auditors

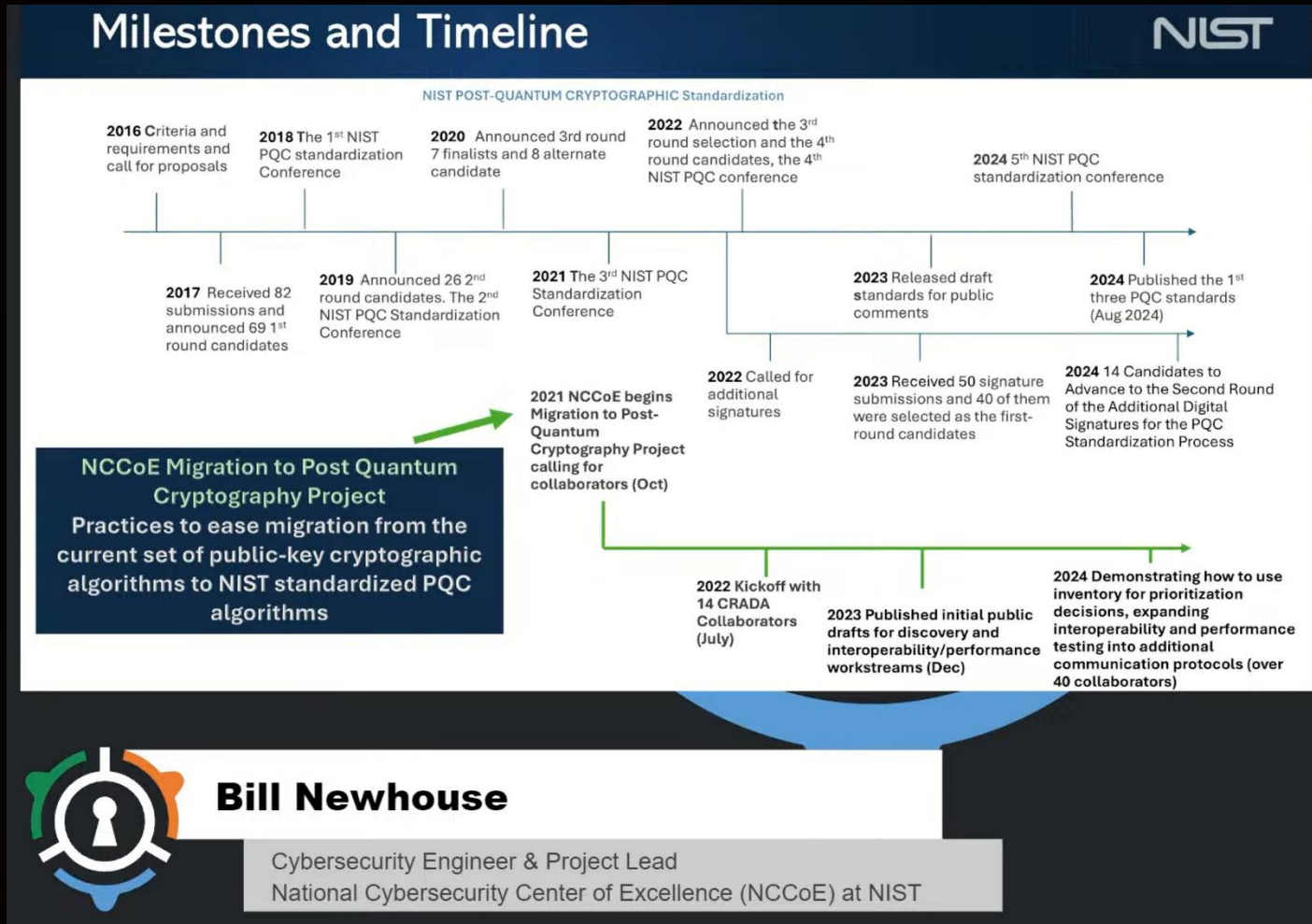
...have set up the **deadline of 2030-2035 for quantum readiness**



Slide Source: Mr. Marin Ivezic, 2025.

# PQC: A Short Primer

## PQC Timeline – Historical Perspective



**Bill Newhouse**

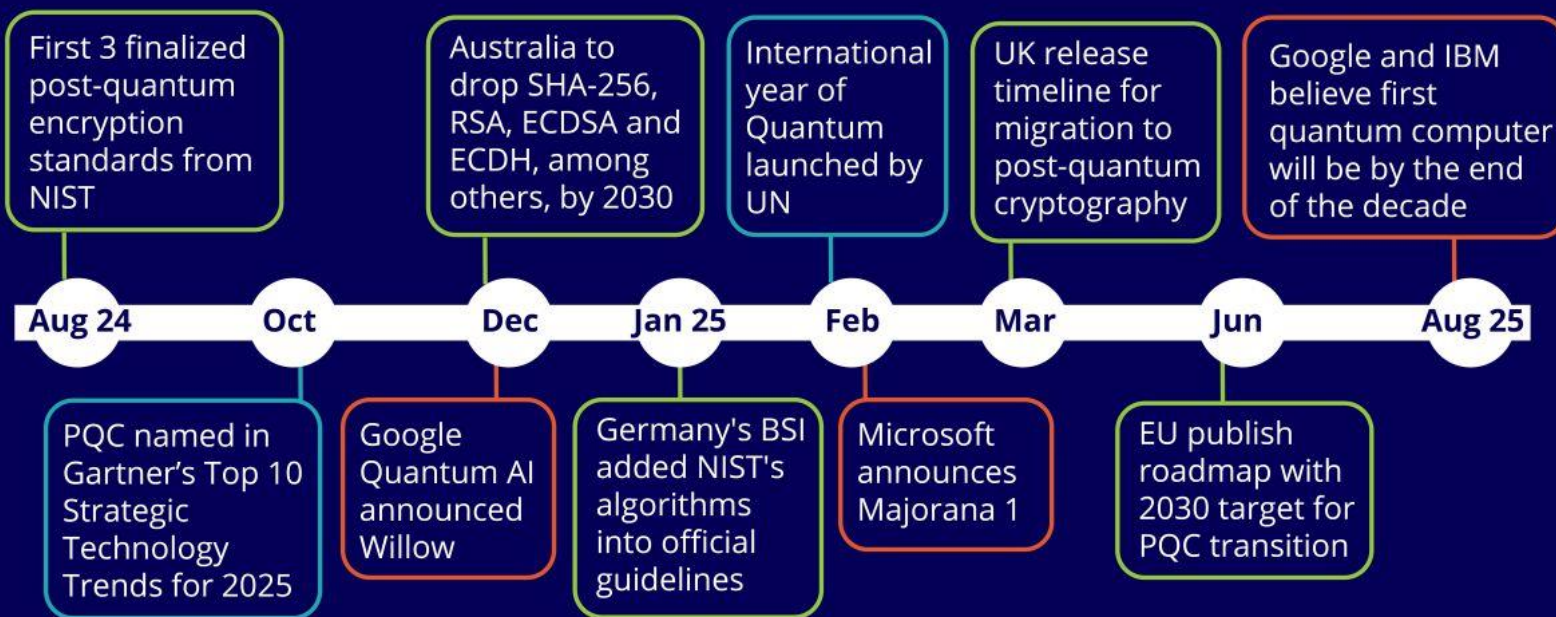
Cybersecurity Engineer & Project Lead  
National Cybersecurity Center of Excellence (NCCoE) at NIST

# PQC: A Short Primer

## Timeline of PQC Momentum

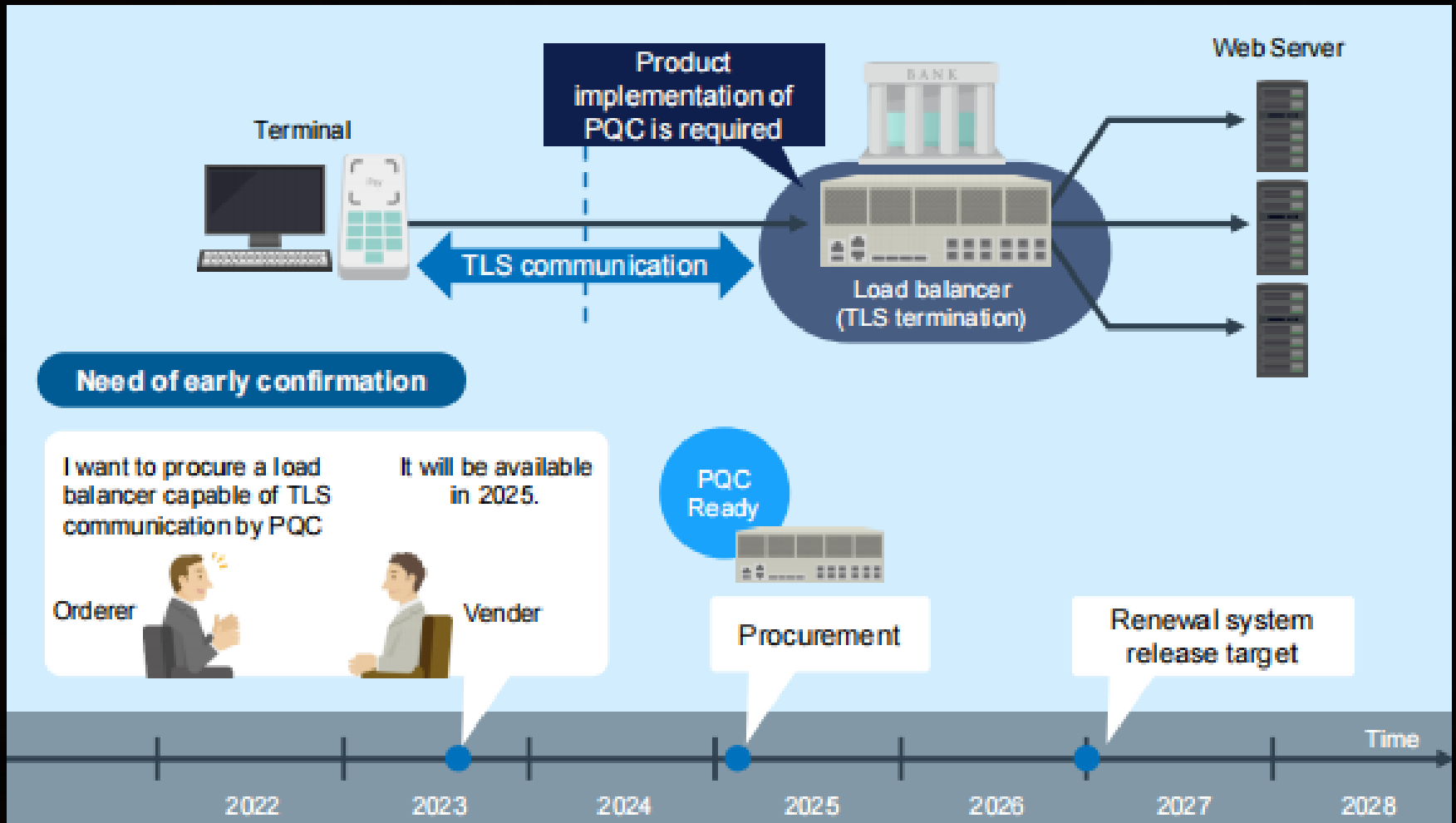
### Cutting Out the Quantum Noise

Timeline: A year of PQC momentum



# PQC: A Short Primer

## Timeline of PQC Momentum



# PQC: A Short Primer

## Mosca's Theorem

### MOSCA'S THEOREM

Based on Mosca's Theorem  $(X+Y)>Z$ , if the amount of time you need your encrypted data to be secure (X) + how long it will take to implement a quantum secure solution into your current infrastructure (Y) is greater than how long it will take to develop a sufficiently strong enough scale quantum computer (Z), then it's time to worry.

$$X + Y > Z$$

How long do you need your encrypted data to be secure?

