CYBER EAGLE

PROACTIVE PREDICTIVE PROTECTED

Quantum Exposure & Trust Longevity Assessment

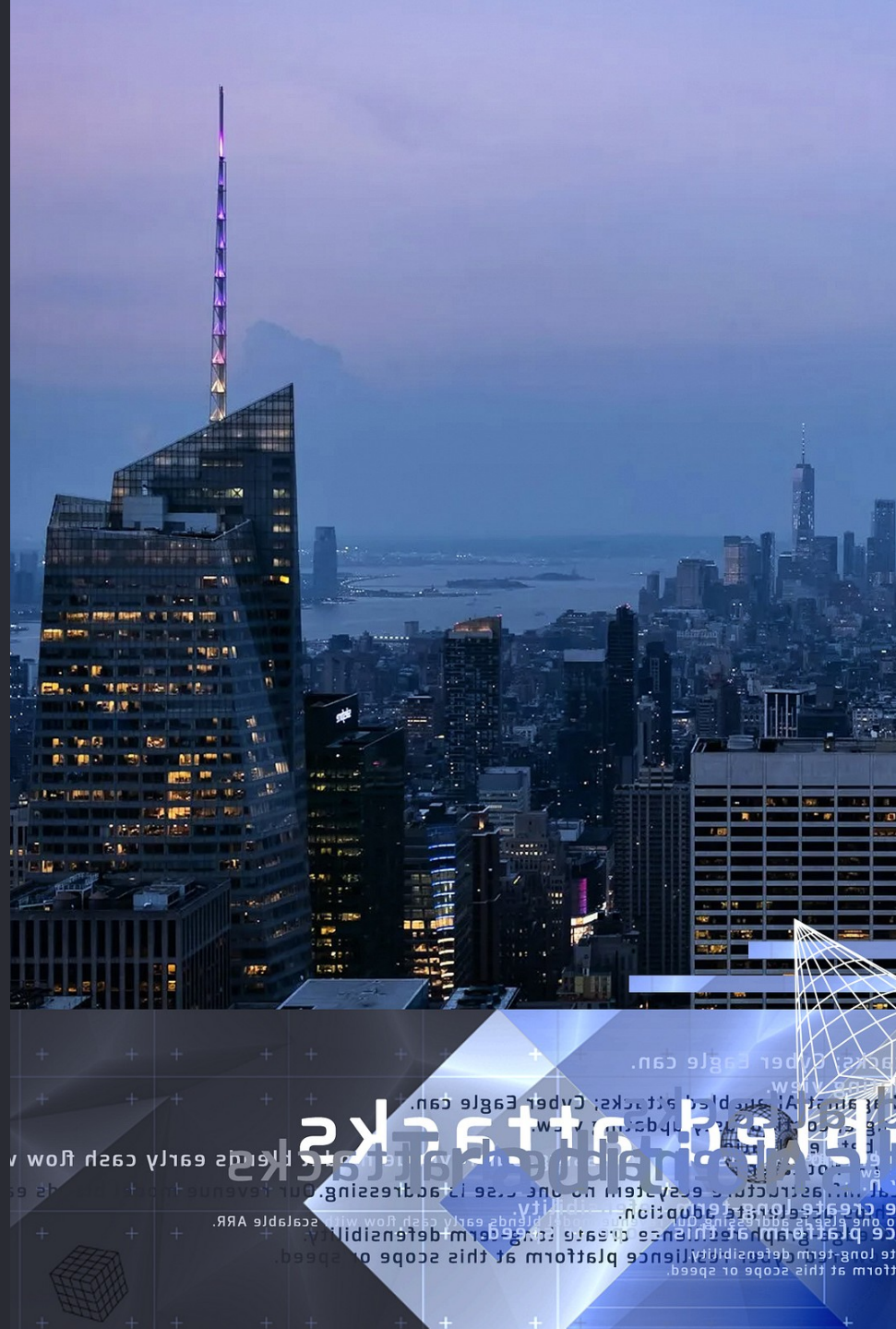
Why this matters now?

