How to Sell Post-Quantum Readiness by Combining it with a Zero Trust Journey

Robert Hann
Global Vice President of Sales, Cryptographic Center of Excellence at Entrust
Making the Connection – Using Zero Trust as the vehicle for PQ Readiness

Robert Hann, VP Digital Center of Excellence
Agenda

• Managing Cryptography
• Board priorities
• Zero Trust adoption and maturity
• Common journey elements
• Where can PQC help Zero Trust Maturity?
• Recommendations
A day in the life of......you!
Management of Cryptographic Assets

Problem Statements:

- PKI and crypto ARE critical infrastructure and expanding
- It is a false assumption that systems are “forever” secured with PKI/crypto
- Risks can be unknown because elements are not visible/managed
- Crypto resources are scarce and expensive
- Best practices are often inconvenient
- Procedures, Policies and platforms are not always robust or maintained
- Many organisations find out too late
The Post Quantum Challenge is Real (but it isn’t technical!)

Thank Quantum! At last we will have budget for crypto best practices & PQC migration.

"The time to prepare for PQ is now"..... "yes, we know!"
Board Priorities

**Advantages of a Quantum Computer Running AI**

Quantum computer AI systems would have a natural advantage over classical computing in many tasks because of their unique ability to apply the principles of quantum mechanics to calculations.

**Technologists Are The New Superheroes On Corporate Boards In The Age Of AI, Blockchain And CyberSecurity**

**Prepare A Cryptographic Inventory**

- Having an inventory of quantum-vulnerable technology and associated criticality of the data enables an organization to begin planning for risk assessment processes to prioritize its migration to PQC. This cryptographic inventory will:
  - Help an organization become quantum-ready — a state where a CRQC is not a threat,
  - Help an organization prepare a transition to zero trust architecture,
  - Help identify or correlate outside access to datasets, as those are more exposed and at higher risk,
  - Inform future analysis by identifying what data may be targeted now and decrypted when a CRQC is available.

**Figure 1: Board directors’ top seven strategic business priorities for 2022/2023**

- **Digital Tech Initiatives** decreased by 12%
- **Workforce** increased by 86%
- **ESG, Health and Sustainability** reached 100%
- **Growth** increased by 24%
- **Financial (other than revenue or profit)** increased by 39%
- **Risk Management** decreased by 214%
- **Business Expansion/Diversification** decreased by 19%
Zero Trust Strategy
the
STAKES
are HIGH

Breaches caused by credential compromise NEARLY DOUBLED over past three years

61%
2022

33%
2020

83%
of companies had two or more data breaches since 2021

$4.3M
Average cost of a breach
We are at an inflection point in Cybersecurity

59% 59% of organizations have NOT deployed Zero Trust strategies.

$219B Cybersecurity spending in 2023.

$1M Zero trust can reduce average breach losses by nearly $1M.

96% 96% of security decision-makers say Zero Trust is critical to their organization’s success.
What is Zero Trust?
Enabling a Resilient & Modern Digital Enterprise

“Zero Trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated.”

- U.S. National Institute of Standards and Technology (NIST)
Establishing a Foundation for Zero Trust

Historically, Zero Trust focused on networks and identity access but now it is a comprehensive approach to cybersecurity including encryption and data security.
POST QUANTUM ZEROTRUST JOURNEY

ESTABLISH GROUP accountable for organization-wide strategy and transition

INVENTORY DATA & FLOWS
Where does my high value data sit, get processed and transmitted → where to start

INVENTORY CRYPTO ASSETS
Automated/manual process for keys, certificates, secrets, and libraries...map to data

CRYPTO AGILITY STRATEGY
Critical for transition; mitigate risk relating to cryptography including people, process, and technology

MODERNISE & DEFEND
Simplify, consolidate, replace point crypto platforms now for a more controlled migration

PQ SECURITY MANAGEMENT
As the standards, regulations, and best practices mature, ensure you are maturing too

TEST AND MIGRATE
With NIST finalist algorithms and while the standards develop – use hybrid

ZERO TRUST
Activity
PQC, an enabler for Zero Trust
PQ Readiness Maturing Zero Trust

- PQ Readiness enhances your Zero Trust maturity:
  - Better cyber hygiene through visibility/governance
  - Risk assessment across the full crypto asset inventory
  - Strengthen ZT Orchestration
  - PQC early to mitigate “Harvest Now – Decrypt Later”
  - PQ/T Hybrid Bridge adds crypto agility
PQ Readiness for Identity

• Using PQC in Identity and Access Management:
  • PQC in authentication protects against compromised MFA tokens and other elements in access requests
  • PQC certificate based MFA (“phishing resistant”) gives enterprise data increased protection
  • PQC on VPNs and remote desktop services mitigates “Harvest Now-Decrypt Later” threat to your long-term data/contracts
Using PQC in Devices:

- Strengthens comms/trust between endpoints and management/application services
- Increased security for sensitive data on endpoints minimizing damage when breached
- On SIEM systems, protection of log data, comms and other critical components improves security and integrity of monitoring and incident response.
- Attackers will find it harder to tamper with or evade detection systems
Zero Trust for Data, Applications & Workloads

• Using PQC in Data, Applications & Workloads:
  • Encrypting sensitive data at rest and data in transit between applications maintains confidentiality and integrity minimizing unauthorized access.
  • Utilizing PQC for certificate based (Virtual) Machine Identity protects the VM against classical and quantum adversaries.
  • Code Signing with PQC further strengthens the protection of threats like spoofing and maintains the integrity of the trust fabric.
Recommendations

- Consolidate the PQ Readiness into your Zero Trust strategy (or even your company AI strategy)
- Elevate/summarize noteworthy Quantum news to Executives
- Tip: Request procurement/security includes PQ Readiness in your supply chain purchasing/assessments
Thank You

Questions?

entrust.com

© Entrust Corporation