How long will it take to implement a quantum secure solution into your current infrastructure?

How long will it take to develop a sufficiently strong enough scale quantum computer?

Source: <https://www.theqrl.org/blog/grasping-the-quantum-threat-with-moscas-theorem/>,

# PQC: A Short Primer

## Cryptographic Agility

“Cryptographic agility, or crypto-agility, is the ability of a system to quickly and easily switch between different cryptographic algorithms and parameters in response to changing security needs or vulnerabilities. This flexibility helps maintain security and adapt to new threats without significant disruptions to the system's infrastructure.”

- Brave AI
- Additional resource: RFC 7696
  - <https://www.rfc-editor.org/rfc/pdf/rfc7696.txt.pdf>

# PQC: A Short Primer

## PQC Migration High-Level Project Plan



### SCHEDULE

- Planning (2 months)
- Assessment (3 months)
- Implementation (8 months)
- Testing (3 months)

### ROLES AND RESPONSIBILITIES

- Project Manager--Manages overall project
- Migration Team--Executes technical tasks
- Security Analyst--Evaluates cryptographic risks
- QA Team--Conducts migration

### QUALITY ASSURANCE

- Define acceptance criteria for each phase
- Perform regular code reviews
- Verify in compliance with security standards

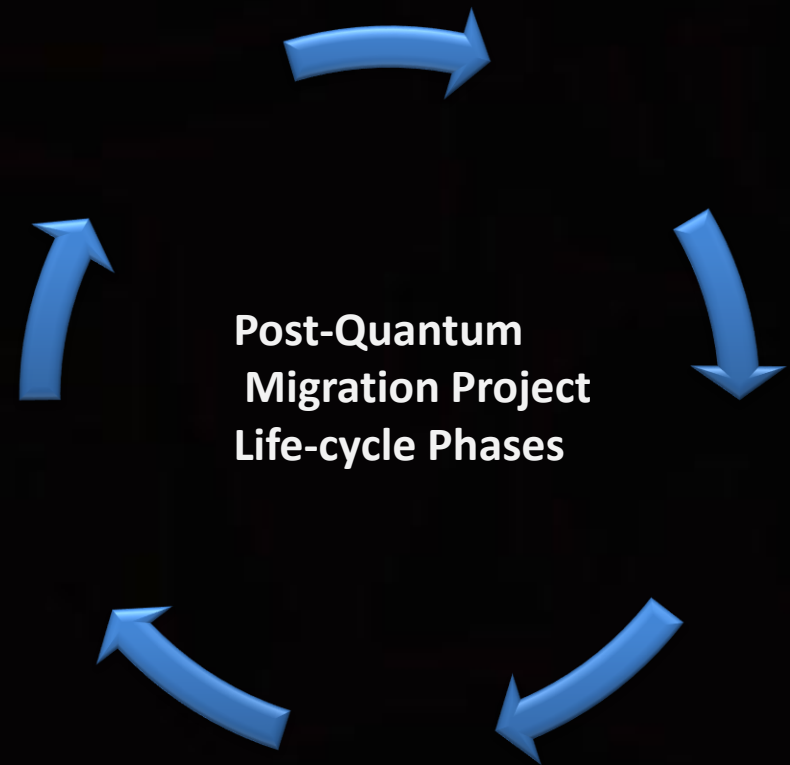
### PROJECT CHARTER

- Objective: to migrate systems to post-quantum cryptography (PQC)
- Focus: on security, and minimal disruption

# PQC: A Short Primer

## PQC Migration High-Level Project Phases

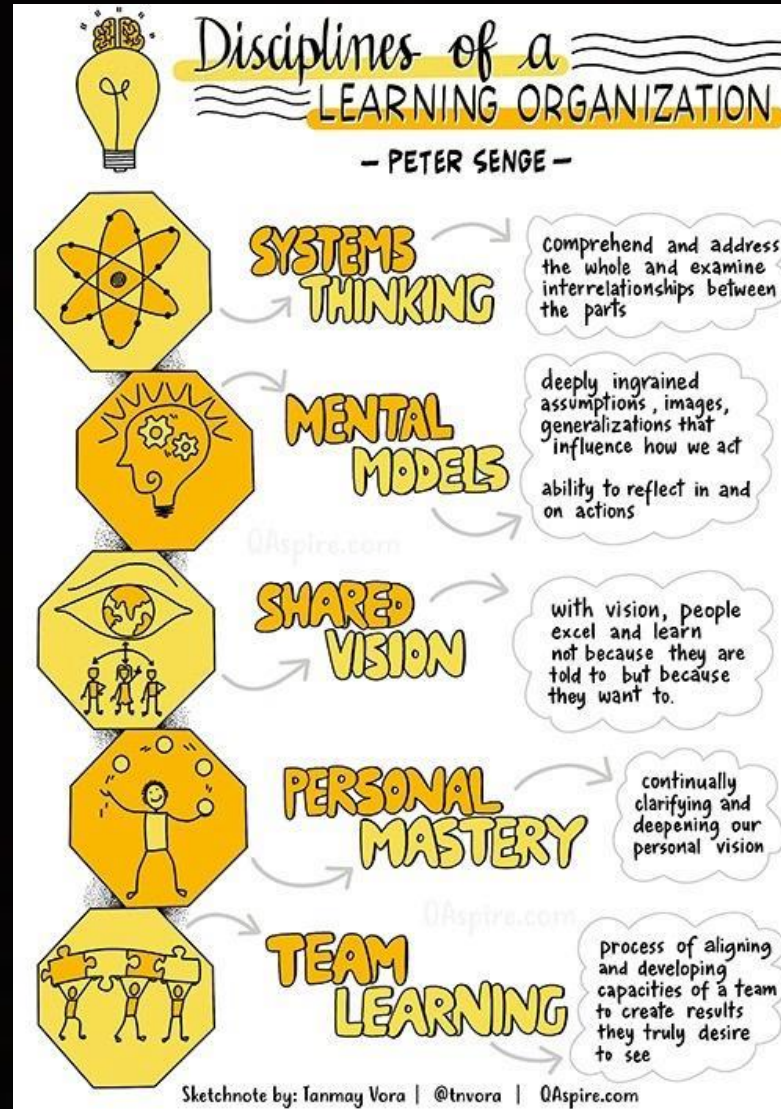
Phase No.	Brief Description
1	Education
2	Create a Plan
3	Collect Data
4	Analyze
5	Take Action / Remediate
6	Review and Improve as Needed



Source: Roger Grimes, Cryptography Apocalypse, 2020.

# Building a PQC Migration Team

How Do You  
Establish and  
Operate a PQC  
Migration Team?  
Peter Senge  
Learning Team  
Disciplines



# PQC: A Short Primer

## PQC Migration Project Roles

### Project Team Roles

Senior Management Sponsor

Project Leader with Quantum Computing Knowledge

IT Security Manager

Other IT Employees as required

Cryptography Subject Matter Expert

End User Representative

Communications Specialist

Accounting/Budgeting/Purchaser

Inventory Manager/Specialist



Source: Roger Grimes, Cryptography Apocalypse, 2020.

# PQC: A Short Primer

## PQC Migration Project Steps

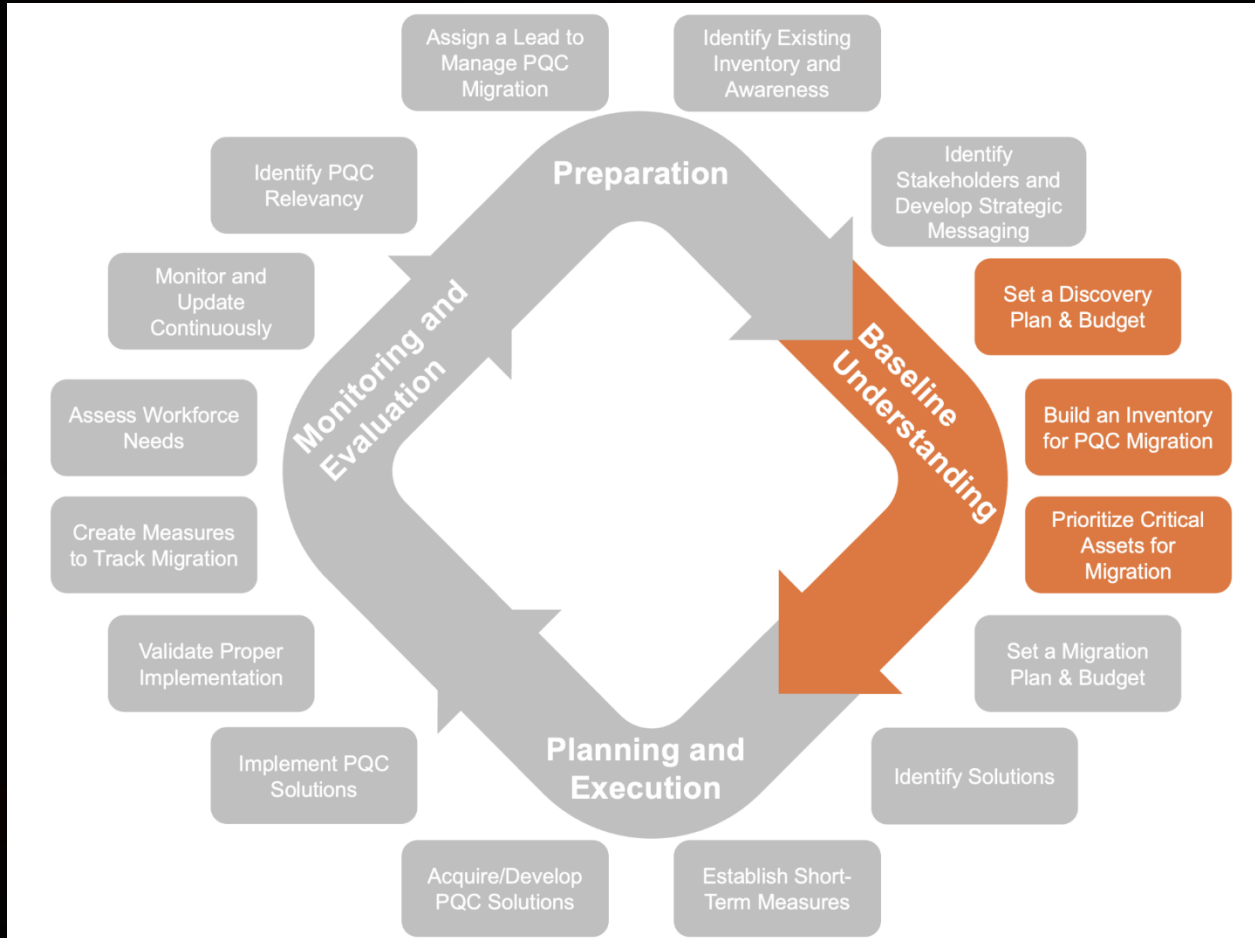
Project Steps	Estimated Time to Complete
Educate	1 month
Form a Project Team and Plan	1 month
Create a Timeline	1 month
Take a Data Protection Inventory	3 months
Analyze the Quantum Plan and Make Recommendations	6 months
Prevent Future Data Leaks	3 months
Strengthen existing traditional Cryptography	12 months
Move to Quantum-Resistant Cryptography	60 months
Move to Quantum-Hybrid Techniques	60 months
Go fully Quantum	Undetermined



Source: Roger Grimes, Cryptography Apocalypse, 2020.