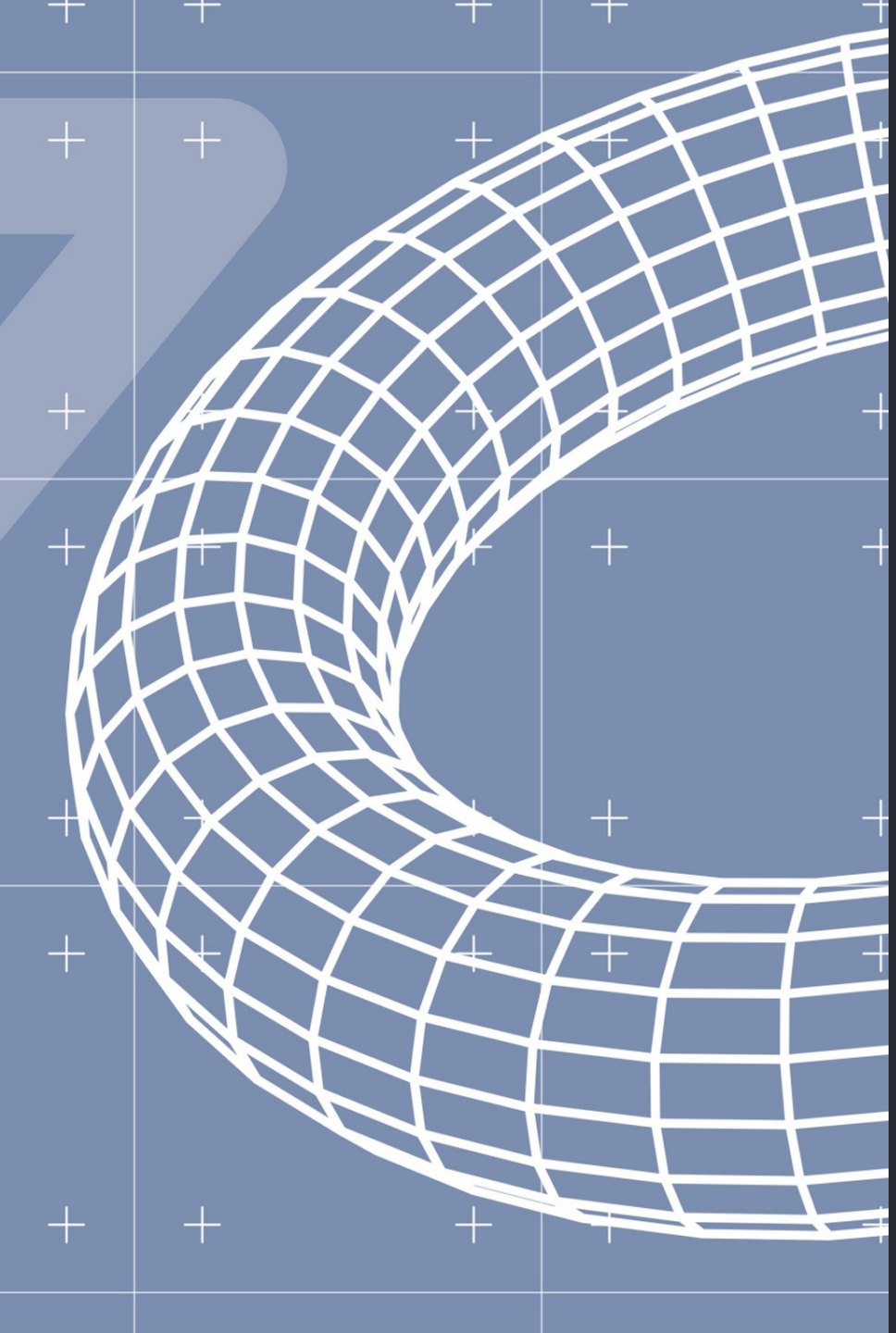
Cyber risk is no longer contained within IT systems.

Across industries, digital issues increasingly produce operational, regulatory, and trust consequences that leadership teams must answer for - often without having been shown the full picture.

As systems become more interconnected and long-lived, the cost of misunderstanding risk grows faster than the cost of addressing it.

This offering exists to address that gap.





What this is

An assessment that identifies where cryptographic trust will fail to remain valid over the lifespan of critical systems, records, and operational assets.

