

10 Ways to Harden Your Network & Pass Your Next Security Risk Assessment

A straight-talk checklist for business owners who can't afford a breach — built from 11 years securing rural healthcare, banks, and small business across Texas, Oklahoma, and New Mexico.

An SRA (Security Risk Assessment) is how auditors — and attackers — measure whether your business is actually protected. **Here's what separates a pass from a finding.** Work down this list; the ones you can't confidently check are exactly where you're exposed.

1 Turn on MFA everywhere

Multi-factor on email, remote access, banking, and every admin login — not just one app. It stops the majority of account takeovers cold.

Most findings: MFA on email only, nowhere else.

2 Patch on a schedule

Operating systems, firmware, and apps — unpatched software is the #1 way in. Set a monthly cadence and verify it actually ran.

"Auto-update is on" is not a patch policy.

3 Segment your network

Keep guest Wi-Fi, security cameras, POS, and clinical/financial systems on separate segments. One infected laptop shouldn't reach everything.

Flat networks fail this every time.

4 Kill everyday admin rights

Nobody should do daily work on an admin account. Least privilege means a compromised user can't hand over the whole network.

Shared "admin" logins are an instant red flag.

5 Back up 3-2-1 — and test it

Three copies, two media types, one off-site/immutable. Then actually restore from it. An untested backup is a hope, not a plan.

Ransomware's favorite victim: no tested restore.

6 Business-grade firewall

Replace the consumer router with a managed firewall doing content filtering and intrusion prevention — and keep its firmware current.

The ISP's free box doesn't count.

7 EDR, not just antivirus

Modern threats walk past basic AV. Endpoint Detection & Response (ideally monitored 24/7) catches what signatures miss.

Free AV alone won't pass a serious SRA.

8 Train your people

Phishing is how most breaches start. Short, regular training plus simulated phishing turns your staff into a firewall instead of the hole.

People are the #1 entry point — and the cheapest fix.

9 Lock down remote access

No open RDP to the internet. Use a VPN or zero-trust access with MFA for anyone working remotely.

Exposed RDP is scanned within minutes of going live.

10 Know & document your compliance

HIPAA, FFIEC/GLBA, SOX — know which apply, and keep written policies and an incident-response plan. Auditors check for the paper, not just the tech.

"We do it, we just didn't write it down" still fails.

Couldn't confidently check a few of these? That's normal — and fixable.

Doing all ten right takes tools and time most teams don't have in-house. That's exactly what we do. Two ways we can help:

Paid Security Risk Assessment — know exactly where you stand

Hosted & Managed Solutions — we run all ten for you