QUICK REFERENCE

Board Presentation Framework

Five slides, ten categories, three questions — the structure that turns cyber risk into a board-ready conversation.

The Five Slides Every Board Briefing Needs

Cyber risk gets dismissed when it is presented as a technical topic. The framework below translates security posture into the language boards understand: risk, accountability, progress, and resource requests. Each slide maps to a business question, not a technical metric.

Slide 1 — Where Do We Stand?

Business question: How exposed are we right now?

- Current score on the quarterly self-assessment (out of 100)
- Trend arrow: up, flat, or down vs. last quarter
- Compare to industry peer benchmark if available
- One sentence of plain-language context — "We are stronger in password discipline than we were last quarter, weaker in vendor oversight."

Slide 2 — The Top 3 Risks This Quarter

Business question: What are the biggest things that could go wrong, and how likely are they?

- Rank top 3 risks by expected financial impact
- For each: a one-line description, likelihood (low/medium/high), and estimated dollar exposure
- Example: "Ransomware via third-party software update — medium likelihood — up to $1.2M in disruption"

Slide 3 — Incidents & Near-Misses

Business question: What have we actually seen happen?

- Incidents this quarter (anonymized if sensitive)
- Near-misses — phishing clicks that did not result in compromise, attempted fraud stopped
- Time-to-detect and time-to-contain trend
- What was learned and what changed as a result

Slide 4 — What We Are Doing About It

Business question: Are we acting, or just watching?

- Key initiatives in flight — 3 to 5 max
- For each: owner, target completion date, status (on track / at risk / blocked)
- Completed initiatives since the last briefing

Slide 5 — What We Need From You

Business question: What decisions are we asking the board to make?

- Budget requests with direct tie to the top risks on slide 2
- Policy approvals — things only the board can authorize
- Strategic questions for board discussion
- Nothing ambiguous: every ask has a yes/no answer the board can give

Quarterly Self-Assessment Categories

Track each out of 10 points. Total becomes slide 1. Audit yourself before the board does it for you.

- **Passwords & Accounts** — unique passwords, MFA coverage, access reviews
- **Computer Security** — antivirus, patching, encryption, disposal
- **Backups** — automated, offsite, tested, ransomware-resistant
- **Email & Phishing** — filtering, DMARC, training, reporting
- **Policies & Training** — written, signed, refreshed quarterly
- **Vendor Oversight** — contracts, reviews, breach notification clauses
- **Incident Response** — written plan, tabletop drills, contact list
- **Physical Security** — screen locks, clean desks, visitor control
- **Data Protection** — encryption, retention, disposal
- **AI Governance** — acceptable-use policy, approved tools, monitoring

The Three Questions Every Board Should Ask

(1) How would we know if we were compromised right now? (2) If we had a ransomware attack tomorrow, could we operate for a week without paying? (3) Who has final accountability for cyber risk — and do they have the authority to match it?