The problem addressed

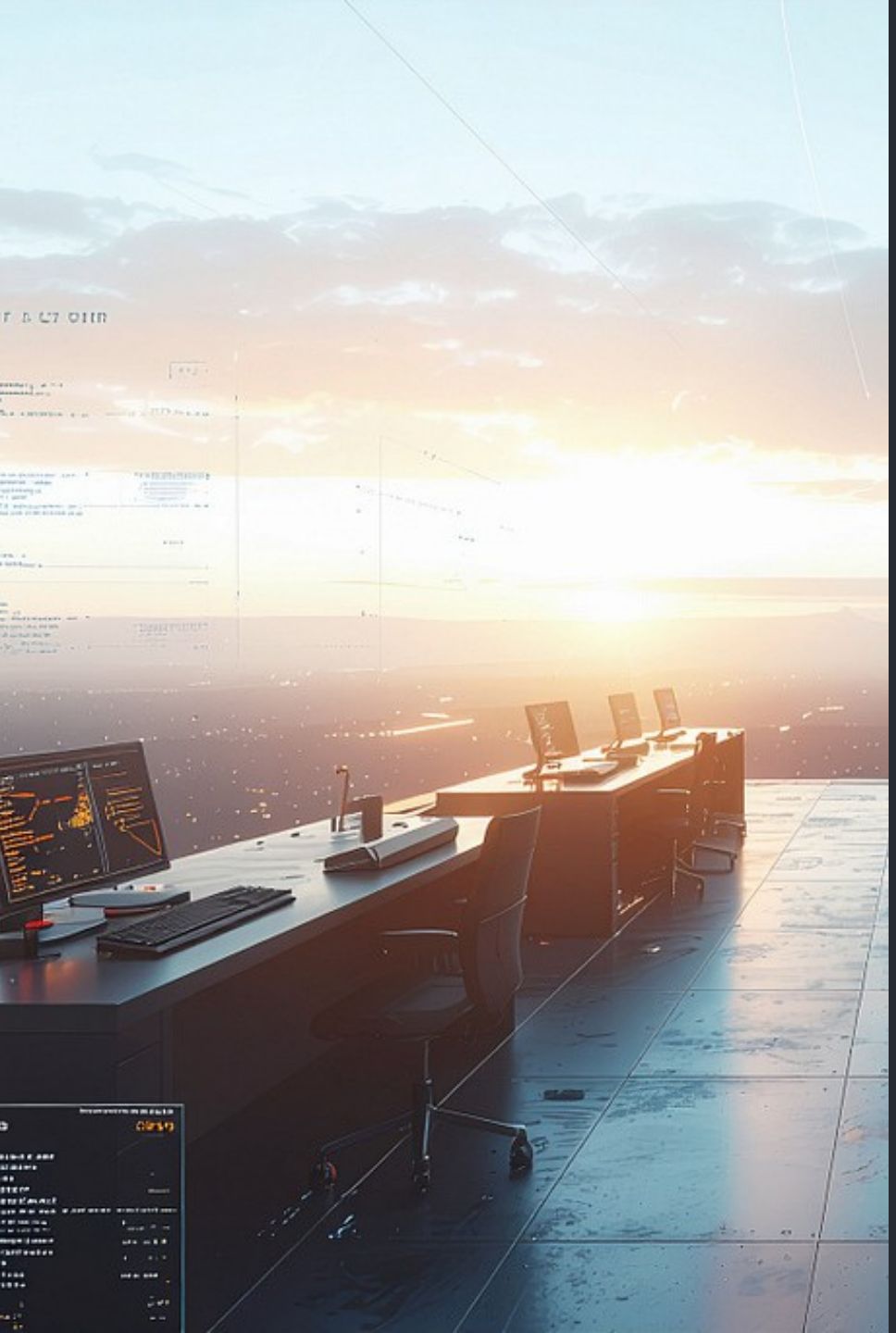
Many systems will outlive current cryptographic assumptions.

When trust fails retroactively, legitimacy fails with it.

What it does

QETLA identifies long-term trust exposure.

- Maps cryptographic dependencies
- Assesses trust longevity risk
- Prioritizes systems requiring early action



How it works

- Executive scoping
- Cryptographic discovery
- Exposure classification
- Roadmap development

What you receive

- Visibility into trust longevity risk
- Clear prioritization
- Executive-ready guidance

Who is this for

Organizations with long-lived systems, firmware, or records.

When organizations typically engage

Organizations engage when leadership recognizes that existing tools or reports no longer provide sufficient confidence, but before disruption forces reactive decisions.

This engagement is designed to:

- Create shared understanding
- Enable defensible decisions
- Reduce uncertainty at the executive level

It is intentionally scoped, proportionate, and designed to fit where the organization is today.

EAGLE

L4BS

Book a strategy briefing

Document: Quantum Exposure & Trust Longevity Assessment (QETLA) | Category: Quantum Readiness & Cryptographic Security | Version: 1.0 | Date: 2026-09-18
Target Audience: Organizations with long-lived systems, firmware, or records Summary: Assessment service identifying where cryptographic trust will fail to remain valid over the lifespan of critical systems, records, and operational assets. Keywords: quantum exposure, trust longevity, cryptographic trust, cryptographic dependencies, long-lived systems, QETLA, cryptographic discovery, risk assessment.