Board Guide to Cyber Risk Oversight

A practical guide for directors, owners and senior leaders of small and mid-sized businesses.

Nov 10, 2026 · @Vijay Srinivas Kothapalli

Executive summary

Cyber risk is now a business risk, not only an IT matter. A single incident can stop orders, expose customer data and damage lender and buyer confidence. The board does not need to manage security tools. It does need to know what could hurt the business, whether management is controlling those risks, and what happens when something goes wrong.

This guide sets out a practical way for a board to do that. It covers what to ask, what to track each quarter, how to prepare for an incident, and how to manage the vendors who hold your data. It is written for businesses where directors may also run the company day to day, and where there is no large security team.

Why cyber risk is a board matter

Smaller businesses are targeted because they are easier to break into, and because they often lack the backup systems and response plans that larger firms have. Attacks commonly arrive through an email that looks ordinary, a shared password, an unpatched device or a supplier with access to your systems.

The consequences fall on the whole business:

- Operations stop while systems are restored, sometimes for days.
- Customer, employee or supplier data may be exposed, with legal duties to inform those affected.
- Bank lenders, insurers and large buyers increasingly ask about security before they commit.
- Payments can be diverted by fraud, and the loss may not be recoverable.

For these reasons, cyber risk belongs on the board agenda alongside finance, legal and people risk.

Oversight versus management

The board sets direction and checks results. Management designs and runs the controls. Keeping these roles apart stops the board from drifting into technical detail, and stops management from reporting only what is comfortable.

Area	Board	Management
Risk appetite	Decides how much disruption and data exposure is acceptable	Proposes limits and reports against them
Priorities	Approves the security budget and the top risks	Builds and runs the plan
Incidents	Receives timely briefings and makes major decisions	Responds, contains and recovers
Vendors	Sets the standard for key suppliers	Assesses, contracts and monitors them
Assurance	Asks for independent checks	Arranges testing and fixes findings

A good test: if the board cannot say what would stop the business for three days, the oversight is not yet working.

Know what matters most

Before discussing controls, the board should agree on what the business cannot lose. Start with a short list of critical assets and dependencies:

1. **Revenue systems:** billing, ordering, dispatch and payment collection.
2. **Customer and employee data:** what you hold, where it sits and who can access it.
3. **Production or service delivery:** the systems or sites that stop work if they fail.
4. **Money movement:** bank access, payment approvals and vendor payments.
5. **Key suppliers:** the outside firms whose outage would stop you.

For each item, record how long it could be down before serious harm (the maximum tolerable outage), who owns it, and where its backups are kept. This list drives every later decision on spending, testing and priorities.

Seven questions every board should ask

Ask these at least once a year, and again after any incident. Good answers are specific, dated and backed by evidence.

1. **What are our most critical systems and data, and who owns them?** Expect a short list with named owners.
2. **If our main system stopped today, how long until we were working again?** Expect a tested recovery time, not an estimate.
3. **When did we last restore from backup, and did it work?** Backups that have never been restored are not proven.
4. **Who can approve a payment or change bank details, and how is that checked?** Expect two-person approval for payments and call-back checks for changed details.
5. **Which suppliers can access our systems or data, and what do their contracts say about security and incidents?**
6. **What have we fixed from the last independent test, and what is still open?**
7. **Who makes the call to notify customers, regulators or the bank, and how fast?** Expect a named person and a written deadline.

An answer such as "our IT provider handles it" is a starting point, not a result. Ask what the provider has actually done, and when.

A quarterly oversight rhythm

Review cyber risk at every quarterly board meeting, with a one-page report from management. Keep the same measures each quarter so trends are visible. The figures below are a starting set; choose the ones that fit your business.

Measure	What it tells the board	Target to aim for
Critical systems with a tested recovery	Whether the business can recover	All critical systems tested in the last 12 months
Backup restore tests passed	Whether backups actually work	Every quarter, full restore of one critical system
Staff completing security awareness training	Whether people can spot attacks	Above 95 percent within 30 days of joining

Measure	What it tells the board	Target to aim for
Critical and high findings open	Known weaknesses still unfixed	Zero critical open beyond 30 days
Privileged accounts reviewed	Who holds administrator access	All reviewed each quarter, unused ones removed
Supplier reviews completed	Whether key vendors are checked	All key suppliers reviewed each year
Incidents reported and closed	How often things go wrong and how fast they are resolved	Each incident with a written root cause
Payment changes verified by call-back	Protection against payment fraud	100 percent of changes to bank details

Ask management to explain any measure that moves the wrong way, and what it will do about it.

Incident readiness: the first 72 hours

Most of the damage from an incident is decided in its first hours. Agree these steps before anything happens, and rehearse them once a year with a short table-top exercise.

