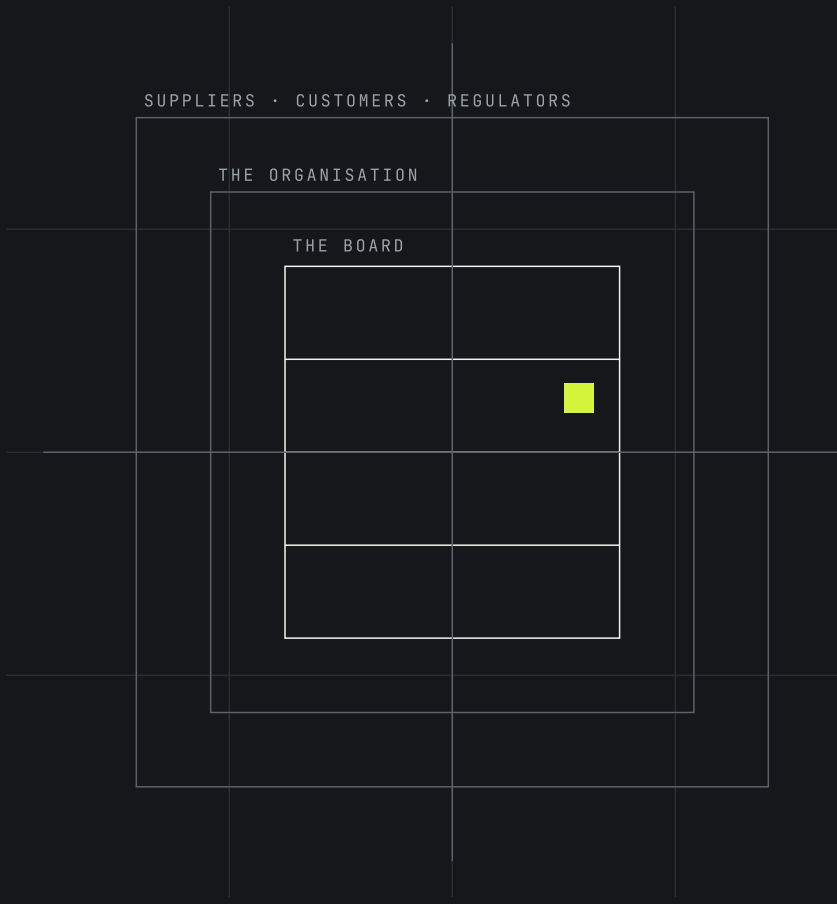

Cyber risk. *A pack for the board.*

Ten questions to ask, five numbers to watch, and what the board decides in the first day of an incident. For directors, trustees and governors.

READING TIME
Fifteen minutes

FOR
Board and committee members

FROM
Privion, London

HOW TO USE THIS PACK

Security is now a *board matter.*

Boards are not expected to run security. They are expected to understand the risk, set how much of it the organisation will accept, and check that it is being managed. This pack is written for that job.

Each section stands on its own. Take the questions into your next board or audit committee meeting, ask for the five numbers each quarter, and agree in advance what the board will decide if an incident happens. The scorecard at the back gives you a quick view of where you stand today.

It follows the spirit of the government's Cyber Governance Code of Practice and the NCSC's Cyber Security Toolkit for Boards, in plain language and without jargon.

I Ten questions for the board 03

II Five numbers to ask for each quarter 05

III The first twenty-four hours of an incident 06

IV Five questions for your critical suppliers 07

V A one-page board scorecard 08

> **A note on tone.** None of these questions should feel like an interrogation. A good security lead will welcome them, and the conversation they start is worth more than any single answer.

Ten questions *worth asking.*

1 What matters most to us, and who owns protecting it?

WHY IT MATTERS

You can't protect everything equally. The board should know which systems, data and services the organisation could not do without.

A GOOD ANSWER

A short, named list, each with an owner, reviewed at least once a year.

