5 Cyber Questions **Boards Should Ask**

Beyond compliance checkboxes

Wylie Blanchard

Most board cyber briefings sound like this:

- Policies?
- Audits?
- Training?
- “No major findings”?

Important. But incomplete.

→

Compliance tells you what exists.

Readiness tells you what works under pressure.

Boards don’t need more technical detail. They need operational clarity.

1) If systems went down tomorrow...

How long until we’re operational again? **And who tested that recently?**

(Backups aren’t the point. Restores are.)

2) How fast do we patch critical issues?

What’s our average time to patch?
And what consistently slows us down?

(A policy isn’t a result. Cycle time is.)

3) Who has access to sensitive data—today?

And when was access last reviewed?

(Privilege creep is quiet —and common.)

→

4) If our lead IT person is unavailable...

without operational gaps?

(Single points of failure aren’t just technical.)

5) What would a real incident cost us?

Downtime. Notification. Recovery. **Are we prepared to absorb the impact?**

(Insurance helps—after you understand exposure.)

→

Good governance isn’t eliminating risk.

It’s knowing **where it lives**—
and whether you can **operate through it**.

What's one board question you've seen consistently surface real risk?

Wylie Blanchard