A Reference Guide For Practice Leaders

The IT Decisions That Protect the Practice

How Partners and CEOs at Law, Accounting, and Healthcare Firms Make Technology Decisions That Hold Up Under Pressure

How to Use This Guide

This is not a checklist to read once and file away. It is written to sit on a shelf, or more realistically in a browser tab, and get opened again whenever a technology decision lands on your desk: a vendor pitch, a renewal notice, an incident, or a partner meeting where someone asks whether the firm is "covered."

Each chapter stands on its own, so you can jump straight to the section that matches the decision in front of you. The guide is organized around the questions a managing partner, CEO, or practice owner actually has to answer, not around the technology itself. You will not find product recommendations here. You will find the reasoning a good advisor would walk you through before you sign anything, hire anyone, or sign off on a budget.

It draws on patterns seen across professional service firms, the kind of firms that carry other people's confidential information as a condition of doing business and that get judged not by their intentions but by what happens when something goes wrong.

Chapter 1: Why This Guide Exists

Law firms, accounting practices, and healthcare providers share something that most businesses do not: the information they hold is not really theirs. A client's litigation strategy, a patient's diagnosis, and a taxpayer's financial history - all of it is held in trust, all of it is held in trust, under a duty that predates any firewall and does not care how it was breached.

That changes what an IT decision actually is. In most industries, a slow server or a missed software update is an inconvenience. In yours, the same failure can become a breach of confidentiality, a violation of a regulatory rule, a malpractice claim, or a call you have to make to every affected client explaining what happened and why it took three weeks to notice.

And yet very few partners were trained to evaluate any of this. Law school teaches the duty of confidentiality. It does not teach how to tell a competent IT provider from one that is quietly cutting corners. The same is true in accounting and in medicine. The people ultimately accountable for the firm's technology risk are usually the least equipped, by training, to interrogate it and the most exposed when it fails.

This guide exists to close that gap without turning you into an IT person. You do not need to understand how a firewall works. You need to know what questions separate a firm that is actually protected from one that only feels protected, and you need a framework for making that call quickly when a decision is in front of you.

> The goal is not to make you technical. It is to make you dangerous to talk to for a vendor who is hoping you won't ask the right question.

Chapter 2: The Real Cost of Getting IT Wrong

Partners tend to think about IT failure as an operational problem: the system goes down, people are annoyed, work gets delayed. That is the version that is easiest to imagine, and it is the least of it.

Downtime is the cheapest failure mode

A day without email or practice management software is a bad day, but it is recoverable. Staff go home, backlogs clear, and within a week nobody outside the firm remembers it happened. This is the failure mode most partners budget for, if they budget for any of it, and it is the one that matters least.

Breach cost is a different category entirely

A ransomware event or unauthorized access to client, patient, or taxpayer data triggers obligations that have nothing to do with how quickly systems come back online. Depending on jurisdiction and the type of data involved, this can mean mandatory breach notification to every affected individual, regulatory reporting, forensic investigation costs, credit monitoring obligations, and in healthcare, direct exposure under HIPAA's enforcement provisions. None of that is optional once triggered, and none of it is fast.

Liability follows the professional, not the vendor

If a firm's IT provider fails to patch a known vulnerability and client data is exposed as a result, the client's recourse runs first through the firm they hired, not through a vendor they never signed an engagement letter with. The duty of confidentiality and the duty of competence sit with the partner. Outsourcing the technology does not outsource the obligation.

Cyber insurance is no longer a backstop you can assume

Insurers have tightened underwriting significantly. Policies increasingly require documented multi-factor authentication, endpoint detection and response, and tested backups as a condition of coverage, not just a discount. Firms that cannot demonstrate these controls at renewal are seeing higher premiums, reduced coverage, or denied claims after an incident because a required control was not actually in place. The insurance you think you have and the insurance you actually have can be two different things, and you usually find out which one applies at the worst possible moment.

Reputational cost is the one partners underestimate most

A breach notification letter to clients is not just a compliance exercise. In professions built entirely on trust, it is a direct hit to the reason clients hired you in the first place. Referral relationships, in particular, are unforgiving of this kind of failure.

None of this is meant to be alarmist. It is meant to establish the actual stakes, because every decision in the chapters that follow only makes sense against this backdrop. A slightly more expensive IT provider that can demonstrate real controls is not a luxury. It is underwriting your own risk.

Chapter 3: Cybersecurity Fundamentals in Plain English

You do not need to become technical to make good decisions here. You need working knowledge of a handful of concepts, enough to recognize whether a provider or an internal setup is actually addressing them.

Most breaches start with a person, not a system

The overwhelming majority of successful attacks begin with phishing: a convincing email that tricks someone into clicking a link, entering credentials, or approving a fraudulent request. Firewalls and antivirus software do very little against this, because the attacker is not breaking in through the network; they are being let in through a person. Any security program that does not include ongoing staff training and simulated phishing testing is addressing the smaller half of the problem.