2 Who is accountable for cyber risk, and how often do we hear from them?

WHY IT MATTERS

When everyone owns security, no one does. Accountability needs a name and a regular slot on the agenda.

A GOOD ANSWER

A named executive, a report to the board at least quarterly, and a clear route to escalate.

3 How would we know if someone was inside our systems today?

WHY IT MATTERS

Attackers often sit unnoticed for weeks before they act. Detection is what shortens that window.

A GOOD ANSWER

Alerts watched by a person or service, with a recent example of something caught and handled.

4 If our systems stopped tomorrow, how long could we keep operating?

WHY IT MATTERS

Ransomware is mostly a business continuity problem. The answer sets how much downtime you can afford.

A GOOD ANSWER

A tested plan with a realistic recovery time for each critical service, and a date it was last rehearsed.

5 Are our backups out of an attacker's reach, and when did we last restore one?

WHY IT MATTERS

Attackers target backups first. A backup that has never been restored is a hope, not a plan.

A GOOD ANSWER

Backups kept separately and protected from deletion, with a successful full restore in the last quarter.

CONTINUED OVERLEAF

6 Which suppliers could hurt us most, and what do we know about them?

WHY IT MATTERS

Many serious incidents start at a supplier. Your risk includes every company with access to your systems or data.

A GOOD ANSWER

A ranked list of critical suppliers, each checked before contract and reviewed each year.

7 Is multi-factor sign-in switched on everywhere that matters?

WHY IT MATTERS

Stolen passwords are still the most common way in. A second factor stops most of those attempts.

A GOOD ANSWER

Yes for email, remote access, admin accounts and suppliers, with any exceptions listed and owned.

8 What does our cyber insurance require of us, and are we meeting it?

WHY IT MATTERS

Policies carry conditions. If controls you declared are not in place, a claim can be reduced or refused.

A GOOD ANSWER

The policy conditions mapped to evidence, checked at each renewal, and the insurer's incident line known.

9 Who decides what in the first day of an incident?

WHY IT MATTERS

Incidents move faster than meetings. Decisions made in advance save hours when hours count.

A GOOD ANSWER

A written plan naming the incident lead, the board's role, outside help on call, and the stance on ransom demands.

10 Is our spending going where the risk is?

WHY IT MATTERS

Security budgets drift towards tools. The board should see spend set against the risks that matter most.

A GOOD ANSWER

A short view linking each major cost to a risk it reduces, and the gaps still open.

> **If an answer is unclear,** that is useful too. Note it, set a date to come back to it, and make sure someone owns the follow-up.

Five numbers, *every quarter.*

A board does not need fifty metrics. These five, tracked over time, tell you whether security is getting better or worse.

01 · SIGN-IN PROTECTION

96% ACCOUNTS WITH MFA

Share of accounts protected by a second factor. Aim for all of them, with any exceptions named.

02 · PATCHING

9 DAYS TO FIX CRITICAL FLAWS

Average time to fix a critical, internet-facing weakness. Fourteen days or fewer is a sound target.

03 · RECOVERY

Aug LAST FULL RESTORE TEST

When a complete restore from backup last worked. Older than a quarter deserves a question.

04 · OPEN RISKS

4 HIGH RISKS OPEN

High risks on the register, how long each has been open, and who owns it. Watch the age, not only the count.

05 · SUPPLIERS

7 of 9 CRITICAL SUPPLIERS REVIEWED

Critical suppliers whose security was checked in the last twelve months.

READING IT

Ask for the trend, not just the figure. A number moving the right way each quarter says more than a single good result. The lime bar marks the one to raise.

FIGURES SHOWN ARE EXAMPLES ONLY

The first *twenty-four hours.*

The board does not run the response. It makes a small number of decisions quickly, and makes sure the right people are doing the rest.

