ATTORNEY ARMOR · 2026 EDITION

Law Firm Cybersecurity Checklist

The 12 controls that actually stop breaches — with the evidence insurers, clients, and bar counsel will ask for. Companion to “How to Protect Your Law Firm From Hackers (2026).”

IDENTITY & EMAIL

- [ ] **1. Phishing-resistant MFA on every mailbox**
  WEEK 1
  FIDO2 security keys or passkeys for all attorneys and finance staff. Not SMS, not authenticator-app codes alone. Disable legacy/basic auth protocols (IMAP, POP, SMTP basic) in Microsoft 365.

- [ ] **2. Conditional access policies**
  WEEK 1
  Block sign-ins from outside your countries of operation, block unmanaged devices from finance/matter data, require MFA re-verification on impossible-travel detections.

- [ ] **3. Email authentication: SPF, DKIM, DMARC at enforcement**
  WEEK 2
  DMARC policy at p=reject so lookalike domains cannot spoof your firm to clients. Monitor DMARC reports monthly.

- [ ] **4. Wire-transfer callback verification**
  WEEK 1 — FREE
  Written rule: no wire instruction accepted or changed by email alone. Verbal callback to a previously known number for any new or changed instructions. Train every person who touches money movement.

DEVICES & DATA

- [ ] **5. Endpoint detection & response (EDR) on every device**
  WEEK 2
  Managed EDR — not legacy antivirus — on all laptops, desktops, and firm phones that access email or files. Someone must actually watch the alerts.

- [ ] **6. Immutable, tested backups**
  WEEK 2
  3-2-1 rule with at least one immutable/offline copy. Quarterly restore test with a written record — insurers now ask for the test evidence, not just the product name.

- [ ] **7. 72-hour patching standard for internet-facing systems**
  ONGOING
  VPNs, firewalls, remote access, website CMS/plugins patched within 72 hours of critical disclosure. Everything else within 30 days.

- [ ] **8. Full-disk encryption & screen locks on all devices**
  WEEK 2
  BitLocker/FileVault enforced via MDM; 10-minute auto-lock; remote wipe enabled for firm data on personal devices (BYOD policy in writing).

> **Why this order:** Controls 1–4 close the two paths behind most firm losses — stolen Microsoft 365 sessions and redirected wires. Everything after that hardens against ransomware and data theft.

TESTING, TRAINING & GOVERNANCE

- [ ] **9. Annual penetration test by an independent firm**
  ANNUAL
  External + internal network penetration test with a written report. Retest after major changes. This is the document cyber insurers and large clients increasingly require.

- [ ] **10. Web application testing for client portals & intake forms**
  ANNUAL
  Client portals, document upload, and intake forms are among the most-attacked law firm assets. They need application-layer testing, not just a network scan.

- [ ] **11. Security awareness training with phishing simulation**
  QUARTERLY
  Legal-specific pretexts: fake DocuSign, court e-filing notices, voicemail transcriptions, opposing-counsel document shares. Keep completion and failure records for insurance renewals.

- [ ] **12. Written incident response plan + WISP**
  WEEK 1–4
  A one-page incident response plan: who to call (breach counsel, forensics, insurer), in what order, within what hours. Plus a Written Information Security Program mapping controls to ABA Model Rule 1.6(c) and any applicable FTC/SEC/state requirements.

QUICK SELF-AUDIT

- [ ] **Do you know every system reachable from the internet under your firm's domains?**
  If not, run an external attack-surface assessment before anything else — you cannot patch what you have not found.

- [ ] **When was your last restore test, and where is the record?**
  “We have backups” is not an answer an insurer accepts anymore.

- [ ] **Could you prove, today, that MFA on partner mailboxes is phishing-resistant?**
  “We use MFA” no longer satisfies underwriters when the MFA is SMS.

> **Get your firm's baseline in about six minutes.** Run the free external security assessment at **attorneyarmor.com**, or see plans for continuous penetration testing, vulnerability assessment, and 24/7 monitoring at **attorneyarmor.com/pricing**. Questions: info@attorneyarmor.com.