

QUARTERLY BOARD CYBER RISK BRIEF · Q3 2026

# Signal in. Decisions out.

A mid-market Midwest manufacturer · ██████ plants · OT-dependent production

Overall posture: **ELEVATED** ▲

● 3 decisions requested

## BOTTOM LINE

Residual cyber risk rose this quarter, driven by one exposure: **third-party remote access into plant (OT) networks**, now **outside board risk appetite**. Fraud risk improved after a finance control change. Quantum exposure is a planning problem, not an emergency, but the roadmap is unfunded beyond inventory. We ask the board for **three decisions** (page 2).

**1 of 6**

top risks outside appetite ▲  
from 0

**\$X.XM/day**

est. production-outage  
exposure band (illustrative)

**58%**

cryptographic inventory  
complete ▲ from 31%

**30 → 3 days**

edge-device critical patch  
window: current vs.  
proposed

## 1 Signals this quarter → 2 What it means for us

Plain language · condensed from external and internal intelligence

### SIGNAL (EXTERNAL)

### WHAT IT MEANS FOR [CLIENT] – RESIDUAL RISK IN BUSINESS TERMS

**RANSOMWARE** Ransomware crews continue to favor manufacturers, where downtime pressure drives payment. Vendor and remote-access paths remain a common way in.

→ Our plant remote-access path for ██████ maintenance vendors is the **most likely route to a production stoppage**. Now outside appetite. **[R1]**

**EXPLOITATION** Flaws in internet-facing firewalls and VPN appliances are being weaponized within days of public disclosure.

→ Our 30-day patch window for edge devices is slower than attacker timelines. Moving critical fixes to **72 hours** closes the gap at minimal cost. **[R2]**

**FRAUD** Payment-redirection fraud increasingly uses AI-generated voice and convincing vendor email threads.

→ A mandatory call-back control on bank-detail changes went live in August. **Exposure reduced**; trend improving. **[R3]**

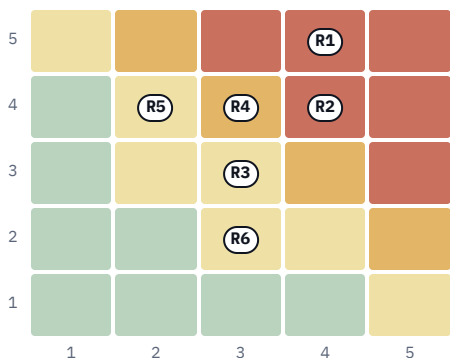
**SUPPLY CHAIN** Attackers keep using trusted suppliers' access and software updates to reach their customers.

→ ██████ of our top-20 suppliers hold privileged access **without breach-notification terms**. Fixable at contract renewal. **[R4]**

**QUANTUM** "Harvest now, decrypt later": encrypted data stolen today could be read once quantum capability matures. NIST published PQC standards (FIPS 203/204/205) in Aug 2024.

→ Design IP and ██████ contracts must stay confidential for **10+ years**. That long-lived data goes **first** in our post-quantum migration. **[R5]**

## 3 Risk posture



Rows: impact (5 = severe)

Columns: likelihood →

## Top-risk register

Residual, after current controls · trend vs. Q2

| #  | RISK                                      | RESIDUAL   | TREND | APPETITE |
|----|-------------------------------------------|------------|-------|----------|
| R1 | Ransomware-driven plant (OT) outage       | ● High     | ▲     | Outside  |
| R2 | Edge-device exploitation / initial access | ● High     | ▶     | At limit |
| R4 | Third-party privileged access             | ● Med-High | ▲     | At limit |
| R5 | Long-lived data exposure (quantum)        | ● Medium   | ▶     | Within   |
| R3 | Payment fraud / business email compromise | ● Medium   | ▼     | Within   |
| R6 | Data leakage via unsanctioned AI tools    | ● Medium   | ▲     | Within   |

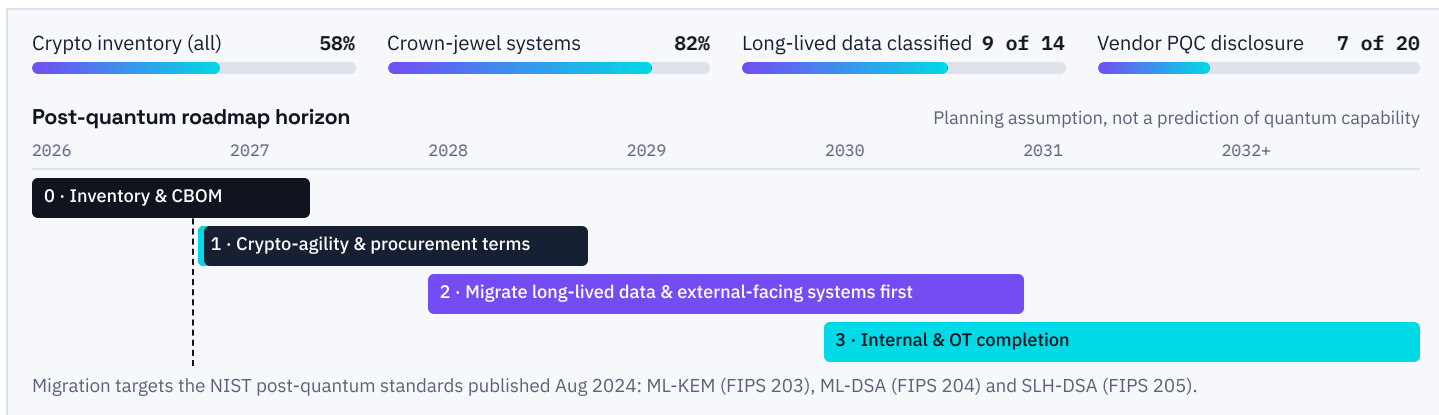
Scores are illustrative 5×5 likelihood × impact ratings for a fictional client. Appetite thresholds per board-approved statement ██████