MFA requires a second form of verification beyond a password, typically a code from a phone or an approval tap. It will not stop every attack, but it stops the overwhelming majority of account takeover attempts, because a stolen password alone is no longer enough to get in. If a vendor or provider cannot confirm MFA is enforced everywhere, email, remote access, and financial systems included, this is the first thing to fix, before anything else on this list.

Multi-factor authentication is the single highest-leverage control available

Antivirus and EDR are not the same thing

Traditional antivirus looks for known malicious files by comparing them against a list of known threats. It is effectively useless against new or customized attacks, which describes most serious ones today. Endpoint Detection and Response (EDR) instead watches for suspicious behavior, such as an application encrypting ffiles rapidly or a process trying to disable security tools, and can isolate a compromised machine automatically before an attack spreads. If your provider is still describing your protection as “antivirus,” ask directly whether you have EDR, and get the answer in writing.

Software vendors release updates constantly, many of them closing security holes that are publicly known and actively being exploited within days of disclosure. A firm running months behind on updates is not "behind schedule"; it is running with known, documented holes in its defenses. Ask how patching is handled and how quickly critical updates are applied, not just whether it happens.

Patching is unglamorous and it is where most preventable breaches happen

Backups only count if they have been tested

A backup that has never been restored is a hypothesis, not a safeguard. The standard worth asking for is the "3-2-1" approach: three copies of data, on two different types of media, with one copy stored off-site or offline, isolated from the systems it is protecting. Beyond that, ask when the last test restore happened and ask to see the result. Many firms discover their backups were incomplete or corrupted only after they needed them, which is the worst possible time to find out.

Taken together, these five items, staff awareness, MFA, real endpoint protection, disciplined patching, and tested backups, represent the bulk of what separates a firm that survives an attempted attack from one that becomes a headline. Everything more advanced is refinement on top of this foundation.

Chapter 4: Compliance Obligations by Profession

Every profession covered in this guide operates under a distinct regulatory and ethical framework governing how client, patient, or taxpayer information must be handled. Your IT setup either supports these obligations or quietly undermines them. This chapter is not legal advice, and none of it substitutes for counsel from your bar association, state board, or compliance officer, but it will tell you what to ask about.

Law Firms

The ABA Model Rules of Professional Conduct establish two obligations that bear directly on technology. Rule 1.6 requires reasonable efforts to prevent unauthorized disclosure of client information, a standard that has been interpreted by state bar ethics opinions to include encryption, access controls, and secure handling of electronic communications. Rule 1.1, competence, was amended by comment to explicitly include understanding the risks and benefits of the technology a lawyer uses. Ignorance of your own systems is no longer a defense; it may itself be the ethics violation.

Practically, this means client data (documents, email, case files) needs access controls limiting who can see what, encryption for data at rest and in transit, and a defensible answer for how client confidentiality is maintained when using cloud storage, e-discovery platforms, or remote work setups. Check your specific state bar's ethics opinions on cloud computing and encryption, since standards vary by jurisdiction.

Accounting Firms

IRS Publication 4557, Safeguarding Taxpayer Data, sets expectations for any preparer handling federal tax information, and non-compliance can affect a firm's ability to participate in e-filing programs. The Gramm-Leach-Bliley Act's Safeguards Rule applies to firms providing financial services, which the FTC has interpreted to include tax preparation and accounting services in many circumstances, requiring a written information security plan, not just informal practices.

If the firm processes card payments for client billing, PCI-DSS requirements layer on top of this. The common thread across all three: documentation matters as much as the underlying controls. A firm that has good security practices but no written information security plan is still out of compliance with the Safeguards Rule on paper, which is exactly where a regulator or a plaintiff's attorney will look first.

Healthcare Practices

HIPAA's Security Rule requires administrative, physical, and technical safeguards for electronic protected health information (ePHI), and the HITECH Act layers on mandatory breach notification requirements with tight timelines once a breach is discovered. Any IT vendor with access to systems containing ePHI, including your MSP, must sign a Business Associate Agreement (BAA) accepting their own compliance obligations under HIPAA. A provider that hesitates to sign a BAA or does not know what one is, is disqualifying itself from working with a healthcare practice regardless of price.

Annual HIPAA risk assessments are a requirement, not a best practice, and "we've never had a breach" is not evidence of compliance. Enforcement actions have repeatedly targeted practices that had no documented risk assessment at all, independent of whether a breach occurred.

Chapter 5: Evaluating and Managing IT Vendors

Most partners choose an IT provider the way they choose a plumber: on responsiveness, price, and a decent first impression. That is a reasonable way to pick a plumber. It is not a reasonable way to pick the entity responsible for protecting the firm's confidentiality obligations.