1. **Contain.** Isolate affected devices or accounts. Do not switch systems off without a record, because evidence is lost.
2. **Assign roles.** Name one incident lead, one person for technical work, one for communication and one who keeps the log.
3. **Preserve evidence.** Keep logs, screenshots and the times of each action.
4. **Assess.** Within the first few hours, establish what was accessed, what is at risk and whether customer or personal data is involved.
5. **Inform.** Brief the board chair or a named director the same day. Contact the bank if money may be affected, your insurer if your policy requires it, and any regulator where a legal duty applies. Check those duties with a lawyer before the incident, not during it.
6. **Communicate.** Prepare short, factual messages for staff, customers and suppliers. Say what you know, what you are doing and when you will update them next.
7. **Recover.** Restore from clean backups, test before reconnecting, and change passwords and access for affected accounts.

8. **Learn.** Within two weeks, write a root-cause review and assign each fix an owner and a date.

Keep an up-to-date contact list for the incident lead, technical support, the bank, the insurer and legal advisers. A printed copy is useful if email is down.

Vendors and outsourcing partners

Many breaches start at a supplier: an IT provider with administrator access, a payroll bureau, a cloud service or an outsourced accounts team. Your duties to customers and staff do not transfer to the supplier.

For each vendor that holds data or access, the board should be able to see:

- What data or systems they can reach, and why.
- Whether their contract requires security standards, incident notice within a set time, and the right to audit.
- Who in your business owns the relationship.
- How access is removed when the contract ends.

Rank suppliers by impact. Review the top few every year, and ask for their latest security assurance in writing. Where a supplier cannot answer simply, treat that as a finding.

People and roles

Technology controls fail most often through people: a shared password, a convincing phishing email or an urgent request to change bank details. Assign clear accountability so that someone owns each area.

Role	Accountable for
Board member for cyber risk	Asking the questions, challenging the answers, reporting to the full board
Senior manager or owner	Budget, priorities and the incident plan
Operations or IT lead	Day-to-day controls, backups, patching and access
Finance lead	Payment approvals and bank detail changes
All staff	Reporting suspicious messages at once and following the rules

Train every person who joins, and refresh the training each year. Short, realistic exercises, such as a simulated fake invoice, teach more than long presentations.

Spending proportionately

There is no fixed percentage of revenue that is right for every business. Spend in proportion to what the critical assets list shows could be lost. A reasonable start for many small businesses is to fund the basics first:

- Multi-factor sign-in on email, banking and administrator accounts.
- Regular, tested backups kept apart from the main systems.
- Timely updates for devices, software and routers.
- Staff training and a payment-verification routine.
- A yearly independent security check of the most important systems.

Spend on these before tools and advanced products. A board that funds the basics and checks that they are working is in a stronger position than one that buys many tools and cannot say what they do.

A 90-day plan for boards starting this work

Period	Action	Owner
Days 1 to 30	Agree the critical assets and dependencies list. Ask the seven questions and record the answers.	Board, with senior management
Days 1 to 30	Confirm who holds administrator access and who approves payments.	Operations and finance leads
Days 31 to 60	Turn on multi-factor sign-in for email, banking and administrator accounts. Test one backup restore.	IT or operations lead
Days 31 to 60	List key suppliers with data or system access, and check their contracts.	Owner or senior manager
Days 61 to 90	Run a one-hour incident table-top exercise with the board and management.	Board chair and senior manager
Days 61 to 90	Adopt the quarterly measures and set the first targets.	Board

At day 90, the board should be able to say what it protects, how it would recover, and what it still needs to fix.

Board checklist for oversight of cyber risk

- [ ] A critical assets and dependencies list is agreed and reviewed each year.
- [ ] Each critical system has a named owner and a tested recovery time.
- [ ] Administrator access is limited, reviewed each quarter and protected by multi-factor sign-in.
- [ ] Backups are kept apart from the main systems and restore tests are recorded.
- [ ] Payments need two approvals, and changes to bank details are verified by call-back.
- [ ] Key suppliers with data or system access are listed, reviewed and contracted for security and incident notice.
- [ ] Staff complete security training when they join and each year after.
- [ ] A written incident plan names the lead, the contacts and the notification duties.

- [ ] A table-top exercise has been run in the last 12 months.
- [ ] Quarterly board reporting covers the agreed measures, with an explanation of any that have worsened.
- [ ] Findings from the last independent check have owners and dates.

About CRCO LLP

CRCO LLP is a Hyderabad-based advisory firm that works with businesses on cybersecurity, data privacy and protection, outsourcing, process improvement and automation. We help boards and owners set practical priorities, test their controls and build the habits that keep risk under watch.

We can help you with the assessment of your critical assets, a review of your supplier risks, a board briefing on cyber oversight, incident readiness exercises and the design of a quarterly reporting pack.

Book a consultation: visit the Contact page on our website, or write to us through the enquiry form.

This guide provides general information only. It is not legal advice. Specific legal duties depend on your sector and circumstances, and should be confirmed with a qualified adviser.