THE FUTURE OF PRODUCT SECURITY

NAVIGATING THE AGE OF AI & QUANTUM COMPUTING

Jacob Combs

CISO and Product Security Leader

20+ years across critical infrastructure and highly regulated industries.

Background in IT, Software Development prepared me for Enterprise and Product Security.

OBJECTIVE

HELP LEADERS MOVE FROM

“WAIT-AND-SEE” TO **ACTION-NOW** ON

AI & QUANTUM THREATS.

WHY THIS MATTERS, WHY NOW

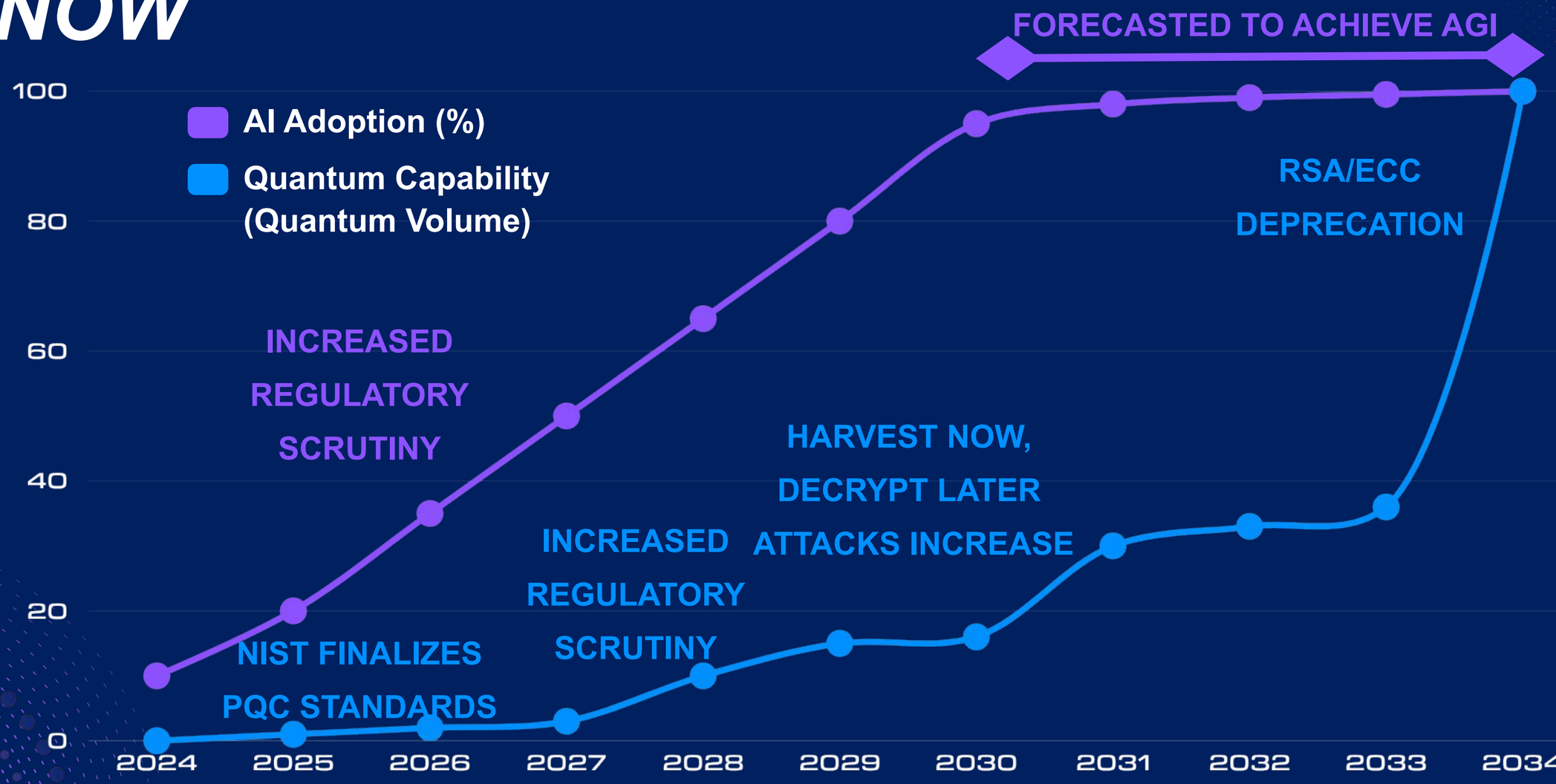


Chart is only for illustration purposes only as it is impossible represent what has not yet occured.