# PQC: A Short Primer

## PQC Migration Project Roadmap



Source: Mitre PQC Coalition, 2025, <https://pqcc.org/>

# PQC: A Short Primer

## Preparing for a PQC Migration

### Prepare for Post-Quantum Cryptography

#### Key Things to Consider

01

Integrating quantum computing technology into existing IT infrastructure will be a complex process.

02

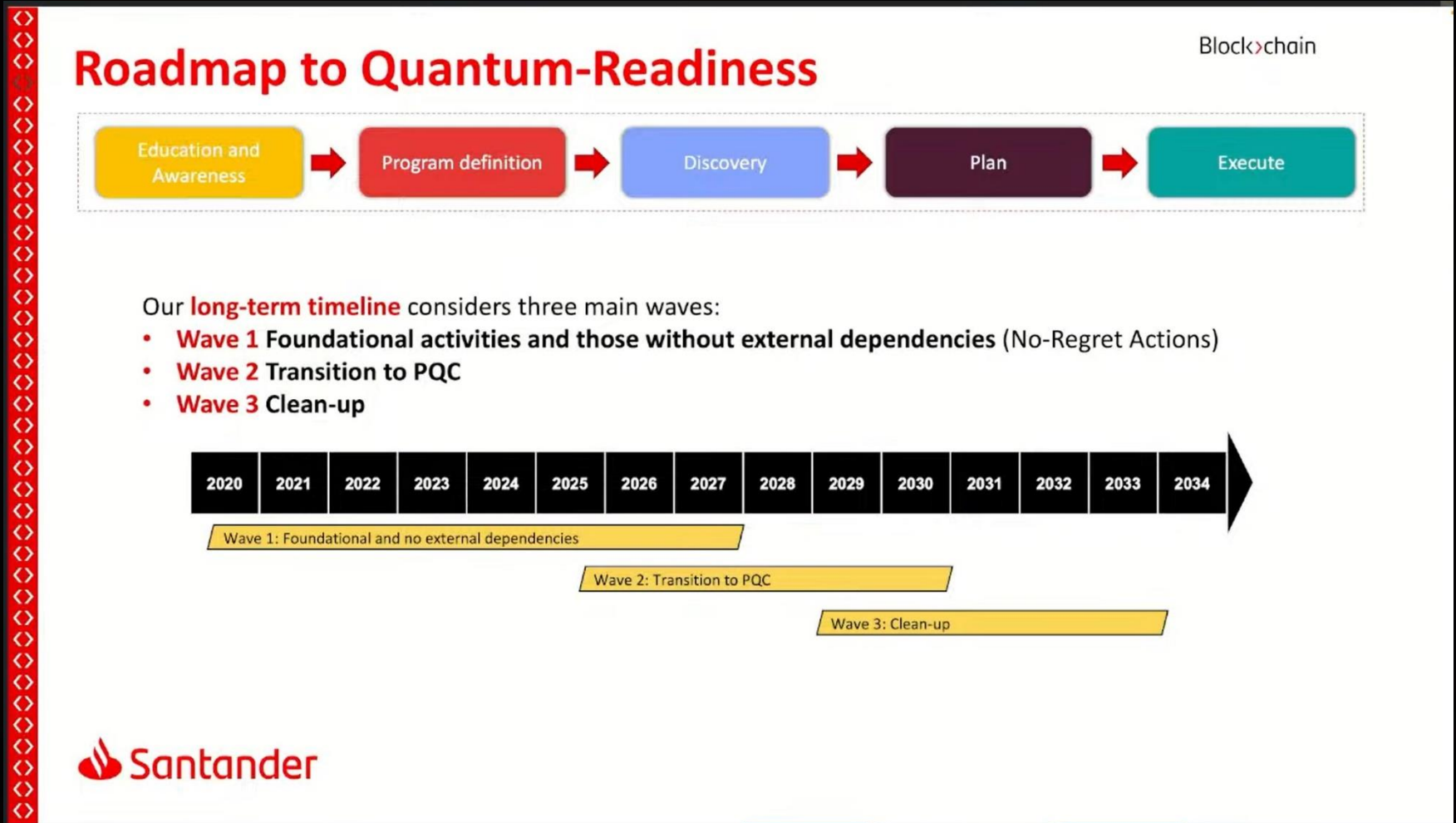
The effort to upgrade to quantum-resilient cryptography will be significant.

03

The amount of time remaining will decrease every day.

# PQC: A Short Primer

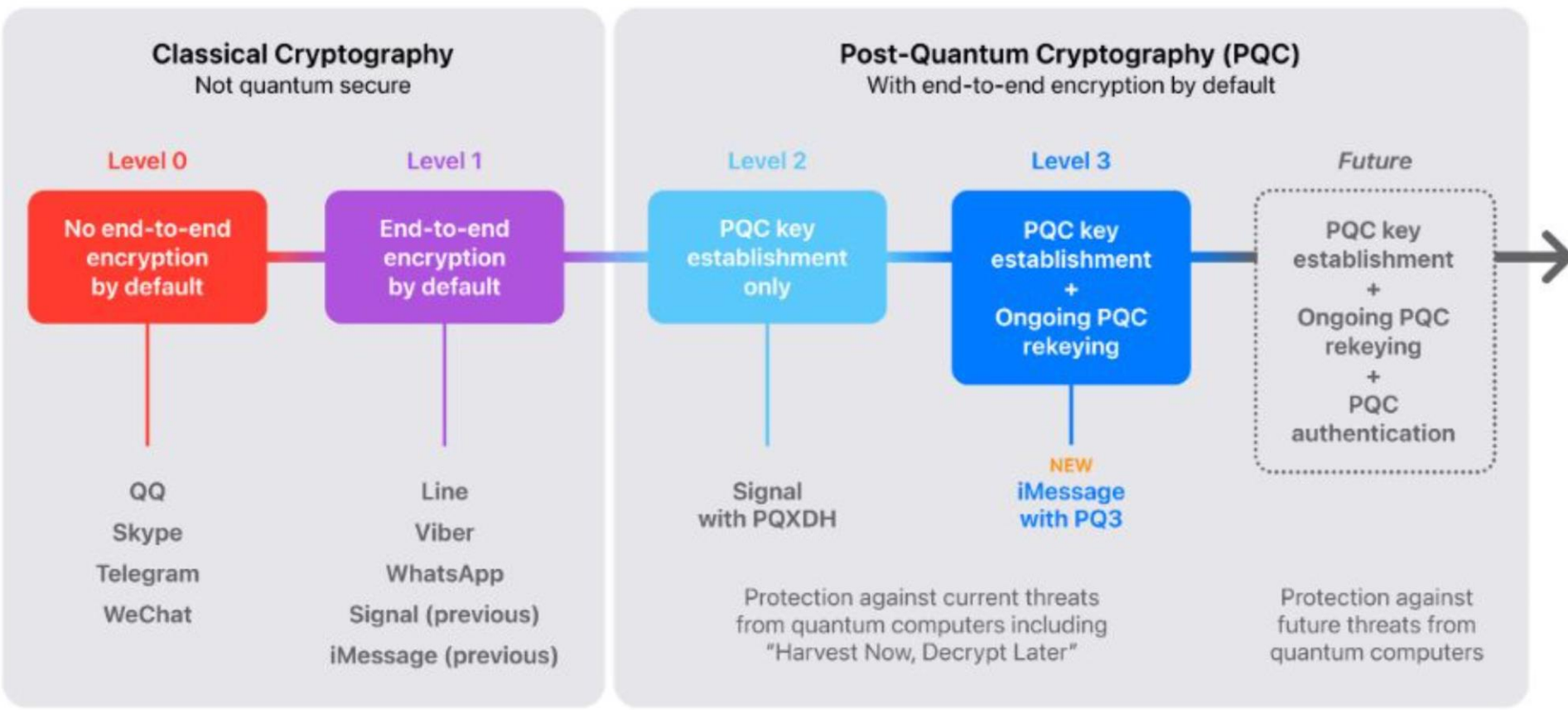
## Timeline – Roadmap to Readiness



# PQC: A Short Primer

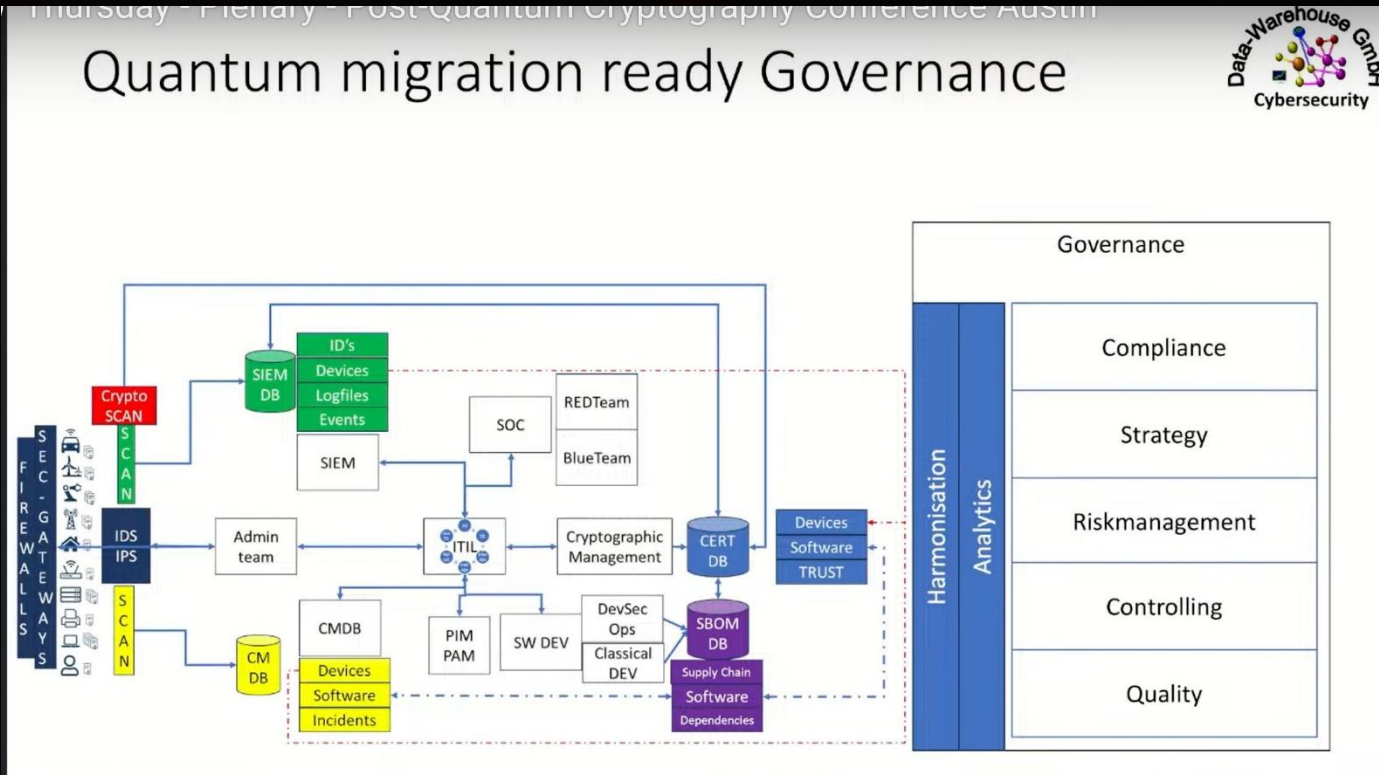
## Quantum-Secure Cryptography in Messaging Apps

