Ceidwad Education

The governor cyber security question pack

Ten questions a governing body can ask about cyber security — with what a good answer sounds like, and what should worry you. No technical knowledge needed. One or two per meeting is plenty.

How to use it: put the question to the leader who owns the risk, in advance rather than as an ambush. Ask for answers to come back in writing where they need checking. “We don’t know” is a safe and useful answer — it is a risk discovered for free.

QUESTION 1

Who is accountable for cyber security, by name — and who actually does the work?

A good answer: Two different names, both known to the board: a leader who owns the risk, and whoever (often an external IT provider) operates the controls. The split is written down.

What should worry you: “IT handle it.” Accountability delegated to a supplier is accountability nobody holds.

Notes / date asked / answer received:

QUESTION 2

When did we last check where we stand, and can I see the result?

A good answer: A dated document — an assessment, an audit, a review — from the last twelve months, with actions that have owners.

What should worry you: Reassurance with no date and no paper. If nothing is written down, the honest answer is “we don’t know where we stand”.

Notes / date asked / answer received:

QUESTION 3

Is multi-factor authentication enforced for every staff account — not just available?

A good answer: “Enforced for all staff and for the administrator accounts, and here is how we know.” MFA means a second check beyond the password, like a code on a phone.

What should worry you: “We have MFA” without the word enforced. Available-but-optional protects only the people who opted in.

Notes / date asked / answer received:

QUESTION 4

If ransomware encrypted everything tonight, what would we still have tomorrow?

A good answer: A backup that an attacker inside the network could not also delete, and a named person who has actually restored from it — with roughly how long a full restore takes.

What should worry you: "We back up to the server." A backup the attacker can reach is part of the ransom.

Notes / date asked / answer received:

QUESTION 5

What happens in the first hour of an incident, and is the plan reachable when systems are down?

A good answer: A printed or separately-stored plan naming who leads, who is called (IT, insurer, and the ICO where personal data is involved), and who speaks to parents.

What should worry you: A plan that lives only on the network — or a plan nobody has rehearsed, even as a twenty-minute conversation.

Notes / date asked / answer received:

QUESTION 6

Are we working to the DfE cyber security standard, and which parts don't we meet yet?

A good answer: A named list of gaps with dates. Not meeting all of it yet is normal; not knowing the gaps is the risk.

What should worry you: "Yes, we're compliant" with no gaps named — the standard is demanding enough that a gap-free answer usually means it hasn't been read.

Notes / date asked / answer received:

QUESTION 7

Which suppliers hold our data, and what have they promised us about security?

A good answer: A short list — MIS, payments, catering, IT provider — of who holds what, with contracts or assurances on file.

What should worry you: Nobody can produce the list. Your data protection duties follow the data into every one of those systems.

Notes / date asked / answer received:

QUESTION 8

When staff receive a suspicious email, what do they do — and do they actually do it?

A good answer: A reporting route staff can name, and examples of it being used recently. Early reports are the school's alarm system.

What should worry you: Blame attached to clicking. A school where people fear owning up hears about incidents last.

Notes / date asked / answer received:

QUESTION 9

What did our insurer or the RPA ask us to have in place — and would a claim succeed today?

A good answer: Somebody has read the policy conditions and checked them against reality, recently. Cover often depends on specific controls being demonstrably in place.

What should worry you: Insurance treated as the plan. A condition failed quietly is cover that isn't there.

Notes / date asked / answer received:

QUESTION 10

When will this board next hear about cyber security — without an incident forcing it?

A good answer: A standing slot — termly is proportionate — with a short report a non-specialist can read.

What should worry you: "When something changes." A risk this size reported only on failure is not being governed.

Notes / date asked / answer received:

Drawn from the NCSC's **Cyber Security Toolkit for Boards** and the DfE's **cyber security standard for schools and colleges**, translated for governing bodies by Ceidwad. The full guide, with each question explained: **ceidwad.co.uk/guides/cyber-security-for-governors** ·