Risk Snapshot Pack

Board-ready templates for fast, credible cyber risk reporting

What this pack is for

- Teams without a dedicated security leader (or needing a second opinion).
- Leaders who need a risk narrative the business can act on.
- Reducing sales friction from security questionnaires and audits.
- Creating a realistic 30/60/90 day plan with measurable outcomes.

Included templates

- 1) Risk Register Starter (likelihood/impact/owner/next action)
- 2) Board Reporting Cadence + KPI set
- 3) Ransomware Readiness Checklist (high-signal controls)
- 4) Second-Opinion Questions for your security stack and vendors

How to use this in 60 minutes

- Pick your top 10 risks (don’t exceed 10).
- Assign an owner and next action to each risk.
- Define 3 KPIs leadership will review monthly.
- Choose 5 ransomware controls to validate this week.
- Book a 15-minute call if you want a guided risk snapshot.

theCISO.ca • edc@theciso.ca

Template 1

Risk Register Starter (example structure)

Risk register fields

- Risk statement (what could happen, and why it matters)
- Business impact (revenue, operations, legal, customer trust)
- Likelihood (Low/Med/High) and impact (Low/Med/High)
- Current controls (what you already do)
- Gaps (what's missing)
- Next action (one step you will do next)
- Owner and due date

Tip: Write risks in plain English

Example: "A compromised admin account could allow ransomware to encrypt file shares, delaying shipping for 5–1

Template 2

Board Reporting Cadence + KPIs (starter set)

Monthly cadence (simple)

- Top 10 risk register changes (up/down/new/closed)
- Key metrics (below)
- Incidents / near misses and lessons learned
- Roadmap progress and decisions needed
- Vendor renewals / tool changes with risk impact

Starter KPIs

- MFA coverage (% of users and % of privileged accounts)
- Time to patch critical vulnerabilities (median days)
- Backups tested (restore test frequency and success rate)
- High-risk admin access paths closed (count)
- Incident response readiness (tabletop completed Y/N; action items closed)

Checklist

Ransomware Readiness (high-signal controls)

Validate these first

- Privileged accounts use MFA and are segmented from daily-user accounts.
- Admin access is least-privilege; remove standing admin wherever possible.
- Backups are immutable/offline and restore-tested (not just “backed up”).
- Critical systems are segmented; lateral movement is constrained.
- Email controls reduce phishing risk (DMARC, filtering, awareness).
- Endpoint protection is tuned; detections are reviewed, not ignored.
- An IR plan exists with contacts, escalation, and communications steps.
- A tabletop exercise has been done in the last 12 months.

Second Opinion

Questions to ask your security stack (and vendors)

High-signal questions

- Which 3 risks are materially reduced by this tool, and how do we measure it?
- What alerts are we ignoring, and why? (noise vs signal)
- Where do we have blind spots (identity, cloud configs, endpoints, SaaS)?
- Can we demonstrate a restore within RTO/RPO for critical systems?
- What’s our current mean time to patch critical vulns?
- If admin credentials are stolen, what limits blast radius today?
- Which vendors can access our sensitive data, and is access controlled and logged?
- What would we stop doing if we cut our toolset by 20%?