Corporate security strategy scorecard

Eight questions, one per strategy in the guide. Circle one answer per question and add the points. 0 to 8 is Reactive, 9 to 16 is Managed, 17 to 24 is Intelligence-led.

01

SCORE

Risk assessment

When did you last complete a documented corporate security risk assessment with ranked risks and named owners?

- 0 Never or nobody can find it
- 1 More than two years ago
- 2 Within the last 12 to 24 months
- 3 Within the last 12 months and after every major change

02

SCORE

Layered defense

How many of these are in place: badge access control, EDR or XDR on endpoints, MFA on all critical systems, encrypted backups?

- 0 One or none
- 1 Two
- 2 Three
- 3 All four, verified by audit

03

SCORE

Incident response

Does a written incident response plan exist, with escalation criteria and when was it last exercised?

- 0 No written plan
- 1 Written, never exercised
- 2 Exercised in the last year
- 3 Tabletop or live drill in the last six months

04

SCORE

Awareness training

How do employees receive security awareness training?

- 0 They do not
- 1 One session at onboarding
- 2 Annual training
- 3 Quarterly sessions plus phishing simulations with a tracked failure rate

05

SCORE

Vendor security

What happens before a vendor gets access to your systems or data?

- 0 Nothing formal
- 1 A questionnaire, sometimes
- 2 A security review and contract clauses on access and breach notification
- 3 Review, contract clauses and continuous monitoring of vendor access

06

SCORE

Zero Trust

How is access to internal systems decided?

- 0 Anyone on the network can reach most systems
- 1 VPN plus passwords
- 2 MFA and role-based access on key systems
- 3 MFA, least privilege, micro-segmentation and continuous verification

07

SCORE

Frameworks and compliance

Is the program mapped to a named framework such as NIST CSF 2.0, ISO 27001 or ASIS SRA-2024?

- 0 No framework
- 1 A framework was chosen but controls are not mapped
- 2 Controls mapped, gaps documented
- 3 Mapped, audited by a third party and reviewed annually

08

SCORE

Monitoring and measurement

How is the program monitored and reported?

- 0 Ad hoc, when something breaks
- 1 Periodic vulnerability scans
- 2 Scans, external threat monitoring and an annual audit
- 3 Continuous monitoring plus quarterly KPI and KRI reporting to executives

TOTAL 0 to 8

Reactive

Controls exist in pockets. Start with the risk assessment, the written incident response plan and MFA on every critical system.

TOTAL 9 to 16

Managed

Core controls and a plan on paper. Map controls to one framework, add external threat monitoring and report KPIs quarterly.

TOTAL 17 to 24

Intelligence-led

The program anticipates threats. Keep the edge with red team exercises, third-party audits and OSINT-driven monitoring.