

Internal Security Readiness Assessment



Critical Questions for Your Organization

Staff & Training

1. Have you ever tested your staff's ability to identify phishing emails? When was the last time?
2. Do you have mandatory security training for all staff?
3. Does everyone know the incident reporting process?

Financial Controls

4. Do you have specific protocols for verifying financial requests? (Phone verification, multiple approvals)
5. Is access to financial accounts limited to necessary people only?

Communications & Data

6. Are client communications encrypted?
7. Is sensitive data encrypted on devices and servers?

Compliance & Insurance

8. Does your cyber insurance cover data breach, cyber extortion, and legal defense? (Do you have cyber insurance?)
9. Are you compliant with relevant regulations? (GDPR, CCPA, HIPAA, state bar rules)

Red Flags to Watch For:

- Unexpected password resets or login attempts from unfamiliar locations
- Emails with misspelled domains or urgent requests that bypass normal procedures
- Colleagues asking about strange requests they received from you

If You See These: Change passwords immediately, notify IT, review account activity.

Quick Assessment

- Mostly "Yes" answers: You're protected. Keep monitoring.
- Mostly "Some" answers: You have gaps. Address financial controls and encryption first.
- Mostly "No" answers: You have significant risk. Get professional help now.

Questions? Let's talk through your security posture.

This is educational, not legal advice. For guidance on your specific situation, let's talk.

