



Your firm already runs on *confidentiality*. Now it runs on *security*, too.

Protecting a client's information today means protecting the systems that hold it — and the rules of professional conduct expect lawyers to understand the technology they rely on. The good news: **you don't need a full-time security executive to meet that bar**. You need senior judgment, on a schedule and budget that fit a firm your size. That's what a fractional Chief Information Security Officer (CISO) provides — security leadership by the day, not the year.

A CISO and your IT provider do different jobs

BETTER TOGETHER

We don't replace your IT company or compete with them — we set the direction and own the risk, which makes their work more effective.

YOUR IT / MANAGED-SERVICES PROVIDER

Keeps the technology running

- Help desk and day-to-day support
- Networks, devices, email, and Wi-Fi
- Software updates and patching
- Backups and antivirus tools
- Onboarding new attorneys and staff

The hands on the keyboard — keeping the lights on.

YOUR FRACTIONAL CISO

Owns the strategy, risk & accountability

- Defines what "secure enough" means for your firm and clients
- Aligns you with ethics duties, client requirements & cyber insurance
- Vets the outside vendors who touch client data
- Builds the policies and the incident plan
- Reports to the partners in plain business terms

The judgment and accountability — deciding what good looks like.

Think of it as the difference between the team that **maintains the building** and the person responsible for **deciding it's safe to occupy**. Your IT provider keeps the systems healthy; we make sure the right systems, rules, and habits are in place — and that someone senior is accountable for them.

Most incidents start with a person, not a server

YOUR END-USERS

The biggest risk at a law firm usually isn't exotic hacking — it's an ordinary email on a busy day. A paralegal opens a fake invoice. An attorney approves a wire to a spoofed account during a closing. A password gets reused across sites. None of this means your people are careless; it means they're human, and these attacks are built to look completely normal. We focus on the human layer with practical, plain-English training and simple guardrails — multi-factor logins, wire-verification steps, and clear "who to call" habits — so a single honest mistake never turns into a client crisis.

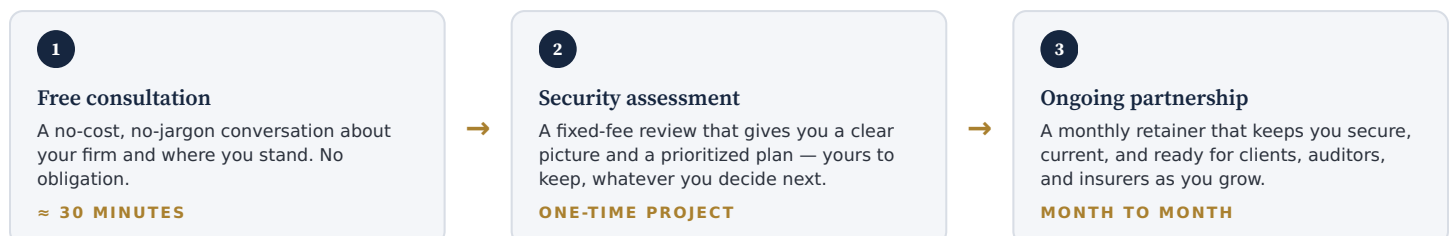
What we handle for you

FIVE FOCUS AREAS

1	Risk Assessment & Roadmap	A plain-language baseline of where your firm stands today, with a prioritized, budget-aware plan you own. Your starting point.
2	Confidentiality & Compliance	Aligning your safeguards with your ethical duties, client security requirements (including outside-counsel guidelines), and your cyber-insurance application.
3	Vendor & Cloud Risk	Vetting the e-discovery, practice-management, and cloud tools that hold client data — so their weaknesses don't quietly become yours.
4	Policy & Governance	The written policies, sensible rules, and partner-level reporting that turn good intentions into a program you can defend.
5	Incident Readiness	A simple, tested plan for "what do we do if...", plus a walkthrough with your team, so a bad day stays contained and short.

How we start — simple and low-risk

THREE STEPS



Led by a security executive with 20+ years as a corporate CISO — holding the Certified Information Security Manager (CISM) and Certified Chief Information Security Officer (CCISO) credentials. **Independent by design:** we sell judgment, never products, and take no commissions on any tool or vendor we recommend. Our only job is what's right for your firm.

Protect your practice. Enable your growth.

Senior cybersecurity leadership, right-sized for your firm.

Book your free consultation

fracciso.com