

LEGAL

Cybersecurity for Law Firms: Essentials Guide

Protect client confidentiality, trust account funds, and your license.

Law firms hold exactly what attackers want: confidential client files, wire instructions, and access to settlement money. The duty of competence now includes technology, and clients increasingly send security questionnaires before they hire you. These are the essentials every firm should have in place.

How to use it: tick what you have in place today. Anything left unticked is a conversation worth having.

01 Protect client data

- ☐ **Encryption on every laptop, phone, and backup**
A lost unencrypted laptop can become a disclosure obligation.
- ☐ **Document management with access controls by matter**
Ethical walls should be enforced by the system, not by memory.
- ☐ **Secure client portal or encrypted email for sending documents**
Stop emailing unencrypted PDFs of financial records.
- ☐ **Retention and destruction policy that matches your engagement letters**
Keep what you must, delete what you can.
- ☐ **Vendor review for e-discovery, billing, and cloud providers**
Their breach is your problem.

02 Stop the common attacks

- ☐ **Multi-factor authentication on email, document management, and remote access**
Stolen passwords are the top way in.
- ☐ **Wire transfer verification by phone using a known number**
Business email compromise targets closings and settlements.
- ☐ **Advanced email filtering with impersonation and lookalike-domain detection**
Attackers spoof clients, courts, and opposing counsel.
- ☐ **Endpoint detection and response monitored 24/7**
Ransomware moves fast after hours.
- ☐ **Security awareness training plus phishing simulations every quarter**
Paralegals and billing staff are targeted most.
- ☐ **Separate admin accounts for IT tasks**
Nobody browses the web as an administrator.

03 Be ready to respond

- ☐ **Daily backups with one immutable or offline copy, restores tested**
Ransom demands lose leverage when you can restore.
- ☐ **Written incident response plan with breach counsel and insurer contacts**
Florida law (FIPA) requires notice to affected individuals within 30 days.
- ☐ **Cyber insurance with the controls it requires actually in place**
Misstated answers on the application can jeopardize a claim.
- ☐ **Remote work standards for home networks and personal devices**
Court-from-home created new gaps.
- ☐ **Annual security assessment with written findings**
Useful evidence when clients send questionnaires.

Red flags we see most

- Wire instructions are confirmed by replying to the email.
- Partners are exempt from multi-factor authentication.
- Former associates still have document access.
- You cannot answer a client security questionnaire without guessing.

Where to start

Implement a call-back rule for every payment or wire change. It is free, takes a day to roll out, and stops the most expensive attack firms face.

Want a second set of eyes?

Book a free 30-minute IT assessment. A senior technician walks through this checklist with you and tells you what to fix first. No sales script, no obligation.

Book a free assessment

(813) 999-0086

swfit.io/free-consultation