### Quantum-Secure Cryptography in Messaging Apps



# PQC: A Short Primer

## PQC Migration and IT Governance



**Alexander Löw**

CEO at Data-Warehouse

# PQC: A Short Primer

## PQC and Presidential Politics

PQC Topic	Biden EO 14144 (Jan 2025)	Trump EO Amendment (Jun 2025)	Difference
Recognition of Quantum Threat (CRQC)	CRQC described as a major threat that could break public key cryptography globally.	Same language retained verbatim in §4(f).	No difference.
CISA PQC Product Category List	DHS/CISA, in coordination with NSA, must publish and maintain list of PQC-ready product categories.	Same requirement, with explicit deadline of Dec 1, 2025.	Only change: fixed date instead of relative timeline.
PQC Procurement Trigger	Any product solicitation 90 days after listing must require PQC support.	Removed entirely. No procurement enforcement based on PQC readiness.	Deletes linkage between the CISA list and mandatory government purchasing.
Agency Deployment of PQC/Hybrid Algorithms	Agencies must adopt PQC or hybrid KEM as soon as technology becomes available.	Removed entirely.	Agencies are no longer obligated to deploy PQC even when available.
TLS 1.3 (or successor) Mandate	NSA (for NSS) and OMB (for non-NSS) must issue guidelines to ensure TLS 1.3 or better is adopted no later than Jan 2, 2030.	Same requirement retained with a fixed publication deadline: Dec 1, 2025.	Only deadline phrasing changes; goal remains.
International PQC Engagement	Requires State and Commerce to promote global adoption of NIST-standard PQC within 90 days.	Removed. No diplomatic or export coordination on PQC.	Deletes U.S. international advocacy on post-quantum migration.
SSDF and Patch Guidance (NIST SP 800-218, 800-53)	Mandated frequent updates to SSDF and security controls, with a focus on PQC software practices.	Kept intact in §2(c), including Dec 2025 update deadline.	No change in this technical guidance track.

# PQC: A Short Primer

## Q-Day Estimator

q-day.org/crqc-readiness-benchmark-q-day-estimator/

Q-DAY

Q-Day Estimator

My Prediction & Timeline

Articles

Search for

About Me

Home / CRQC Readiness Benchmark (Q-Day Estimator)

## CRQC Readiness Benchmark (Q-Day Estimator)

Read about the approach and relevant attributes in the two articles above. Then use the CRQC Readiness Benchmark (Q-Day Estimator) tool below to turn assumptions into a defensible, crypto-specific forecast. The tool converts four inputs, LQC (logical qubits), LOB (logical operations budget), QOT (logical ops/sec), and an annual growth factor, into a Composite CRQC Readiness Score and a projected “Q-Day” (when week-scale factoring of RSA-2048 becomes practical). Start with Conservative / Median / Aggressive presets, then tweak to match vendor claims or your own view of roadmaps and error-correction progress. This is intentionally focused on cryptographic breakability, not generic “quantum advantage,” so it may diverge from headline qubit counts.

Source: <https://q-day.org/crqc-readiness-benchmark-q-day-estimator/>

# PQC: A Short Primer

## Q-Day Estimator

The screenshot shows the 'Q-Day Estimator' web application. The header includes the 'Q-DAY' logo, a navigation menu with 'Q-Day Estimator', 'My Prediction & Timeline', and 'Articles', and a search bar. The main content area is titled 'CRQC Readiness Benchmark (Q-Day Estimator)' and includes a brief introduction: 'An interactive way to explore how close we may be to a cryptographically relevant quantum computer (CRQC) for breaking RSA-2048. Adjust assumptions below to see how the projected Q-Day shifts. Methodology & discussion. Disclaimer: this tool is for experimentation and scenario analysis only.'

Below the introduction are several input sections:

- Scenarios:** Buttons for 'Conservative', 'Median', and 'Aggressive', with a note: 'Load a starting scenario, then tweak parameters to explore.'
- Logical Qubit Capacity (LQC):** A dropdown menu set to '10'. Description: 'Count of error-corrected (logical) qubits available.'
- Logical Operations Budget (LOB):** An 'Exponent (10^x):' dropdown set to '12' and a value dropdown set to '1000000000000'. Description: 'Reliable logical operations available (circuit depth).'
- Quantum Operations Throughput (QOT):** An 'Exponent (10^x):' dropdown set to '6' and a value dropdown set to '1000000'. Description: 'Logical operations per second (throughput).'
- Growth factor (x per year):** A dropdown menu set to '2.5'. Description: 'Annual capability multiplier for the composite score.'
- Advanced formula (optional):** A dropdown menu with a right-pointing arrow.

On the right side, there are two summary boxes:

- Composite CRQC Readiness Score:** A large box displaying '0.010'.
- Projected Q-Day:** A box displaying '2031 (6 years from now)'.

Below these is a line graph titled 'Projected CRQC Readiness score over time'. The x-axis represents years from 2025 to 2045, and the y-axis represents the 'Q-Day threshold (ex)'. A blue line shows the readiness score increasing over time, crossing a horizontal dashed line at the 'Q-Day 2031' threshold around the year 2031.

At the bottom, there is a 'CRQC Explainer (AI)' section with a 'Persona:' dropdown set to 'CISO', a 'Strictness:' dropdown set to 'Allow Synthesis', and buttons for 'Explain above result', 'Ask PostQuantum.com', 'PDF', and 'Reset'.

Source: <https://q-day.org/crqc-readiness-benchmark-q-day-estimator/>

# PQC: A Short Primer

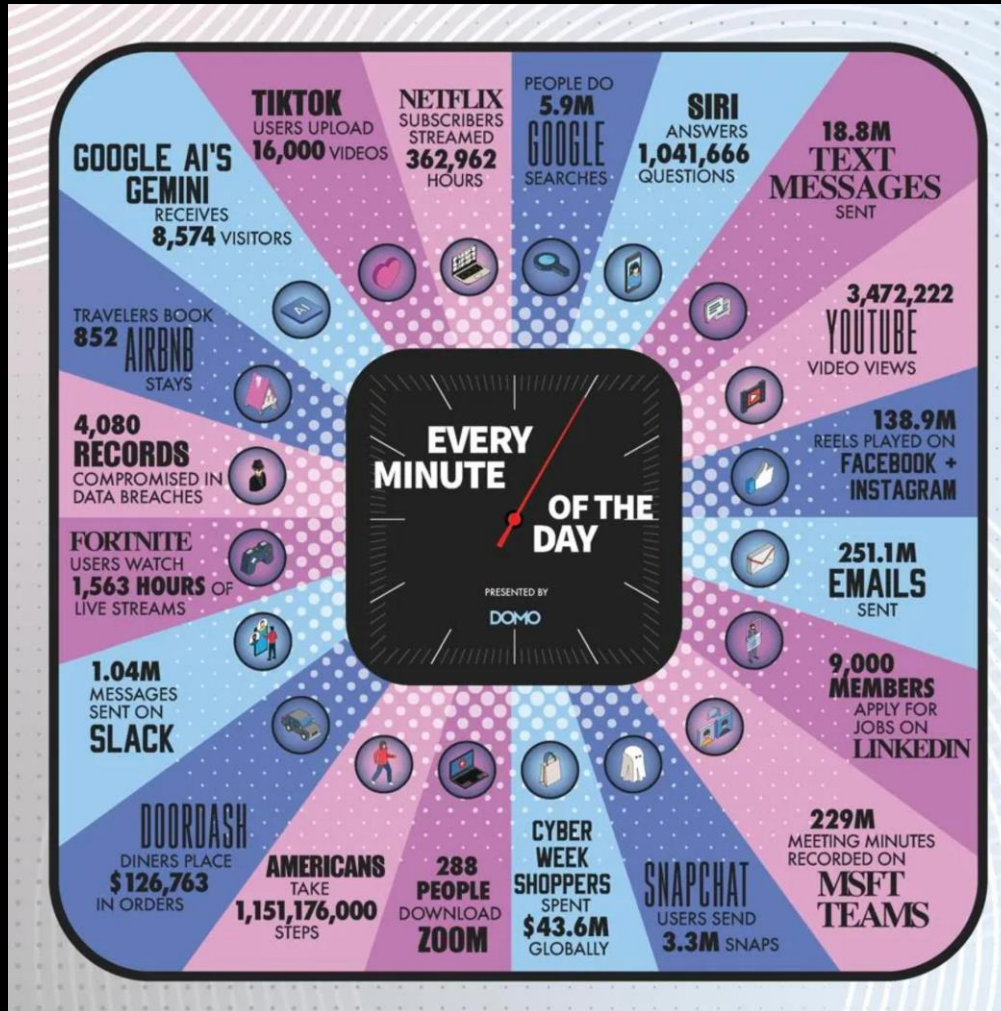
## Two Very Dirty Secrets

- How Networked Computers Communicate
  - They transmit electronic messages whether cryptography is present or not, and whether it is configured properly, or not.
- Harvest Now, Decrypt Later ( HNDL ) is a very cruel, harsh reality.
  - You can accomplish a perfect PQC Migration project and still be incredibly vulnerable, because of PAST network communication activity. ( I wish this was not true, but it is TRUE.)

# What Is Harvest Now, Decrypt Later? ( HNDL )

- Data that traverses the Internet is usually encrypted.
- The Bad Guys and Nation States are capturing and storing this data that is encrypted using older encryption algorithms.
- Between 2028 and 2031, when CRQC computers become commonplace, the harvested data can be decrypted at the time and place of the Bad Guys' choosing and they use this decrypted data to their advantage.
- Note that the decrypted data can also be data that belongs to organizations that have completed their PQC Migrations, because the harvest data was encrypted using older algorithms that are vulnerable to cryptanalytic attacks of Quantum Computers.

