

Seven cyber questions every charity trustee should be able to answer

You don't need technical knowledge to govern cyber risk well. You need to know which questions to ask — and roughly what a good answer sounds like.

QUESTION 1

What would actually stop if we lost access to our systems tomorrow?

☐

Good: names actual services and timescales.

Probe: a technical answer that never mentions a beneficiary.

QUESTION 2

Who has access to our most sensitive information — and should they?

☐

Good: reviewed on a date, with findings and removals.

Probe: “only those who need it” — intention, not evidence.

QUESTION 3

When did we last test a restore — not just check the backup ran?

☐

Good: an actual restore, and how long it took.

Probe: “backups run nightly and we’ve never had a problem.”

QUESTION 4

What are we required to protect — by law, funder, or contract?

☐

Good: a list of obligations the board has seen.

Probe: nobody has mapped what's been promised.

QUESTION 5

In the first hour of a serious incident, who decides what?

☐

Good: a named lead, escalation route, and a tested plan.

Probe: a plan exists but nobody can say when it was opened.

QUESTION 6

Which of our suppliers could hurt us if they were breached?

☐

Good: knows which few matter and has asked them properly.

Probe: assumes suppliers are someone else's problem.

QUESTION 7

Are staff putting our information into AI tools?

☐

Good: clear written guidance, named tools, staff told.

Probe: “we don’t allow it” — with no way to know.

Sort what you find into three groups.

You will find gaps. Every organisation has them. What matters is not turning seven questions into a twenty-item plan that stalls by week three.

NOW

Real harm if it happened
Fixable in weeks
Usually: backups,
stale access, admin MFA

NEXT

Needs planning or budget
Sequenced deliberately
Usually: supplier reviews,
incident plans, certification

LATER

Genuinely worth doing
Not urgent
Parked honestly, not
quietly forgotten

Three things finished beats fifteen things started.

That is true of most charity work, and it is certainly true of security. The goal is not a board that understands cyber security — it is a board that knows whether the organisation is managing it well.

IF IT WOULD HELP

Not sure how your organisation would answer these?

That's exactly what a Cyber Security Health Check is for — where you stand, what to fix first, and a one-page summary your trustees can actually read. hello@cyberforpurpose.co.uk