10-Point IT Risk Checklist for LA Law Firms

> **A self-assessment for managing partners, office managers, and IT leads at law firms in Greater Los Angeles.** Ten questions every law firm should be able to answer about its IT and security posture. If you can't answer any of these confidently, there's risk worth addressing.

Author: George Bederyan · Verta IT Solutions LLC **Audience:** LA law firms · 5-25 attorneys **Use:** Self-assessment, internal review, vendor evaluation **Time to complete:** ~10 minutes

---

Why this checklist exists

Most law firms don't have a dedicated IT person — and the ones that do often have an overworked generalist juggling helpdesk tickets, vendor coordination, and "the printer is broken again." Strategic IT risk usually sits unaddressed until something breaks.

This checklist is the questions a privileged client conversation between us would surface. Answer honestly. Where you don't know the answer, write "unknown" — that's information too.

The 10 questions

1. Email security and impersonation

If a paralegal received an email that looked like it was from a managing partner asking them to wire trust account funds, what would stop them from acting on it?

The answer should involve at minimum: (a) sender authentication (SPF/DKIM/DMARC configured on your domain), (b) anti-phishing controls in Microsoft 365 Defender or equivalent, and (c) a written policy that wire transfers require verbal confirmation regardless of email source.

If your answer is "they'd probably notice it's fake" — that's not a control, that's hope. Business Email Compromise (BEC) is the #1 cyber loss category for law firms.

2. Client document confidentiality

If a litigation paralegal's laptop is stolen tonight, can anyone read the client documents on it?

Required answer: full-disk encryption (BitLocker on Windows, FileVault on macOS) is enforced on every firm device. Verifiable in Microsoft Endpoint Manager or equivalent. If the laptop is unencrypted, you have a potential ABA Model Rule 1.6 confidentiality breach the moment it goes missing.

3. Backup verification

When was the last time your backup system was tested by actually restoring a file, document, or mailbox — not just by reading the green status indicator?

If the answer is "we've never tested it" or "I don't know" — your backup is theoretical, not actual. Verta IT's experience: 30-40% of new client backup systems have a silent failure somewhere when first tested. Backups are only as good as the last successful restore test.

4. Privileged access controls

Who in your firm can access the firm's M365 admin console, your case management system's admin console, or your accounting software's admin login? Are those passwords stored anywhere a non-admin could find them?

If the answer involves a shared spreadsheet, a sticky note, or "everyone knows the password" — that's a privileged access compromise waiting to happen. Required: a password manager with admin-level vault, multi-factor authentication on every admin login, and a written list of who has access to what.

5. Multi-factor authentication coverage

Is multi-factor authentication (MFA) required on every business login — M365, case management, billing system, banking — for every user including the managing partner?

Specifically including the managing partner. The #1 cyber-insurance claim trigger in 2025 was BEC on an executive who had MFA disabled "because it's annoying." If MFA isn't enforced firm-wide, cyber insurance will likely pay less or nothing on a BEC claim.

6. After-hours and weekend coverage

If a ransomware attack hits your firm at 9 PM on a Saturday before a Monday court filing, who do you call? What's the response commitment?

Required answer: written incident response plan with named contacts, escalation paths, and after-hours support arrangement. Not "we'll figure it out" — that costs an extra day during the critical response window when ransomware actors are still active.

7. Vendor and software inventory

Can you list every software application your firm pays for in the last 12 months, the renewal dates, and who in the firm uses each? Are any duplicates or unused?

Most law firms over-pay for software by 15-30% because of orphaned licenses, duplicate tools, and abandoned trials. A simple inventory typically saves $200-500/user/year. If you don't have one, you're funding software no one uses.

8. Conflict-of-interest data segregation

If your firm represents both parties in a related matter (different attorneys, with an ethical wall), does your case management system technically prevent unauthorized access between the two matters?

ABA Model Rule 1.10 expects functional, not just policy-based, conflict walls. Required: case management system with role-based access controls, audit logging of who accessed what document when, and documented periodic review.

9. Email retention and discovery readiness

If served with a litigation hold or subpoena tomorrow requiring all firm email related to a specific client for the last 5 years — could your firm produce it, in defensible format, within the required timeframe?

Required: M365 retention policies configured per firm's data retention schedule, eDiscovery capability (M365 Business Premium with Purview Suite OR M365 E3/E5 with Compliance), and a documented

process for litigation hold execution. If retention isn't configured, your firm may have already deleted emails that should have been preserved.

10. Cyber insurance binder posture

Read your cyber insurance application from this year. Did your firm answer "yes" to having MFA on all accounts, endpoint detection and response (EDR) deployed, backup tested in the last 90 days, and incident response plan in place — and is each of those actually true?

Cyber insurance carriers are increasingly auditing post-claim. A "yes" on the application that doesn't match reality at the time of claim is a fraud denial. The cost of a misaligned answer can be hundreds of thousands of dollars in unreimbursed breach response.

How to use this checklist

Score honestly: - [YES] **Yes, verified** = control is in place AND recently tested - [!] **Yes, but not tested** = control exists but you haven't validated it - [NO] **No / Unknown** = gap or you don't have visibility

A score of 7+ Yes-Verified = your firm has strong IT/security posture.

A score of 4-6 = typical small/mid-sized firm. Real risk exposure exists.

A score of 0-3 = high risk profile. A managed IT partner can probably bring you to 7+ within 90 days of onboarding.

What Verta IT does about this list

Verta IT specializes in IT and security for LA law firms and CPA firms. We'll walk through this checklist with you on a no-cost 30-minute call — you get an honest read on where your firm sits, and an idea of what closing the gaps would look like. No pressure to engage. Most firms learn something useful regardless.

If you want that conversation:

George Bederyan Founder, Verta IT Solutions LLC - Email: george@vertait.com - Phone: (747) 444-0233 - Web: vertait.com

Sherman Oaks based. Serving Greater Los Angeles law firms and CPA practices.

This document is informational. It does not constitute legal advice, cyber insurance advice, or a formal IT audit. For a defensible compliance posture, engage qualified counsel for the legal and ethics questions and a qualified IT partner for the technical controls.

— Verta IT Solutions LLC · 14320 Ventura Blvd, Unit #1093, Sherman Oaks, CA 91423