CEO Cybersecurity Readiness Assessment Checklist

Instructions

Use this assessment to evaluate your organisation's executive cybersecurity readiness and operational resilience maturity.

Score each item:

- Yes = 2 points
- Partial/In Progress = 1 point
- No = 0 points

Governance & Leadership

☐ Executive leadership receives regular cybersecurity risk updates.

☐ Cybersecurity responsibilities are clearly assigned.

☐ Leadership understands operational cyber dependencies.

☐ Cybersecurity is discussed during strategic planning.

☐ Incident escalation procedures are clearly defined.

Operational Resilience

☐ Critical operational systems have been identified.

☐ Backup and recovery procedures are tested regularly.

☐ Business continuity plans include cyber disruption scenarios.

☐ Incident response exercises are conducted periodically.

☐ Leadership understands ransomware response procedures.

Employee Awareness & Human Risk

☐ Employees receive regular phishing awareness training.

☐ Staff understand how to report suspicious activity.

☐ Executives participate in cybersecurity awareness initiatives.

☐ Remote workforce security guidance exists.

☐ Insider risk is considered in governance planning.

Vendor & Technology Oversight

☐ Third-party vendors undergo cybersecurity review.

☐ MFA is implemented across critical systems.

☐ Monitoring and detection capabilities are in place.

☐ Leadership understands major cybersecurity technology investments.

☐ Vendor accountability expectations are documented.

Compliance & Strategic Readiness

☐ Cyber insurance coverage is reviewed regularly.

☐ Governance documentation is maintained consistently.

☐ Data privacy obligations are understood operationally.

☐ Cybersecurity metrics are reviewed at the executive level.

☐ Continuous cybersecurity improvement initiatives exist.

Scoring Results

40–50 Points — Strong Executive Cyber Maturity

Your organisation demonstrates strong executive engagement, operational preparedness, and cybersecurity governance maturity.

Continue refining:

- resilience planning,
- vendor oversight,
- employee awareness,
- and incident readiness.

20–39 Points — Moderate Organisational Exposure

Your organisation has foundational cybersecurity practices but may still face operational and governance gaps.

Focus on:

- strengthening visibility,
- improving preparedness,
- clarifying accountability,
- and enhancing resilience planning.

0–19 Points — High Business Risk

Your organisation may face significant operational exposure involving:

- weak preparedness,
- limited governance,
- poor visibility,
- or insufficient incident readiness.

Immediate priorities should include:

- leadership engagement,
- incident planning,
- employee awareness,

and governance improvement.