Cyber Risk / Governance Lead: senior interview pack

Translating cyber risk for executives, setting priorities with limited budget and defending decisions. Free from thallanaresh.com. Answers are outlines to adapt with your own examples.

Risk acceptances signed by the wrong people

Reviewing risk acceptances, you find many signed by team leads for risks well above their authority level.

Situation read: The acceptances look valid on paper but lack proper authority, so the organisation carries risk nobody senior agreed to.

What I'd do first: Map each acceptance against the delegation-of-authority matrix and re-route the largest ones to the right level.

Trade-offs: Re-approving all of them takes executive time; ignoring it leaves the governance gap.

What I'd tell leadership: I would tell leadership the number above authority in broad terms, the re-approval plan, and a workflow change that enforces the matrix automatically.

What interviewers listen for

- Knows delegation of authority
- Fixes the workflow
- Prioritises by exposure

Executives disagree on the top cyber risk

In a workshop, the COO says the top risk is downtime, the General Counsel says data privacy fines, and the CTO says insider threat.

Situation read: Each view reflects their exposure; the disagreement is useful information.

What I'd do first: Turn each concern into a scenario with impact and likelihood, then score them against the same criteria.

Trade-offs: Consensus may dilute focus; picking one may alienate others.

What I'd tell leadership: I would show the scenarios side by side and agree a prioritised list with owners, revisiting it quarterly.

What interviewers listen for

- Uses scenarios to compare views
- Facilitates rather than dictates
- Ends with owners

Three regulatory deadlines land in the same month

New incident-reporting, resilience-testing and privacy obligations all take effect in the same month. Each owner says theirs is the priority.

Situation read: Competing obligations share controls; treating them separately triples the work and confuses teams.

What I'd do first: Map the obligations to shared capabilities (incident classification, testing evidence, records) and find which gaps carry penalties or reporting exposure first.

Trade-offs: Unified delivery is efficient but slower to start; parallel projects show early progress but duplicate effort.

What I'd tell leadership: I would present one integrated plan with legal deadlines marked, the order of delivery and the residual non-compliance risk during the transition.

What interviewers listen for

- Finds shared capabilities across rules
- Prioritises by legal exposure
- Makes transitional risk explicit

A flagship security programme is over budget and late

An identity modernisation programme you sponsor is twice its timeline and well over budget. The steering committee asks whether to stop it.

Situation read: Sunk cost is irrelevant; the question is the remaining cost against the risk it still removes.

What I'd do first: Re-baseline what is delivered, what remains and which risks the remaining scope actually reduces, then look for a smaller scope that captures most of the value.

Trade-offs: Stopping wastes the learning and leaves legacy risk; continuing unchanged repeats the overrun.

What I'd tell leadership: I would recommend a re-scoped phase with fixed milestones and stop criteria, and state plainly which risks stay open if leadership cuts it.

What interviewers listen for

- Ignores sunk cost
- Re-scopes to value
- Sets stop criteria

A regulator asks for your cyber governance overnight

A regulator requests evidence of board oversight of cyber risk within two weeks. Minutes mention cyber rarely.

Situation read: Evidence of oversight is thin; inventing it would be worse than the gap.

What I'd do first: Gather what exists (reports, committee packs, decisions), and be clear about improvements under way.

Trade-offs: Over-polishing risks credibility; under-preparing risks findings.

What I'd tell leadership: I would brief the board on the request, agree a standing cyber agenda item, and submit factual evidence with a plan.

What interviewers listen for

- Is honest with regulators
- Strengthens governance going forward
- Prepares the board

Nobody owns operational technology risk

Plant systems are run by engineering, while security reports to IT. A recent near-miss shows OT risk falls between teams.

Situation read: Ownership gaps are the root issue; technical fixes alone will not stick.

What I'd do first: Agree a RACI between engineering and security, and start with an asset inventory for the most critical sites.

Trade-offs: Imposing IT controls may disrupt operations; leaving OT alone keeps the gap.

What I'd tell leadership: I would propose joint governance with clear ownership and a phased risk plan agreed with operations leaders.

What interviewers listen for

- Diagnoses ownership problems
- Respects operational constraints
- Phases the plan

A near miss nobody reported

You learn in passing that a misdirected file containing customer data was recalled last month. It was never logged as an incident.

Situation read: Under-reporting hides trends and may breach internal or legal reporting duties.

What I'd do first: Log it, assess whether any notification duty applies, and find out why staff felt it did not need reporting.

Trade-offs: Punishing the team discourages future reporting; ignoring it normalises silence.

What I'd tell leadership: I would report the near miss and the under-reporting pattern, and propose a no-blame near-miss channel with simple criteria.

What interviewers listen for

- Values near-miss data
- Checks legal duties
- Builds a reporting culture

A critical pen test finding days before launch

Days before a product launch, testers find a critical authentication flaw. Marketing has paid for launch events.

Situation read: Launching with a known critical flaw could expose customers and the company.

What I'd do first: Assess exploitability and possible fixes or mitigations quickly with engineering.

Trade-offs: Delaying costs money and reputation; launching risks a breach.

What I'd tell leadership: I would give leadership a clear recommendation with options (fix, mitigate and launch limited, or delay), and the risk owner signs the decision.

What interviewers listen for

- Gives options with clear risk
- Gets the decision owned
- Moves quickly

Teams game the security metrics

Vulnerability closure rates look great, but you learn teams are closing tickets as 'accepted' without approval.

Situation read: Metrics drive behaviour; this one rewards closing over fixing.

What I'd do first: Audit a sample of closures, and change the metric to separate fixed from accepted with approval.

Trade-offs: Calling out teams may cause defensiveness; ignoring it erodes trust.

What I'd tell leadership: I would report the corrected figures and explain the metric change, focusing on the process rather than individuals.

What interviewers listen for

- Checks the integrity of metrics
- Redesigns incentives
- Handles it without blame

Presenting a 90-day plan as a new risk lead

You join as the cyber risk lead. The CEO asks for your plan in a week.

Situation read: You need to listen before prescribing, but also show early direction.

What I'd do first: Meet key stakeholders, review recent incidents, audits and the register, and identify quick wins and major gaps.

Trade-offs: Moving fast risks wrong priorities; moving slowly loses momentum.

What I'd tell leadership: I would present a listening phase, early priorities, and how I will report progress, with one or two quick wins.

What interviewers listen for

- Balances listening and action
- Uses existing evidence
- Sets clear reporting