# Internet Minute - 2025



Source: <https://bondhighplus.com/blog/what-happens-in-an-internet-minute/>

# Internet Minute – 2015 to 2025

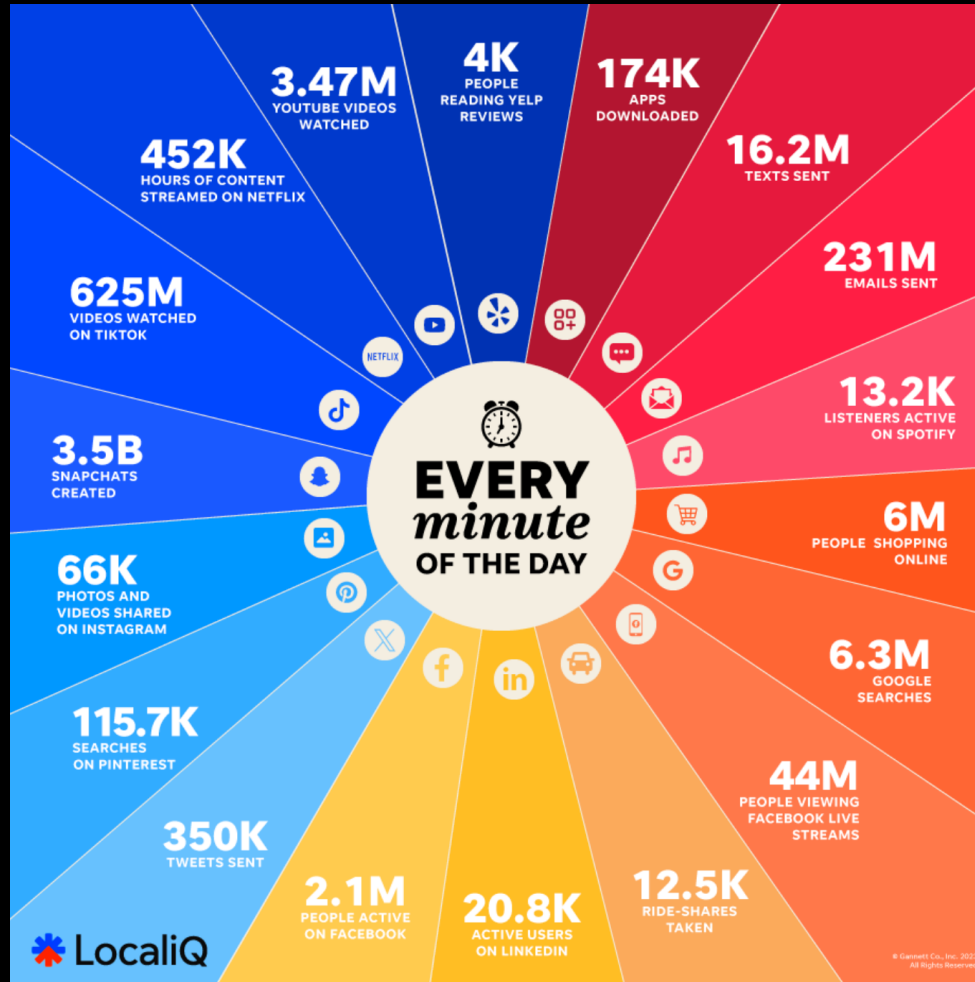


Year	Emails Sent	Google Searches	YouTube Views	TikTok Views	Online Spend	App Downloads	Instagram Activity
2025	231M+	6.3M+	3.47M	625M videos watched	\$43.6M+	174K	66K photos shared
2024	231M	6.3M	3.47M	625M videos watched	\$43.6M (peak minute)	174K	66K photos shared
2023	231M	5.9M	3.67M	167M videos watched	\$1.5M+ (est.)	174K	694M songs streamed
2022	231M	5.9M	508 hrs uploaded	1B+ interactions	\$443K (Amazon only)	437K transfers	527K photos shared
2021	225M (est.)	5.7M (est.)	5.0M (est.)	167M (est.)	\$1.3M (est.)	450K (est.)	800K (est.) scrolling
2020	190M	4.1M	4.7M	N/A	\$1.1M	400K	694K scrolling
2019	188M	3.8M	4.5M	N/A	\$996K	390K	347K scrolling
2018	187M	3.7M	4.3M	N/A	\$862K	375K	174K scrolling
2017	156M	3.5M	4.1M	N/A	\$751K	342K	46K posts uploaded
2016	150M	2.4M	2.78M	N/A	\$203K	51K	527K photos shared
2015	204M	2M+	1.3M	N/A	\$83K	47K	3,000 uploads



Source: <https://bondhighplus.com/blog/what-happens-in-an-internet-minute/>

# Internet Minute - 2025



Source:  
<https://localiq.com/blog/what-happens-in-an-internet-minute/>



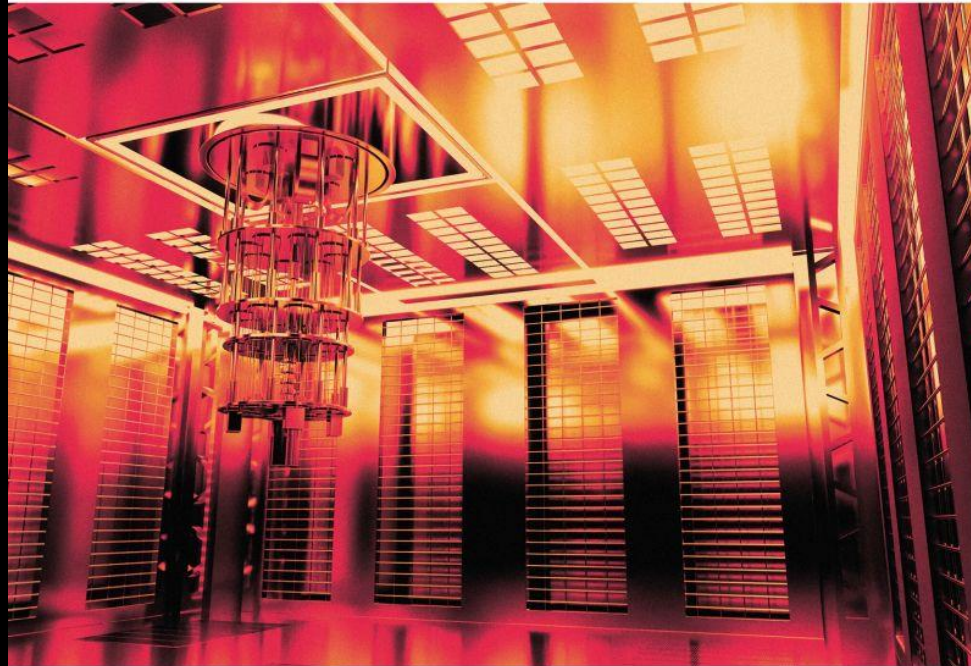
# PQC: A Short Primer

## Conclusion

- Q-Day is a reality, and unlike Y2K when we knew the deadline was December 31, 1999, we don't know the exact date. Many believe it will occur between 2028 and 2031.
- Regulators and Compliance Organizations are mandating the requirements to get these projects done.
- These projects are not easy and require time and effort by experts. Work with experts to get it done.
- Start now. Procrastination is three issues:
  - You may not finish before Q-Day
  - The longer you wait, the more expensive it will get
  - Regulatory issues may incur fines and in worst case, prison time.
- HNDL is the kind of technology problem that should have us ALL worried.

# HAPPY Q-DAY

Warning: It'll be the worst holiday in the history of the world.



BY AMIT KATWALA

ILLUSTRATIONS BY NICHOLAS LAW

# Q Day is the finish line for PQC readiness





# PQC: A Short Primer

## Questions and Answers



# *Supplemental Slides*


# Quantum References

- Ahsan, M., Meter, R V., and Kim, J. (2015). Designing a Million-Qubit Quantum Computer Using a Resource Performance Simulator. A scholarly article published at the ACM in December 2015. Retrieved from: <https://tinyurl.com/ya2q92xa>.
- Aaronson, S. (2013). Quantum Computing Since Democritus. Published by Cambridge University Press, Cambridge, UK.
-  Backes, K. (2025). "Quantum Sensors for Complementary PNT and Resilient Communications. Published and Compyrighted by Mitre Corporation. Retrieved from [https://www.westconference.org/WEST25/Custom/Handout/Speaker0\\_Session11709\\_1.pdf](https://www.westconference.org/WEST25/Custom/Handout/Speaker0_Session11709_1.pdf) .
- Bricmont, J. (2017). Quantum Sense and Nonsense. Published by Springer. Louvein la Nouve, Belgium.
- Bloom, S. (2024). "What Is Quantum Sensing and How Does It Work?". Published on December 24, 2024. Retrieved from <https://scientificorigin.com/what-is-quantum-sensing-and-how-does-it-work>.
- Chancé, A., et al. (2024). "AI-driven Quantum Molecular Sensing For Cybersecurity". A presentation to QSECDEF on November 24, 2024. Retrieved from <https://bit.ly/4dyhOgd> .
- Chongo. (2021). Homeless Interpretation of Quantum Mechanics. (Self-Published). Yosemite National Park, CA.
- Davidovich, L. (2024). "Quantum Sensing: Beyond the Classical Limits of Precision", A research paper published at the Institute of Quantum Science and Engineering, Texas A&M University, College Station, Texas. Retrieved from <https://arxiv.org/pdf/2401.136588> .
- Da Silva, W. (2015). Quantum computer coding in silicon now possible. Published at the University of New South Wales Newsroom on November 17, 2015. Retrieved from <https://newsroom.unsw.edu.au/news/science-tech/quantum-computer-coding-silicon-now-possible> .
- DeAngelis, S. (2014). A Glossary of Quantum Computing Terms. Retrieved from <https://www.enterrasolutions.com/blog/glossary-quantum-computing-terms/> .
- Esat, T., et al. (2024). " A Quantum Sensor for Atomic-Scale Electric and Magnetic Fields ". Am article published at Nature Nanotechnology, July 25, 2024. Retrieved from <https://www.nature.com/articles/s41565-024-01724-z.pdf> .
-  Esterlis, I. (2024). Quantum Sensing (condensed matter perspective) - A presentation prepared for the Wisconsin Summer School for Science, University of Wisconsin Madison, Augus 28, 2024. Retrieved from [https://www.physics.wisc.edu/quantum-summer-school/wp-content/uploads/sites/16/2024/09/quant\\_science\\_summer\\_school\\_2024.pdf](https://www.physics.wisc.edu/quantum-summer-school/wp-content/uploads/sites/16/2024/09/quant_science_summer_school_2024.pdf) .
- Fedorov, A. K. , Kiktenko, E. O., and Lvovsky, A. I. (2018). Quantum computers put blockchain security at risk. Published November 19, 2018 in Nature. Retrieved from: <https://www.nature.com/articles/d41586-018-07449-z> .
- Firestone, A/ (2025). The Quantum Reckoning: Why and How Cryptography Must Evolve Before Quantum Computers. Retrieved from <https://www.linkedin.com/pulse/quantum-reckoning-why-how-cryptography-must-evolve-before-firestone-dtele/?trackingId=Knpz4RwNunjFTZP%2FQoUSqA%3D%3D> .



