

Healthcare **CYBER RISK READINESS CHECKLIST**

Take a 2-minute self-assessment to gauge your readiness across key cyber risk areas.

Ownership & Decision Authority



A cybersecurity lead is formally designated.



Cyber responsibilities are clearly mapped across leadership.



Security decisions are reviewed at the executive level.



Policy & Documentation

-  Written cybersecurity policies are current and accessible.
-  Staff receive regular training on those policies.
-  System changes and data access updates are documented.

Incident Readiness & Drill Frequency

-  We have a documented incident response plan.
-  Tabletop drills or response exercises are conducted twice per year.
-  Roles and escalation procedures are clearly outlined.

Get a clear view of where coverage ends and risk begins.

Your MSP focuses on availability. Compliance requires a different lens. This sidecar review highlights the blind spots your IT provider may not cover—HIPAA, CMMC, NIST CSF, Zero Trust, and more—without the blame game.

Contact Us:

-  protectthecube.com
-  info@protectthecube.com
-  888-408-CUBE

Technical Coverage

-  All systems and applications are regularly patched.
-  MFA is enforced across users and systems.
-  Backups are encrypted, verified, and tested.

Audit/Insurance Documentation Preparedness

-  We can produce documentation of our cybersecurity controls within 24 hours.
-  Logging, access control, and asset inventories are maintained.
-  Compliance and insurance records are ready for external review.