HOUR 0 TO 1

Contain

- Incident lead takes charge
- Affected systems isolated, not wiped
- Chair or chief executive told
- Start a written log of decisions

HOUR 1 TO 4

Bring in help

- Call your incident response partner
- Notify your insurer, often a policy condition
- Take legal advice early
- Agree who speaks for the organisation

HOUR 4 TO 24

Decide and tell

- Assess whether personal data is affected
- Plan notifications to regulators and customers
- Brief staff on what to say and not say
- Set the next update for the board

Decisions that belong to the board

I **Spend.** Approve outside help without waiting for the next meeting.

II **Notification.** The ICO expects a reportable personal data breach within 72 hours of becoming aware of it. Sector regulators may have their own deadlines.

III **Communication.** What customers, staff and the public are told, and when.

IV **Ransom.** Your stance agreed in advance, with legal advice. Paying does not guarantee recovery and can raise sanctions questions.

> **Print this page.** Keep a paper copy with your incident plan and the key phone numbers. When systems are down, the plan on the shared drive may be out of reach too.

Five questions for *critical suppliers.*

Send these before you sign, and again each year. How a supplier answers tells you as much as what they say.

01 ### What access to our systems and data will you have?

Ask for the specifics: which systems, which data, how many of their people, and from where.

02 ### How do you protect it, and can you show us?

Certifications such as ISO 27001 or Cyber Essentials help, as long as the scope covers the service you are buying.

03 ### How quickly will you tell us about an incident?

Look for a time written into the contract, and a named contact on both sides.

04 ### Who else handles our data on your behalf?

Their suppliers become your risk. Ask for the list and how they are checked.

05 ### What happens to our data when the contract ends?

Agree how it is returned or deleted, and how you will know it has been.

> **Keep it in proportion.** Spend most of your effort on the handful of suppliers that could stop your business or expose your most sensitive data.

Where do we *stand today?*

Answer honestly, as a board. It takes five minutes and makes a good opening item for your next meeting.

STATEMENT	YES	PARTLY	NO
01 We know which systems and data matter most, and who owns each	☐	☐	☐
02 A named executive is accountable for cyber risk	☐	☐	☐
03 The board hears about cyber risk at least quarterly	☐	☐	☐
04 We have agreed how much cyber risk we will accept	☐	☐	☐
05 Multi-factor sign-in protects email, remote access and admin accounts	☐	☐	☐
06 A full restore from backup has worked in the last quarter	☐	☐	☐
07 We have a written incident plan and have rehearsed it this year	☐	☐	☐
08 The board has agreed its stance on ransom demands	☐	☐	☐
09 Critical suppliers are checked before contract and each year	☐	☐	☐
10 We meet the conditions of our cyber insurance, with evidence	☐	☐	☐
11 Board members have had a cyber briefing in the last year	☐	☐	☐
12 We could answer a customer's security questionnaire with confidence	☐	☐	☐

Mostly yes

A solid base. Keep testing it, and use the five numbers to make sure it stays that way.

Mostly partly

Common, and very fixable. Pick the three that matter most and give each an owner and a date.

Several no

Worth an independent view soon, before a customer, insurer or incident asks the question for you.

ABOUT PRIVION

A senior adviser *for your board.*

Privion is a UK cyber security advisory practice led by Ashley Adkins, an ISO 27001 practitioner with more than twenty years' experience. We help boards understand their risk, meet what clients and regulators expect, and respond well when something goes wrong.

Security advisory

A fractional CISO for your leadership team, on a retained or project basis.

ISO 27001 and assurance

From gap analysis to certification, plus the evidence clients and insurers ask for.

Incident response

Containment, investigation and recovery, led personally from the first call.

Board and third-party risk

Board briefings, supplier assurance and readiness for client security reviews.

TALK IT THROUGH

privion.co.uk/start

CALL

020 3095 6789

EMAIL

enquiries@privion.co.uk

This pack is general guidance for boards and does not replace advice on your own circumstances. You are welcome to share it in full with colleagues and fellow directors. © 2026 Privion.