SCOPING OUR FOCUS

BACK TO FOUNDATIONS

AI SYSTEM SAFETY, FAILURES, & LIMITATIONS

AI PURSUING ITS OWN GOALS IN CONFLICT WITH HUMAN GOALS OR VALUES

LACK OF TRANSPARENCY OR INTERPRETABILITY

LACK OF CAPABILITY OR ROBUSTNESS

MULTI-AGENT RISKS

MIT AI RISKS REPOSITORY https://airisk.mit.edu/

AI IN APPLICATIONS & SYSTEMS

The Pragmatic Threats

CONFIDENTIALITY

DATA EXTRACTION & INFERENCE ATTACKS

MODEL INVERSION & STEALING

INTEGRITY

DATA POISONING

MODEL EVASION

AVAILABILITY

MODEL DEGRADATION OVER TIME

LACK OF ROBUSTNESS, GENERALIZABILITY

THE QUANTUM THREAT: BREAKING TODAY'S TRUST ANCHORS

DECRYPTION OF SENSITIVE DATA

COMPROMISED AUTHENTICATION & INTEGRITY

ENHANCED DENIAL-OF-SERVICE ATTACKS

PQC TRANSITION CHALLENGES

- **Performance Overheads**
- **Integration Complexity**
- **Extended Lifecycles & Data Retention**

KEY REGULATORY & STANDARDS SIGNPOSTS

AI

OWASP Top 10 for Large Language Model Applications

NIST AI Risk Management

ISO/IEC 42001

EU AI Act

PQC

NIST PQC Standardization Process

ETSI Quantum Safe Cryptography

IETF Drafts & RFCs

INTEGRATED GOVERNANCE: EMBEDDING AI SECURITY

AI Risk Assessment and Threat Modeling

- Extend existing threat modeling to AI-specific vulnerabilities.
- Assess risks from training data, model architecture, and deployment environment.

AI Security Testing & Validation

- Implement adversarial testing, fuzzing, bias detection, and explainability checks.
- Validate model robustness against unexpected or malicious inputs.

Secure AI Design and Development

- Integrate security and privacy-preserving techniques into the AI development lifecycle.
- Secure data pipelines, model versioning, and access controls.

AI Monitoring, Logging, and Incident Response

- Continuously monitor models for performance drift, anomalous behavior, and signs of abuse or attack.
- Develop AI-specific incident response playbooks.

INTEGRATED GOVERNANCE: NAVIGATING THE PQC TRANSITION

Discover & Assess

- Crypto Inventory
- Risk Assessment & Prioritization
- PQC Algorithm Assessment

Implement & Validate

- Secure Implementation
- Validation & Testing

Design & Pilot

- Crypto-Agility by Design
- Pilot Projects
- Performance Testing

Monitor & Maintain

- Secure Update Mechanisms
- Monitor PQC Vulnerabilities

YOUR FIRST STEPS TOWARDS AI & QUANTUM RESILIENCE

Inventory & Assess

- Map devices in service beyond 2030 & their current cryptography.
- Trace all ML model versions & their training datasets.

Update Design Controls & SDLC

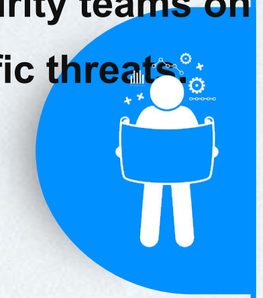
- Mandate crypto-agility for all new designs.
- Incorporate AI robustness & security requirements.

Enhance 3rd Party Risk Management

- Require Software Bill of Materials (SBOM).
- Demand Model Bill of Materials (Model-BOM) for AI components.

Educate & Plan

- Initiate PQC transition planning, starting with high-risk, long-lifecycle devices.
- Train development and security teams on AI-specific threats.



SECURING THE FUTURE: CORE PRINCIPLES

CONVERGING URGENCY

USER TRUST & SYSTEM RESILIENCE ARE PARAMOUNT

PROACTIVE & INTEGRATED GOVERNANCE

ACTION IS NOW – ADAPT OR BECOME OBSOLETE

FINAL THOUGHT

The future of secure products is not about predicting perfectly, but about building **the resilience to adapt effectively.**