INCIDENT RESPONSE CHECKLIST

(NO BS VERSION)

A 30-second gut check to see if your team is actually ready.

www.tylerforrester.com

1. BASIC READINESS

Stuff you should already have... but most teams don't.

- □ Who's in charge when everything breaks? (IR lead identified)
- □ Everyone knows who to call at 2 AM
- □ You have ONE place where all contacts actually live
- □ You know who can officially declare an incident
- □ You have a secure comms channel (not Slack... seriously)

2. THE PLAN ITSELF

If you miss even one of these, your IR plan is basically a Word doc.

- □ Clear triggers: What counts as an incident here?
- □ Severity levels: How bad is bad?
- □ Containment steps: What's the first move?
- □ Eradication steps: How do we kill it?
- □ Recovery steps: How do we get back online?
- □ Evidence handling: Who collects what and where does it go?
- □ Tooling list: Which logs, consoles, and platforms matter most?

3. TABLETOP REALITY CHECK

Not theory — actual muscle memory.

- □ You've run a scenario in the last 12 months
- □ Your team didn't freeze, argue, or shrug
- □ Someone took notes that didn't end up lost
- □ You left with real improvements (not "we should communicate better")

4. AUDIT SURVIVAL

What SOC 2 / ISO / HIPAA reviewers will ask before anything else.

- □ "Show me your IR plan."
- □ "Show me proof it was reviewed this year."
- □ "Show me a tabletop from this year."
- □ "Show me the improvements from that tabletop."
- □ "Show me where all IR artifacts live."

If any of those make you sweat, that's your gap.

5. INSTANT RED FLAGS

A quick litmus test nobody admits out loud:

- □ We haven't updated our plan in a year (or... ever)
- □ We've never done a tabletop
- □ Nobody can find the last IR plan
- □ We rely on a vendor and hope they "just handle it"
- □ If an auditor showed up today, we'd stall

Ready to stop guessing and get a real IR plan?

Get it off your plate → Click here to get Incident Ready now.!