Questions worth asking before signing anything

- What is your average response time for a critical issue, and is that a guarantee in the contract or an aspiration in the sales deck?
- Do you enforce MFA and EDR across every client environment as a default, or is it an optional add-on?
- How often do you actually test backup restores, and can you show documentation of the last one?
- Do you carry your own cyber liability insurance, and what does it cover if your negligence causes our breach?
- Who owns our data, credentials, and documentation if we terminate the relationship, and how quickly can we get them?
- Is our environment supported by a team, or does critical knowledge live in one person's head?
- Will you sign a Business Associate Agreement or equivalent, and have you done so before?

Red flags

A provider that cannot answer these questions specifically, that hedges with generalities, or that seems mildly offended to be asked, is telling you something important. So is a provider still operating on a purely reactive, break-fix model, where they get paid more when things go wrong? That model has no financial incentive to prevent problems, only to resolve them, and the incentive structure will show up eventually in how proactive your protection actually is.

Understand what you're actually buying

Managed services and break-fix support are fundamentally different arrangements, not points on the same spectrum. Managed services is generally a flat-fee relationship where the provider is financially incentivized to prevent problems, because more incidents cost them money, not you. Break-fix bills by the hour when something breaks, which means the provider's revenue is tied to your failures. Know which one you are buying, because the sales conversation often blurs the line.

The exit clause matters more than the onboarding pitch

Ask, before signing, exactly what happens if the relationship ends: how quickly you get full administrative access to your own systems back, whether documentation is handed over, and whether there are any contractual barriers to leaving. A provider confident in the value they deliver will not need to trap you into staying.

Chapter 6: Business Continuity and Disaster Recovery

Every firm has some version of a backup. Far fewer have a tested plan for what actually happens in the hours after a serious incident, and that gap is where most of the damage occurs.

Two numbers worth understanding

Recovery Time Objective (RTO) is how long the firm can tolerate being down before the disruption becomes unacceptable. Recovery Point Objective (RPO) is how much data the firm can afford to lose, measured in time: if backups run nightly, an incident at 4pm means everything since last night's backup is gone. Neither number should be decided by the IT provider in isolation. They are business decisions a partner should set explicitly, because they determine how much redundancy, and cost, is actually justified.

What the first hour of a ransomware event actually looks like

Systems lock up or display a ransom note. Nobody is certain yet how far the compromise has spread. The instinct is to start troubleshooting immediately, which is often the wrong move, because it can destroy forensic evidence and give an active attacker more time inside the network. A documented incident response plan should specify, in advance, who has authority to make the call to isolate systems, who contacts insurance and legal counsel, who contacts law enforcement, and who is responsible for client or patient communication if a notification becomes necessary. Deciding this in the moment, under pressure, with people who have never rehearsed it, is how a bad day becomes a bad month.

Tabletop exercises are worth the two hours they cost

A tabletop exercise is a walkthrough, not a live drill: the partners and key staff sit down and talk through a hypothetical incident step by step, confirming who does what. It routinely surfaces gaps that look fine on paper, an insurance policy nobody has actually read, a client notification process nobody has actually drafted, before they matter in a real event. Once a year is a reasonable cadence for most firms this size.

Chapter 7: Budgeting for IT Without Overspending or Underspending

There are two ways to get IT budgeting wrong, and professional service firms manage to hit both, sometimes in the same year.

Underinvestment hides its true cost

A firm paying a bargain rate for reactive, break-fix support looks like it is saving money on a monthly comparison. It rarely is, once you account for the cumulative cost of downtime, the security gaps that go unaddressed because nobody is proactively managing them, and the eventual cost of an incident that better-configured systems would have prevented. The cheapest provider on paper is frequently the most expensive one over three years; it just spreads the cost across incidents instead of a predictable invoice.

A more useful framing than a flat percentage

Generic benchmarks ("spend X percent of revenue on IT") are a weak starting point because they ignore what the firm actually holds and what obligations apply to it. A more useful exercise: estimate the realistic cost of your firm's worst plausible incident, notification costs, downtime, regulatory exposure, and reputational damage, and use that number to sanity-check whether your current spend is proportionate. A firm that would face six figures in exposure from a single breach and is paying a few hundred dollars a month for IT support has a mismatch worth examining, regardless of what percentage that represents.

Ask for the total cost, not the line-item cost

A quote that looks lower often excludes items a more thorough proposal includes by default: backup testing, security awareness training, after-hours incident response, cyber insurance documentation support. Compare total scope, not just the monthly number at the bottom of the page.

Chapter 8: Building an IT Governance Rhythm

The firms that handle technology well are not the ones with the most advanced tools. They are the ones that treat IT as a standing item of governance, reviewed on a regular cadence, rather than a topic that only comes up when something breaks.