# Quantum References

- Gerschenfeld, N. and Chuang, I. L. (1998). Quantum Computing with Molecules. Published in the June 1998 edition of Scientific American magazine. Retrieved from: <http://cba.mit.edu/docs/papers/98.06.sciqc.pdf> .
- Grimes, R. A. (2020). Cryptography Apocalypse” Preparing for the Day When Quantum Computing Breaks Today’s Crypto. Wiley, Hoboken, NJ.
- Gomes, L. (2018). Quantum Computers Strive to Break Out of the Lab. Published at IEEE Spectrum on March 22, 2018 Retrieved from <https://spectrum.ieee.org/computing/hardware/quantum-computers-strive-to-break-out-of-the-lab>.
- Government Accountability Office (CAO) (2025). Science & Tech Spotlight - Quantum Sensors. GAO-25-107876, January 2025. Retrieved from <https://www.gao.gov/assets/gao-25-107876.pdf> .
- Gururaja, W. (2016). "Advances in Quantum Sensors: Principles and Applications". Published in IJRAR, June 2018, Volume 3, Issue 2. Retrieved from <https://ijrar.org/download.php?file=IJRAR19D6172.pdf> .
- Grimes, R. A. (2020). Cryptography Apocalypse. Hoboken, NJ., Wiley.
- Herman, A. (2018). Winning the Race in Quantum Computing. Published in American Affairs Journal. Retrieved from: <https://americanaffairsjournal.org/2018/05/winning-the-race-in-quantum-computing/> .
- Hidary, J. D. (2019). Quantum Computing: An Applied Approach. Published by Springer Nature. Switzerland.
- Hoff, T. (2009). Lecture by Ted Hoff at U.C. Berkley. Located at: <https://www.youtube.com/watch?v=7MgHsgoilQ4&t=80s> .
- Hurley, W. (2018). Quantum Computing Standards. A webinar presented on April 24, 2018 and located at <https://www.youtube.com/watch?v=qKt7dOf4pXY&t=7s> .
- IBM. (2018). IBM Q. Located at <https://www.research.ibm.com/ibm-q/>.
- IEEE. (2018). IEEE P7130 - IEEE Nomenclature Standard. Quantum Computing Working Group. Located at: <https://standards.ieee.org/develop/project/7130.html> .
- IEEE. (2018). IEEE P7131 - IEEE Benchmarking Standard. Quantum Computing Working Group. Located at: <https://standards.ieee.org/develop/project/7131.html> .

# Quantum References

- Johnston, E., et al. (2019). Programming Quantum Computers. Published by O'Reilly. Sebastapol, CA.
- Ivezic, M. (2025). Q-Day Estimator. Retrieved from <https://q-day.org/crqc-readiness-benchmark-q-day-estimator/> .
- Kaye, P., et al. (2010). An Introduction to Quantum Computing. Published by Oxford University Press. Oxford, UK.
- Kholodov, I. (2009). The von Neumann Computer Model. From the CIS-77 course at Bristol Community College. Retrieved from: <http://www.c-jump.com/CIS77/CPU/VonNeumann/lecture.html> .
- Klarreich, E. (2018). Graduate Student Solves Quantum Verification Problem. Published in Quanta Magazine, October 8, 2018. Retrieved from <https://www.quantamagazine.org/graduate-student-solves-quantum-verification-problem-20181008/> .
- Lored, R. (2020). Learn Quantum Computing with Python and IBM Quantum Experience. Published by Packt Publishing. Birmingham, UK.
- Malinowski, R. (2024). The Power of Mosca's Theorem: How It Helps Us Grasp the Quantum Threat. Retrieved from <https://www.theqrl.org/blog/grasping-the-quantum-threat-with-moscas-theorem/>.
- McMahan, D. (2008). Quantum Computing Explained. Published by Wiley Interscience. Hoboken, NJ.
- Miller, S. (2018). DARPA digs into the details of practical quantum computing. Retrieved from: <https://gcn.com/articles/2018/07/12/darpa-quantum-architecture.aspx> .
- Mitre PQC Coalition. (2025). Mitre PQC Coalition Roadmap. Retrieved from <https://pqcc.org/> .
-  Nielsen, M., and Chuang, I. (2016).. Quantum Computation and Quantum Information, 10<sup>th</sup> edition. Published by Cambridge University Press. Cambridge, UK.
- National Science and Technology Council (NSTC) (2022). "Bringing Quantum Sensors to Fruition", Retrieved from <https://www.quantum.gov/wp-content/uploads/2022/03/BringingQuantumSensortoFruition.pdf>
- New York Times. (2018). The next tech talent shortage: Quantum computing researchers. Retrieved from <https://indianexpress.com/article/technology/science/the-next-tech-talent-shortage-quantum-computing-researchers-5412552/> .
- Nomura, Y., et al. (2018). Quantum Physics, Mini Black Holes, and the Multiverse. Published by Springer. Switzerland.

# Quantum References

- Panetta, K. (2017). The CIO's Guide to Quantum Computing. Published November 29, 2017. Retrieved from <https://www.gartner.com/smarterwithgartner/the-cios-guide-to-quantum-computing/> .
- Perry, R. T. (2012). Quantum Computing from the Ground Up. Published by World Scientific. Singapore.
- Polkinghorne, J. (2002). Quantum Theory: A Very Short Introduction. Published by Oxford University Press. Oxford, UK.
- Quantum Foundry Copenhagen (2025). Quantum Foundry Copenhagen, Retrieved from <https://qfcph.com/> .
- QED-C (2025). State of the Global Quantum Industry 2025. Retrieved from <https://quantumconsortium.org/publications/stateofthequantumindustry2025/>,
- Qnami. (2025). Retrieved from <https://qnami.ch/portfolio/quantum-foundry/>.
- Quantum Computing Playground. (2014). Located at <http://www.quantumplayground.net/#/home> .
-  Rieffel, E. and Polak, W. (2011). Quantum Computing: A Gentle Introduction. Published by MIT Press. Cambridge MA.
-  Sattel, S. (2016). The Future of Computing - Quantum & Qubits. Retrieved from: <https://www.autodesk.com/products/eagle/blog/future-computing-quantum-qubits/> .
- Santos, F. P. D. (2024). "Quantum Sensors: Principles and Ground Applications". A presentation presented to LNE-Syrte, Paris Observatory. Published in NKG Science Week Online, March 12, 2024. Retrieved from <https://www.nordicgeodeticcommission.com/wp-content/uploads/2024/05/Talk-NKG.pdf>
- Seskir, Z. (2022) Quantum Sensors: Principles, Types, and Applications (according to ChatGPT). Retrieved from [https://www.researchgate.net/profile/Zeki-Seskir/publication/366168027\\_Quantum\\_Sensors\\_Principles\\_Types\\_and\\_Applications\\_according\\_to\\_ChatGPT/links/639470a811e9f00cda32f91d/Quantum-Sensors-Principles-Types-and-Applications-according-to-ChatGPT.pdf](https://www.researchgate.net/profile/Zeki-Seskir/publication/366168027_Quantum_Sensors_Principles_Types_and_Applications_according_to_ChatGPT/links/639470a811e9f00cda32f91d/Quantum-Sensors-Principles-Types-and-Applications-according-to-ChatGPT.pdf)
- Silva, V. (2018). Practical Quantum Computing for Developers. Published by Apress. New York, NY.
- Sutor, R, S, (2019). Dancing with the Qubits. Published by Packt Publishing. Birmingham, UK.
- Wikipedia. (2011). Quantum Machine. Retrieved from: [https://en.wikipedia.org/wiki/Quantum\\_machine](https://en.wikipedia.org/wiki/Quantum_machine) .
- Wikipedia. (2018). Article on Quantum Superposition. Retrieved from [https://en.wikipedia.org/wiki/Quantum\\_superposition](https://en.wikipedia.org/wiki/Quantum_superposition).

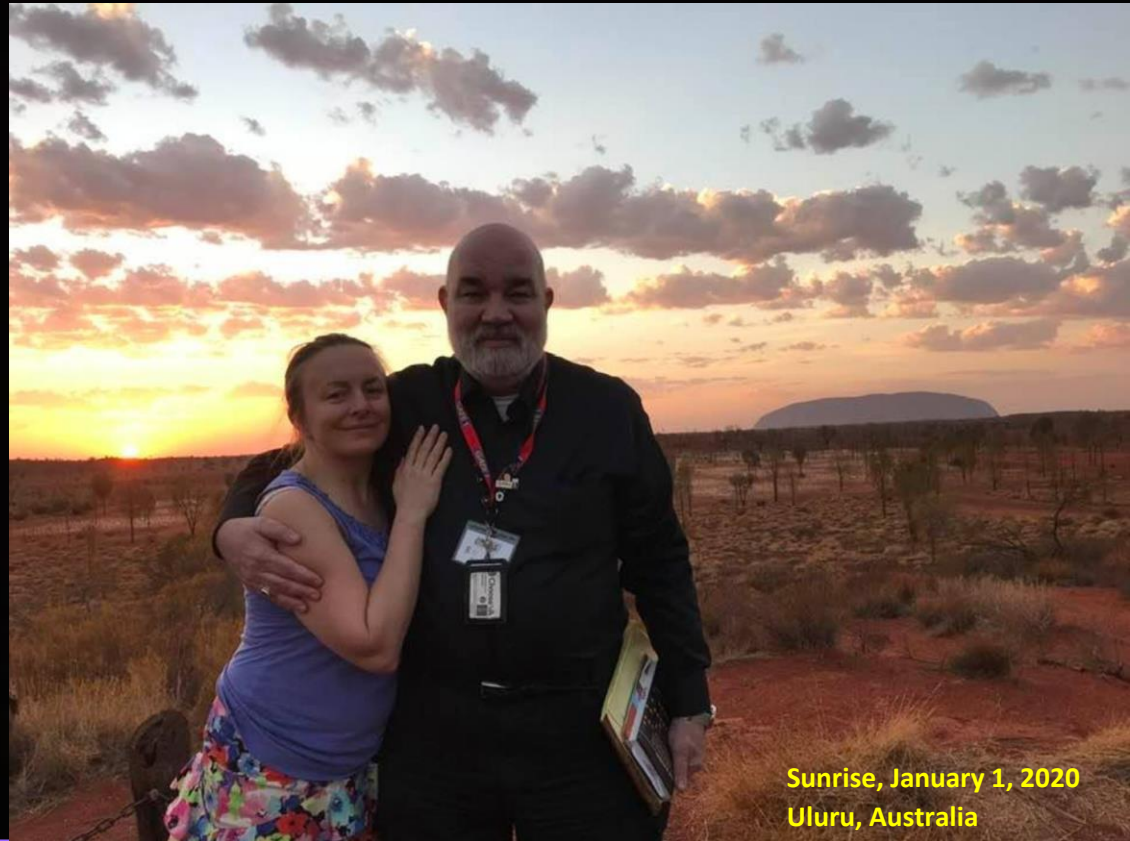
# Quantum References

- Wikipedia. (2025). What is Quantum Sensing?. Retrieved from [https://en.wikipedia.org/wiki/Quantum\\_sensor](https://en.wikipedia.org/wiki/Quantum_sensor) .
- Woody, L.S. (2022). Essential Mathematics for Quantum Computing. Published by Pakt. Birmingham, UK.
- Wilburn R. and Harris, K. Theory of Quantum Mechanics and Its Implications. Retrieved from <https://80000hours.org/podcast/episodes/david-wallace-many-worlds-theory-of-quantum-mechanics/> .
- Williams, C. P., and Clearwater, S. R. (1998). Explorations in Quantum Computing. Published by Springer-Verlag. New York, NY.
- Williams, C. P., and Clearwater, S. R. (2000). Ultimate Zero and One: Computing on the Quantum Frontier. Published by Springer-Verlag. New York, NY.
- Wilson, L. (2015). The Rise of Quantum Computers - The Current State of Cryptographic Affairs. Retrieved from <http://www.activecyber.net/rise-quantum-computers-current-state-cryptographic-affairs/> .
- Wikipedia. (2011). Quantum Machine. Retrieved from: [https://en.wikipedia.org/wiki/Quantum\\_machine](https://en.wikipedia.org/wiki/Quantum_machine) .
- Wikipedia. (2018). Article on Quantum Superposition. Retrieved from [https://en.wikipedia.org/wiki/Quantum\\_superposition](https://en.wikipedia.org/wiki/Quantum_superposition) .
- Wikipedia. (2025). What is Quantum Sensing?. Retrieved from [https://en.wikipedia.org/wiki/Quantum\\_sensor](https://en.wikipedia.org/wiki/Quantum_sensor) .
- Wilburn R. and Harris, K. Theory of Quantum Mechanics and Its Implications. Retrieved from <https://80000hours.org/podcast/episodes/david-wallace-many-worlds-theory-of-quantum-mechanics/> .