### SINCE LAST BRIEF

✓ Payment call-back control live (R3)   ✓ Crown-jewel crypto inventory 82%   ✗ OT vendor-access gap open → Decision 1



## 4 Quantum readiness status

Status: **AMBER** · inventory on track · roadmap funded through Phase 0 only

## 5 Decisions requested of the board

Cost bands are illustrative order-of-magnitude, not quotes

| DECISION 1 · RISK R1                                                                                                     | DECISION 2 · RISK R5                                                                                      | DECISION 3 · RISKS R2, R4                                                                                                         |
|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>Close the plant remote-access gap</b>                                                                                 | <b>Fund post-quantum Phase 1</b>                                                                          | <b>Tighten the risk appetite statement</b>                                                                                        |
| Bring the only out-of-appetite risk back inside within two quarters.                                                     | Finish the inventory and build crypto-agility into purchasing before the next platform refresh.           | Turn two "at limit" risks into enforceable standards the team can run.                                                            |
| <b>A</b> Accept. R1 stays outside appetite; formal exception required <b>\$0</b>                                         | <b>A</b> Defer to FY28. Refresh cycle locks <b>\$0 now</b> in non-agile crypto                            | <b>A</b> No change to current statement <b>\$0</b>                                                                                |
| <b>B</b> Broker all vendor access through a monitored access gateway; MFA at every plant <b>\$250–400K + \$60–90K/yr</b> | <b>B</b> Phase 1: complete inventory, crypto-agility standard, vendor clauses <b>\$150–250K 12 months</b> | <b>B</b> Adopt 72-hour critical edge patching, plus breach-notice & PQC-disclosure terms at supplier renewal <b>Within budget</b> |
| <b>C</b> Full OT network segmentation program, 18 months <b>\$1.2–1.8M</b>                                               | <b>C</b> Accelerated: Phase 1 plus pilot migration of long-lived data <b>\$400–600K</b>                   | <b>C</b> B, plus immediate renegotiation of all top-20 supplier contracts <b>\$40–80K legal</b>                                   |
| <b>RECOMMEND B</b> now; bring C back as a FY27 decision gate.                                                            | <b>RECOMMEND B.</b> Defensible horizon at modest cost.                                                    | <b>RECOMMEND B.</b> Fixes at renewal, no new spend.                                                                               |
| <input type="checkbox"/> Approve <input type="checkbox"/> Amend <input type="checkbox"/> Defer                           | <input type="checkbox"/> Approve <input type="checkbox"/> Amend <input type="checkbox"/> Defer            | <input type="checkbox"/> Approve <input type="checkbox"/> Amend <input type="checkbox"/> Defer                                    |

## 6 What we're watching next quarter

| WATCH ITEM                                               | TRIGGER → PRE-AGREED ACTION                                            |
|----------------------------------------------------------|------------------------------------------------------------------------|
| Critical flaws in our VPN / firewall vendor              | Public exploit → patch or isolate within 72h; chair notified if missed |
| Ransomware activity against regional manufacturing peers | Peer incident in our sector → re-run OT tabletop within 30 days        |
| PQC roadmaps from ERP and PLM vendors                    | No roadmap by renewal → escalate to procurement, flag in Q4 brief      |
| AI voice-cloning attempts on finance staff               | Any attempt detected → extend call-back control to payroll changes     |
| Cyber insurance renewal questionnaire (Q1)               | New control requirements → cost and gap memo to committee              |

### HOW THIS BRIEF WAS BUILT

- 01 Discover:** intel sources, crypto inventory, and the board's open questions from last quarter.
- 02 Structure:** every signal is mapped to a named risk, an owner and an appetite threshold.
- 03 Advise:** translated into residual risk, capital and timeline, with options the board can actually choose between.
- 04 Embed:** the team runs this cadence quarterly without us in the room.

**Signal, not theatre.**  
**Leave a system, not a PDF.**

Request a principal briefing:  
info@shurikencyber.com