2025 Texas Law Firm Cybersecurity Checklist

ABA Model Rule 1.6 & Texas Bar Compliant

As a Texas attorney, you have an ethical duty to protect client confidentiality—and that now includes your technology. The ABA and State Bar of Texas require lawyers to make *reasonable efforts* to prevent unauthorized access to client information stored electronically.

This 15-point checklist helps you evaluate whether your firm's cybersecurity measures meet current professional responsibility standards. Use it as a self-assessment tool or share it with your IT provider to identify gaps before they become problems.

Why Cybersecurity Compliance Matters for Texas Law Firms

Data breaches at law firms are increasing. According to the ABA's 2024 Legal Technology Survey, 29% of law firms reported a security breach at some point, with smaller firms often being the most vulnerable targets.

The consequences of inadequate cybersecurity extend beyond data loss:

- **Professional discipline** from the State Bar of Texas for failing to safeguard client information
- **Malpractice liability** if a breach results in harm to clients or their cases
- **Breach notification costs** under Texas Business & Commerce Code Chapter 521
- **Reputation damage** that can take years to rebuild with clients and referral sources
- **Business interruption** from ransomware or system compromises affecting case deadlines

15-Point Law Firm Cybersecurity Checklist

Instructions: Review each item and mark your current status. Items marked "No" or "Unsure" represent potential compliance gaps that should be addressed.

#	Security Requirement	Your Status
1	Multi-Factor Authentication (MFA) enabled on all email accounts, practice management software, and cloud applications	☐ Yes ☐ No ☐ Unsure
2	Client data encrypted at rest (stored files) and in transit (emails, file transfers)	☐ Yes ☐ No ☐ Unsure
3	Security awareness training provided to all attorneys and staff (minimum quarterly)	☐ Yes ☐ No ☐ Unsure
4	Written cybersecurity and acceptable use policy reviewed within the last 12 months	☐ Yes ☐ No ☐ Unsure
5	Endpoint detection and response (EDR) or managed antivirus deployed on all workstations and laptops	☐ Yes ☐ No ☐ Unsure
6	Automated daily backups with verified restore testing performed at least monthly	☐ Yes ☐ No ☐ Unsure
7	Documented incident response plan that all staff know how to activate	☐ Yes ☐ No ☐ Unsure

#	Security Requirement	Your Status
8	Access controls follow principle of least privilege (staff only access what they need)	☐ Yes ☐ No ☐ Unsure
9	Mobile device policy enforced for any personal devices accessing firm data	☐ Yes ☐ No ☐ Unsure
10	Guest WiFi network separated from the network containing client data	☐ Yes ☐ No ☐ Unsure
11	Email security with anti-phishing protection and malicious attachment scanning	☐ Yes ☐ No ☐ Unsure
12	Vendor security review completed for all cloud services storing client data	☐ Yes ☐ No ☐ Unsure
13	Secure client communication method available (encrypted email or client portal)	☐ Yes ☐ No ☐ Unsure
14	Vulnerability assessment or penetration test performed within the last 12 months	☐ Yes ☐ No ☐ Unsure
15	Cyber liability insurance policy current with coverage appropriate for your firm size	☐ Yes ☐ No ☐ Unsure

How Did You Score?

13-15 Yes responses	Strong foundation. Focus on maintaining these controls and addressing any gaps.
8-12 Yes responses	Moderate risk. Prioritize closing gaps in authentication, backup, and training.
7 or fewer Yes responses	Significant exposure. Consider a professional security assessment promptly.

Texas Bar & ABA Compliance Requirements

The requirements in this checklist are derived from the following professional responsibility rules and ethics opinions. These establish the legal framework for your firm's technology obligations.

ABA Model Rule 1.6(c) — Confidentiality of Information

"A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

This rule, adopted in 2012, explicitly requires lawyers to implement safeguards for electronic client data. "Reasonable efforts" is determined by the sensitivity of the information, the likelihood of disclosure, and the cost of additional safeguards.

ABA Formal Opinion 477R — Securing Communication of Protected Client Information

This opinion clarifies that lawyers must use reasonable efforts to ensure client communications are secure. It specifically addresses email encryption, requiring lawyers to consider the sensitivity of information when determining whether encryption is necessary. For highly sensitive matters, unencrypted email may not satisfy professional obligations.

ABA Formal Opinion 483 — Lawyers' Obligations After an Electronic Data Breach

When a data breach occurs, lawyers must: (1) stop the breach and restore systems, (2) determine what client information was accessed, (3) notify affected clients, and (4) notify law enforcement if appropriate. Having an incident response plan (Checklist Item #7) is essential for compliance.

Texas Disciplinary Rules of Professional Conduct 1.05

Texas Rule 1.05 governs confidentiality and prohibits revealing confidential client information without consent. The State Bar of Texas has made clear that this obligation extends to electronic information, requiring Texas lawyers to implement appropriate security measures.

Texas Business & Commerce Code Chapter 521

This state law requires businesses—including law firms—that own or license computerized data containing sensitive personal information to notify affected individuals following a breach. Notification must occur "as quickly as possible" after determining a breach occurred. Penalties for non-compliance can be significant.

Common Law Firm Security Vulnerabilities

Based on assessments of Dallas-Fort Worth area law firms, these are the most frequently identified security gaps:

Email Compromise

Business email compromise (BEC) remains the top threat to law firms. Attackers target trust accounts, wire transfers, and real estate closings. Without MFA and advanced email security, a single compromised credential can lead to six-figure losses.

Ransomware

Law firms are prime ransomware targets due to time-sensitive case deadlines and confidential data. Proper backups, endpoint protection, and network segmentation are essential defenses. Many firms discover their backup strategy is inadequate only after an attack.

Legacy Systems

Older practice management systems, unsupported Windows versions, and outdated network equipment create exploitable vulnerabilities. Regular technology assessments help identify systems that need updating or replacement.

Staff Training Gaps

Human error causes most security incidents. Without regular security awareness training, staff may fall for phishing emails, use weak passwords, or mishandle sensitive documents. Quarterly training significantly reduces these risks.

Next Steps for Your Firm

If your assessment revealed gaps, you're not alone. Most firms we work with have room for improvement, and addressing these issues doesn't have to be overwhelming.

Quick wins to implement this week:

- Enable MFA on Microsoft 365, practice management software, and banking portals
- Verify your backup is running successfully and test a restore
- Review who has access to sensitive client files and remove unnecessary permissions

For a comprehensive assessment: ITECS provides complimentary network and security assessments for Dallas-Fort Worth law firms. We'll evaluate your current security posture, identify vulnerabilities, and provide a prioritized remediation roadmap—with no obligation.

Schedule Your Complimentary Security Assessment

ITECS Outsourcing | Dallas-Fort Worth Law Firm IT Support

(214) 444-7884 | **itecsonline.com/law-firms**

Serving Dallas, Plano, Frisco, Fort Worth, and the DFW Metroplex for 23+ years

Local IT support means we're minutes from the George L. Allen, Sr. Courts Building, the Dallas Bar Association, and law offices throughout Uptown and Downtown Dallas.