# PQC: A Short Primer

## About Me


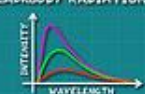



1. E-Mail [williamslater @ gmail.com](mailto:williamslater@gmail.com)
2. Phone 1-312-342-2626
3. CEO and owner of Slater Technologies, Inc. (since 1989)
4. In Quantum since 2011
5. Started in Cybersecurity in the U.S. Air Force: 1977.
6. Former U.S. Air Force Computer System Staff Officer who served at Strategic Air Command HQ.
7. Programming Languages: 43
8. 3 Graduate Degrees
  - MS Computer Information Systems
  - MBA
  - MS Cybersecurity
9. 88 Certifications including CISSP, SSCP, CISA, PMP.
10. Certified Project Manager with over 25 years experience.
11. Born and Raised in Memphis, Tennessee
12. Lives and works in Chicago, Illinois, USA
13. Published Author: <https://billslater.com/writing>
14. Working with QSECDEF since September 2024.
15. Happily married to Joanna Roguska since December 2000.
16. Working with Joe Reddix and The Reddix Group since 2024.
17. Avid fan of Andreas Vollenweider Music ( since 1985), Chess (since 1964), and Judo (since 1968).
18. Voracious Reader with 18,000 physical books and 8000 digital books.
19. Meyers-Briggs: INFP.
20. Non-Denominational Christian (since 1973).








Sunrise, January 1, 2020  
Uluru, Australia

# THE MAP OF QUANTUM PHYSICS

## PRE-QUANTUM MYSTERIES

**ATOMIC SPECTRA**  
  
**BLACKBODY RADIATION**  
  
**THE STABLE ATOM**  
  
**RADIOACTIVITY**  
  
**PHOTOELECTRIC EFFECT**  






## QUANTUM FOUNDATIONS

**THE WAVE FUNCTION**  
  
**PARTICLE-WAVE DUALITY**  
  
**THE BORN RULE**  
  
**INTERFERENCE PATTERN**  
  
**DOUBLE SLIT EXPERIMENT**  
  
**THE SCHRÖDINGER EQUATION**  




$$i\hbar \frac{\partial}{\partial t} \Psi = -\frac{\hbar^2}{2m} \nabla^2 \Psi + V(\mathbf{r}) \Psi$$
  
**THE DIRAC EQUATION**  

$$i\hbar \gamma^\mu \partial_\mu \psi - mc\psi = 0$$









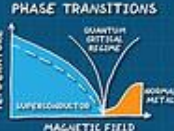




## INTERPRETATIONS OF QUANTUM MECHANICS

**COPENHAGEN**  
  
**MANY WORLDS THEORY**  
  
**CONSISTENT HISTORIES**  
  
**QBISM**  
  
**AND MANY OTHERS...**  
 STOCHASTIC INTERPRETATION  
 COSMOLOGICAL INTERPRETATION  
 QUANTUM BAHYSENISM  
 ALTERNATIVE COLLAPSE  
 TRANSACTIONAL INTERPRETATION

## QUANTUM GRAVITY

**M-THEORY**  
  
**STRING THEORY**  
  
**LOOP QUANTUM GRAVITY**  






## QUANTUM PHENOMENA

**PARTICLE PROPERTIES**  
 POSITION, MASS, ELECTRIC CHARGE, WEAK HYPERCHARGE, LEFT/RIGHT FAMILY NUMBER, SPIN, ANGULAR MOMENTUM, COLOR CHARGE, FLAVOR, BARYON NUMBER, LEPTON NUMBER  
**QUANTUM SPIN**  
  
**SUPERPOSITION**  
  
**SCHRODINGER'S CAT**  
  
**ENTANGLEMENT**  
  
**QUANTUM TUNNELING**  
  
**SUPERCONDUCTIVITY**  
  
**COOPER PAIRS**  
**QUANTUM HALL EFFECT**  
  
**SUPERFLUIDITY**  
  
**PHASE TRANSITIONS**  
  
**CASIMIR EFFECT**  
  
**TOPOLOGICAL PHASE TRANSITIONS**  
  
**ZERO-POINT ENERGY**  
  
**MAGNETIC RESONANCE IMAGING**  




## QUANTUM THEORY

**POSTULATES (PARAPHRASED)**



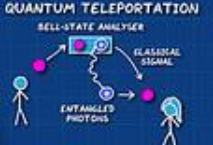


1. WAVE FUNCTION DETERMINES EVERYTHING.
2. ALL OBSERVABLES HAVE OPERATORS
3. OBSERVABLES ARE HERMITIAN
4. EIGENFUNCTIONS OF OPERATORS ARE INDEPENDENT
5. EXPECTATION VALUE INTEGRAL
6. TIME DEPENDENT SCHRÖDINGER EQUATION

**PATH INTEGRALS**  
  
**QUANTUM FIELD THEORY**  
  
**SYMMETRIES**  
  
**HILBERT SPACE**  


## PARTICLE PHYSICS

**QUANTUM CHROMODYNAMICS**  
 STRONG FORCE  
  
**ELECTROWEAK INTERACTIONS**  
 ELECTROMAGNETISM + WEAK FORCE  
 $\gamma, W^-, W^+, Z^0$   
**QUANTUM ELECTRODYNAMICS**  


## QUANTUM INFORMATION

**QUANTUM CRYPTOGRAPHY**  
  
**QUANTUM COMMUNICATION**  
  
**QUANTUM TELEPORTATION**  
 BELL-STATE ANALYSER  
 CLASSICAL SIGNAL  
 ENTANGLED PHOTONS  
  
**QUANTUM COMPUTING**  
 QUBITS  
 QUANTUM SIMULATION  
  
**QUANTUM COMPLEXITY**  
 COMPUTATIONAL COMPLEXITY  
 P SPACE  
 NP PROBLEMS  
 BQP  
 P PROBLEMS  


## THE STANDARD MODEL OF PARTICLE PHYSICS

**QUARKS**  
 u, d, s, c, b, t  
**LEPTONS**  
 e,  $\mu$ ,  $\tau$ ,  $\nu_e$ ,  $\nu_\mu$ ,  $\nu_\tau$   
**GAUGE BOSONS**  
 $\gamma, W^+, W^-, Z^0$   
**ANTI-MATTER**  
 PROTON, ANTI-PROTON, P, P-bar  
**FEYNMAN DIAGRAMS**  
  
**PARTICLE ACCELERATORS**  


## SOLID STATE DEVICES



**BAND THEORY OF SOLIDS**  
  
**TRANSISTORS**  
 SOURCE, GATE, DRAIN, N-TYPE, P-TYPE  
  
**SOLAR PANELS**  
  
**CHARGE-COUPLED DEVICES**  
 CCD SENSOR  
  
**LIGHT EMITTING DIODES**  
 POSITIVE TERMINAL, NEGATIVE TERMINAL  
  
**LASERS**  
  
**ATOMIC CLOCKS**  
  
**SCANNING TUNNELING MICROSCOPES**  
  
**ATOMIC FORCE MICROSCOPES**  
  
**YOSEPHSON FUNCTION**  
  
**SQUIDS**  


## CONDENSED MATTER PHYSICS




## QUANTUM BIOLOGY

**PHOTOSYNTHESIS**  
  
**BIRD NAVIGATION**  
  
**SENSE OF SMELL**  
  
**ENZYMES**  





## GOLD ATOM PHYSICS

**DEGENERATE ULTRACOLD GASES**  
 DEGENERATE FERMI GAS  
 BOSE-EINSTEIN CONDENSATE  
  
**RYDBERG MATTER**  


## NUCLEAR PHYSICS

**NUCLEAR FISSION**  
  
**NUCLEAR FUSION**  
  
**RADIOACTIVE DECAY**  
 ALPHA DECAY  
 BETA DECAY  
 GAMMA DECAY  


## QUANTUM CHEMISTRY

**ELECTRONIC STRUCTURE**  
  
**MOLECULAR DYNAMICS**  
  
**QUANTUM MONTE CARLO METHODS**  


# Enter the Quantum Zone

Join Our QSECDEF Group Meeting Every Tuesday

3 PM Paris Time, 2 PM UK, 9 AM New York, 8 AM Chicago, 2 AM Wed. Australia

Event Link on Zoom, CLICK HERE:

