/ free resource

Board Security Readiness Checklist

Ten questions every board and leadership team should be able to answer about cybersecurity, with what "good" looks like for each. Use it to start the conversation, not to replace an assessment.

How to use it: answer each question honestly. Score Yes = 2, Partly = 1, No = 0, then total your score at the end.

01 NIST CSF 2.0: Identify

Do we know which systems and data matter most, and who owns each one?

You cannot protect what you have not inventoried. Good looks like: a current list of critical systems, sensitive data, and a named owner for each.

☐ Yes ☐ Partly ☐ No

02 NIST CSF 2.0: Govern

Who is accountable for cybersecurity at the executive level?

Without a named owner, security decisions stall. Good looks like: one executive owns cyber risk and reports to leadership on a set schedule.

☐ Yes ☐ Partly ☐ No

03 NIST CSF 2.0: Govern

What are our top five cyber risks, and are they getting better or worse?

Boards should see risk in business terms, not tool alerts. Good looks like: a ranked risk register reviewed at least quarterly, with trends.

☐ Yes ☐ Partly ☐ No

04 NIST CSF 2.0: Protect

Is multi-factor authentication enforced on email, remote access, and every admin account?

Stolen passwords remain a leading way attackers get in. Good looks like: MFA on 100% of these, with exceptions documented and approved.

☐ Yes ☐ Partly ☐ No

05 NIST CSF 2.0: Protect

How fast do we fix critical vulnerabilities on internet-facing systems?

Attackers exploit known flaws within days of disclosure. Good looks like: a written remediation target, such as 14 days, and a measured track record against it.

☐ Yes ☐ Partly ☐ No

06 NIST CSF 2.0: Recover

Could we restore our critical systems from backup, and when did we last prove it?

Untested backups often fail when they are needed most. Good looks like: offline or immutable backups and a successful restore test within 12 months.

☐ Yes ☐ Partly ☐ No

07 NIST CSF 2.0: Govern

Which vendors hold our sensitive data or connect to our network, and have we assessed them?

Many breaches start at a supplier. Good looks like: vendors tiered by risk, with the highest tier reviewed before signing and each year after.

☐ Yes ☐ Partly ☐ No

08 NIST CSF 2.0: Respond

Do we have an incident response plan, and have leaders practiced it in the last 12 months?

The first hours of an incident decide its cost. Good looks like: a written plan with roles and contacts, tested in an executive tabletop exercise.

☐ Yes ☐ Partly ☐ No

09 NIST CSF 2.0: Protect

Are employees trained to spot phishing, and do we measure how they perform?

People are both the target and the first line of defense. Good looks like: regular training plus simulated phishing with results tracked over time.

☐ Yes ☐ Partly ☐ No

10 NIST CSF 2.0: Govern

Does our cyber insurance match our real risks, and can we meet its security requirements?

Insurers can deny claims when required controls are missing. Good looks like: coverage reviewed against your risk register and every policy condition verified.

☐ Yes ☐ Partly ☐ No

Your total: _____ / 20

16 to 20: Strong
Keep measuring and reporting. Focus on testing and continuous improvement.

10 to 15: Developing
Foundations exist but gaps remain. A prioritized 12-month roadmap will close them.

0 to 9: At risk
Exposure is likely higher than leadership realizes. Start with ownership, MFA, and backups.

Want a second opinion on your answers?

Book a free 30-minute conversation. Plain answers, no sales script.

inquiry@winsconsultingservices.com
(814) 975-9443

Jerald West, D.Sc., CISSP · WINS Consulting Services LLC · Midlothian, Virginia. This checklist is general guidance, not a substitute for a professional assessment. © 2026 WINS Consulting Services LLC.