Quarterly business reviews

A recurring structured conversation with your IT provider, not a sales call, a genuine review: what changed this quarter, what risks were identified, what was remediated, what is still open, and what is coming next. If your current provider has never proposed this, that is worth noting on its own.

Annual risk assessments

Beyond whatever your industry requires (HIPAA risk assessments are mandatory annually for healthcare, for instance), a broader review of the firm's technology risk posture once a year gives partners a documented basis for decisions and a paper trail that matters if a regulator or insurer ever asks what due diligence was performed.

Make it a standing agenda item, not a fire drill

Firms that only discuss IT reactively, after an outage or a scare, end up making decisions under pressure, which tends to produce worse decisions and higher prices. A firm that reviews its technology posture on a fixed schedule, even briefly, catches problems while they are still cheap to fix.

Chapter 9: The Decision Framework and Self-Assessment Scorecard

Use this scorecard periodically, ideally alongside your IT provider or a knowledgeable outside advisor, to get an honest read on where the firm actually stands. Score each item from 1 (not in place) to 5 (fully in place and tested). Be honest rather than optimistic; the value of this tool is entirely in its accuracy.

	1	2	3	4	5
Multi-factor authentication is enforced on all email, remote access, and financial systems	☐	☐	☐	☐	☐
Endpoint detection and response (not just antivirus) is deployed on all devices	☐	☐	☐	☐	☐
Backups follow the 3-2-1 approach, and restores are tested on a documented schedule	☐	☐	☐	☐	☐
Staff receive ongoing phishing awareness training, not a one-time onboarding video	☐	☐	☐	☐	☐
Critical software patches are applied within days, not months, of release	☐	☐	☐	☐	☐
A written incident response plan exists and has been reviewed in the last 12 months	☐	☐	☐	☐	☐
A tabletop exercise has been run in the last 12 months	☐	☐	☐	☐	☐
Our IT provider has signed a BAA or equivalent data protection agreement where required	☐	☐	☐	☐	☐
We know our cyber insurance policy's specific requirements and can demonstrate we meet them	☐	☐	☐	☐	☐
IT is a standing item in partner or leadership meetings, not an as-needed topic	☐	☐	☐	☐	☐
We have documented ownership of, and admin access to, our own data and credentials	☐	☐	☐	☐	☐
An annual risk assessment has been completed and documented	☐	☐	☐	☐	☐

A total score below 36 suggests real, addressable gaps. A score above 50 suggests a firm is in a reasonably strong position, though that position is still worth revisiting annually, since both the threat landscape and the firm itself keep changing.

Appendix A: Industry Quick Reference

	Key Obligations	Watch For
Law	ABA Model Rules 1.1 & 1.6; state bar ethics opinions on cloud computing and encryption	Unencrypted client email; vendors unfamiliar with e-discovery data handling
Accounting	IRS Pub. 4557; GLBA Safeguards Rule; PCI-DSS if processing card payments	No written information security plan; informal practices with no documentation
Healthcare	HIPAA Security Rule; HITECH breach notification; mandatory annual risk assessments	Vendors unwilling or unable to sign a Business Associate Agreement

Appendix B: Glossary

MFA (Multi-Factor Authentication)

A login process requiring a second form of verification beyond a password, such as a code sent to a phone.

EDR (Endpoint Detection and Response)

Security software that monitors devices for suspicious behavior and can isolate a compromised machine automatically, as opposed to traditional antivirus, which only recognizes known threats.

RTO (Recovery Time Objective)

The maximum acceptable length of time systems can be down before the disruption becomes unacceptable to the business.

RPO (Recovery Point Objective)

The maximum acceptable amount of data loss, measured in time, based on how frequently backups are taken.

3-2-1 Backup Rule

A backup standard calling for three copies of data, on two different types of media, with one copy stored off-site or offline.

BAA (Business Associate Agreement)

A contract required under HIPAA between a healthcare provider and any vendor that may access protected health information, obligating the vendor to its own compliance responsibilities.

Break-fix

An IT support model billed by the hour when something breaks, as opposed to managed services, which is typically a flat fee covering ongoing proactive support.

Managed Services

An IT support model, usually flat-fee, where the provider is financially incentivized to prevent problems rather than bill for fixing them.

Tabletop Exercise

A structured discussion-based walkthrough of a hypothetical incident, used to test and refine a response plan without a live disruption.

Patch Management

The process of applying software updates, particularly security updates, in a timely and disciplined way.

A Closing Note

None of this requires becoming a technologist. It requires treating technology decisions with the same rigor you already bring to every other obligation the firm carries, because that is what they are: obligations, not just line items.

This guide was put together by MetroTech, a managed IT provider based in the Tampa Bay area that works specifically with law firms and other professional service businesses navigating exactly these decisions. If it raised questions specific to your firm, that conversation is a natural next step, no pitch required to have it.

MetroTech

727-230-0332

mettec.net