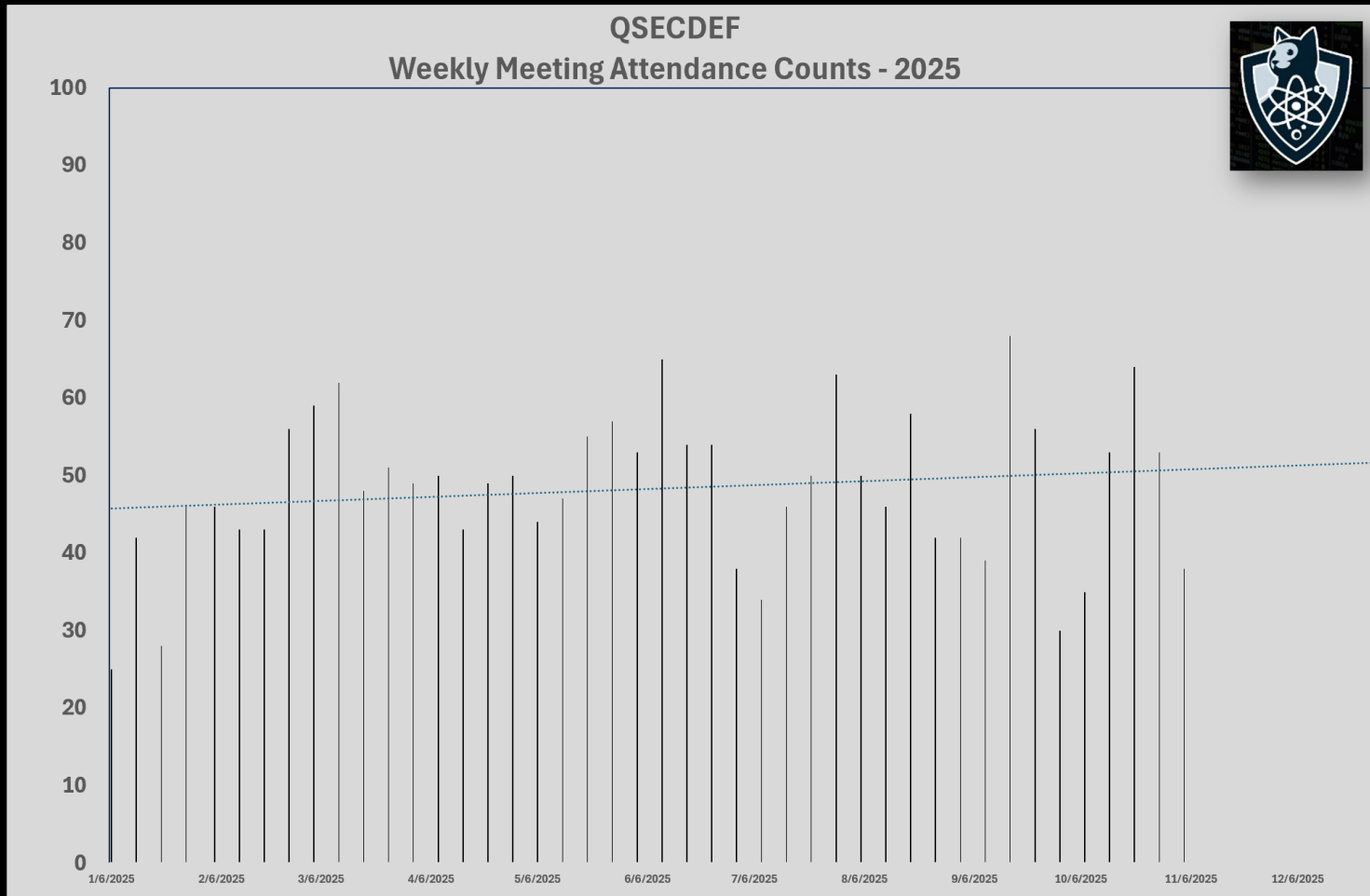
<https://zoom.us/j/91685969165>



# Join Our FREE QSECDEF Group Meeting Every Tuesday

3 PM Paris Time, 2 PM UK, 9 AM New York, 8 AM Chicago, 2 AM Wed. Australia

<https://zoom.us/j/91685969165>

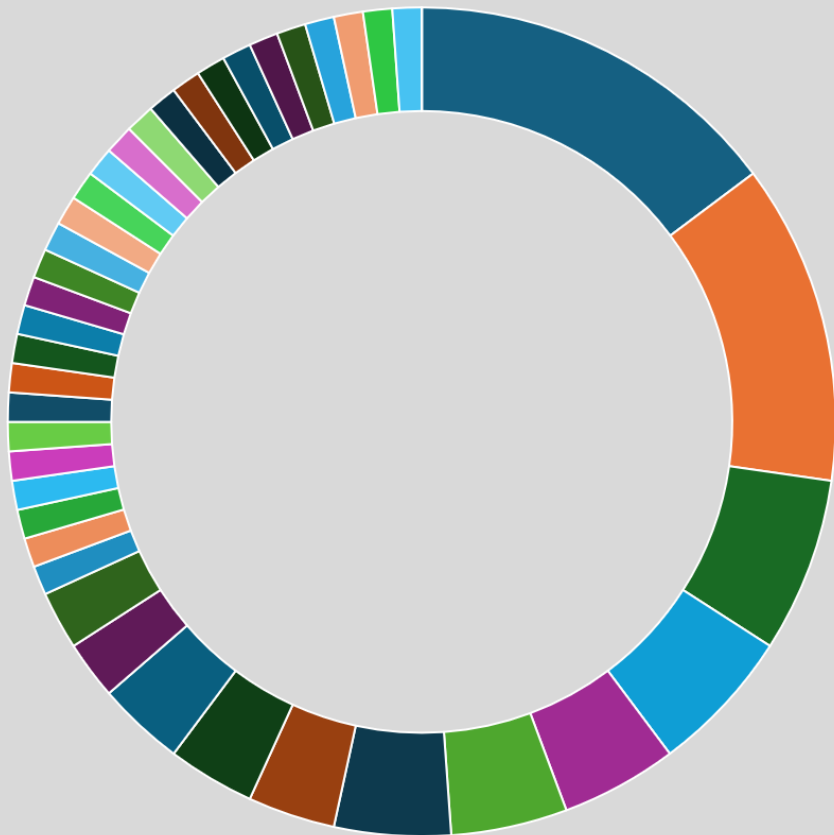


# Join Our FREE QSECDEF Group Meeting Every Tuesday

3 PM Paris Time, 2 PM UK, 9 AM New York, 8 AM Chicago, 2 AM Wed. Australia

<https://zoom.us/j/91685969165>

QSECDEF Topics Covered  
September 2024 - September 2025



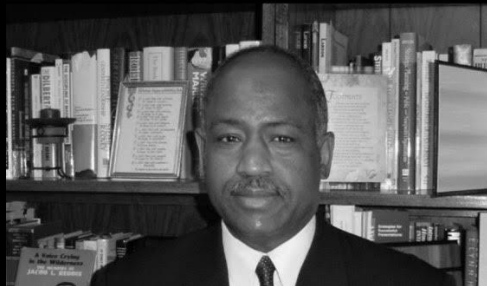
- Post Quantum Cryptography (PQC)
- Quantum Key Distribution (QKD)
- Quantum Networking
- Quantum Satellite Communications
- Quantum and AI
- Quantum Computing, Banking & Finance
- Quantum Random Number Generators (QRNG)
- Quantum Cryptography
- Quantum Foundry
- Quantum Organization Planning
- Quantum and IT Security
- Quantum App Development Tools
- Hybrid Infrastructures with Quantum & HPC
- Quantum & Other Emerging Technologies
- Quantum Algorithms
- Quantum and Cryptographic Agility
- Quantum and Enterprise Integration
- Quantum and the Cosmos
- Quantum Careers & Recruiting
- Quantum Communications
- Quantum Computers
- Quantum Computing and Encodings
- Quantum Cryptanalysis
- Quantum Data Centers
- Quantum Edge Computing
- Quantum Financial Threats: Cryptocurrency & Enabling Money Laundering
- Quantum IP and the Law, Export Policies, Etc.
- Quantum Photonic Systems
- Quantum Programming
- Quantum Safe Cryptocurrency
- Quantum Safe Networks
- Quantum Security
- Quantum Sensors - Space
- Quantum Software Verification on Chain
- Quantum Space Networks
- Quantum Standardization & Start-Ups
- Quantum Startup Analysis and Valuation
- Quantum Technology and the Law
- Quantum Time Applications
- Secure Quantum App Development
- Quantum Memory Management
- Quantum Sensors

# Free Audio Book

## Building a Quantum Foundry

Presented to the QSECDEF Group

Tuesday, June 3, 2025



THE REDDIX GROUP

### Building The Quantum Foundry

Joe Reddix  
William Slater

Visit to Listen

<https://www.youtube.com/watch?v=kuiVO2EkZYM&t=20s>

# Free Presentation

## Building a Quantum Foundry

Presented to the QSECDEF Group

Tuesday, June 3, 2025

From Chicago, Illinois, USA

William Slater

CEO

Slater Technologies, Inc.

---

William Slater

Slater Technologies, Inc

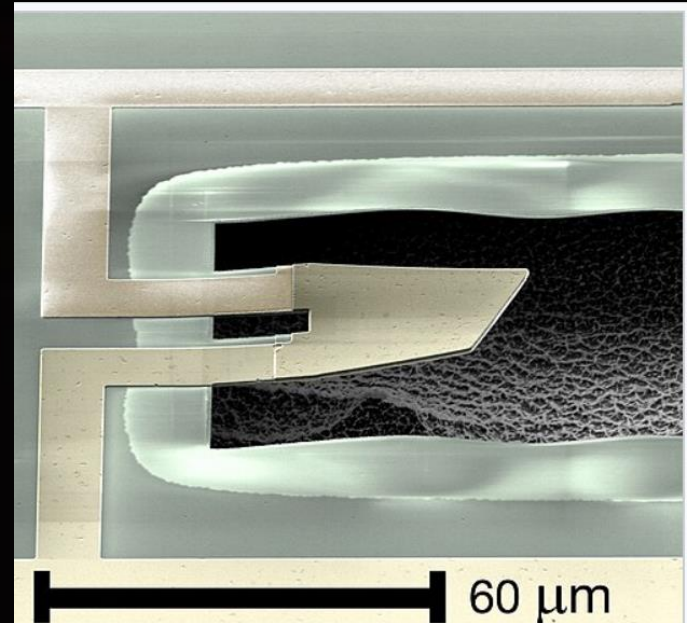
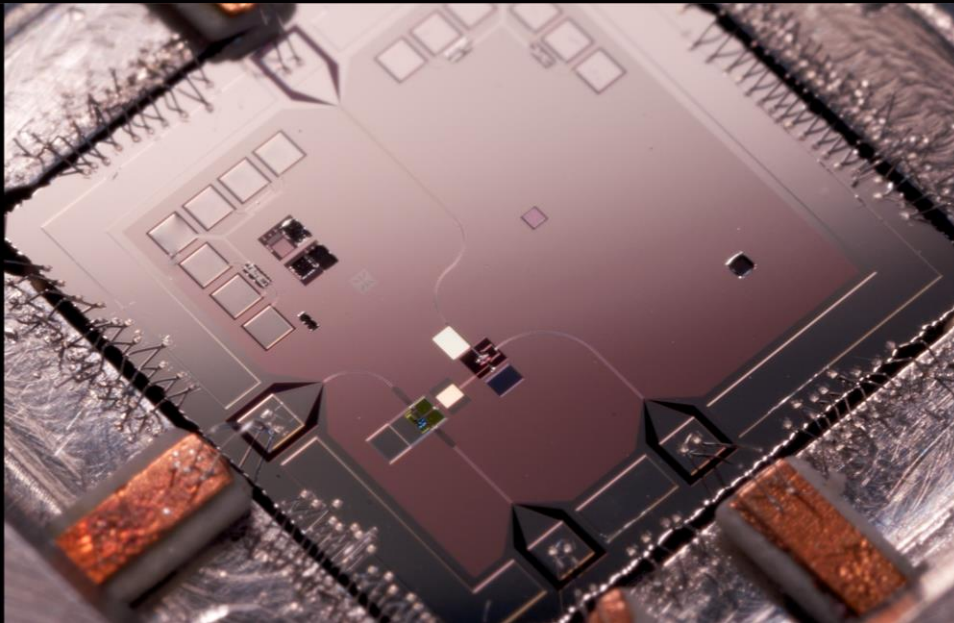
June 3, 2025     

Visit to View and Download William Slater's Slides  
<https://billslater.com.com/quantumfoundryga.pdf>

# PQC: A Short Primer

## World's First Quantum Machine, 2010

Wikipedia, 2011 - [https://en.wikipedia.org/wiki/Quantum\\_machine](https://en.wikipedia.org/wiki/Quantum_machine)



## End of Presentation