Lawyers

Tech mistakes **law firms can't afford to ignore**

nexGen TECHNOLOGY SERVICES

www.nexgen.tech

Running a law firm today means juggling clients, deadlines, compliance, staff, and a constant stream of urgent work.

Technology is supposed to make all that easier.

Yet for many firms, it feels like the opposite.

Computers slowing down at the worst possible moment, email systems that behave unpredictably, software no one really understands… and security worries that never quite go away.

Law firm owners don't choose their profession because they love technology. But ignoring the systems that keep your practice running is not an option.

Threats are increasing, clients expect more, and your state regulatory board assume you've done the basics to keep data safe.

Fortunately, good IT doesn't mean buying the most expensive systems or replacing everything at once. You need to get the fundamentals right to keep your firm secure, make sure your team can work efficiently wherever they are, and have sensible protections in place so a bad day doesn't turn into a disaster.

Why technology sits at the heart of your firm

Legal work has changed.

It's no longer something that only happens in a fixed office, on a handful of desktop PCs.

Lawyers work from home, from court, from client sites, and sometimes from the car between meetings. Files are opened on laptops, phones and tablets, at all hours.

That flexibility is valuable, but it only works if your systems keep up.

Older setups were built for a world where people were mostly in the office, on the office network.

When you stretch those systems to cover remote work, you often end up with slow remote access, clunky workarounds, and shortcuts that quietly create risk.

People email documents to their personal accounts "just this once", use unapproved apps to send files, or store things locally on devices that aren't properly protected.

At the same time, cybercrime has moved from being a background worry to a daily reality.

Cybercriminals actively target professional services firms because they know you hold sensitive information, manage funds, and often work to tight deadlines.

To an attacker, a law firm with weak security is a perfect combination of valuable data and urgency.

On top of this, your reputation rests on trust. Clients assume you will keep their information safe.

A single breach (whether it's a hacked email account, leaked documents, or a ransomware attack) can undo years of careful reputation building.

It doesn't matter whether you're a three-person practice or a national firm. From the outside, a breach is a breach.

So, the question isn't ***"Do we need to think about technology?"***

It's ***"Are we doing enough to make it work for us, instead of against us?"***

Getting clear on your core systems

You don't need to know how to build systems or configure servers. But it does help to have a clear, simple picture of the main moving parts behind your IT.

Most firms have some mix of these core components…

Somewhere that your files and applications live

For some firms, that's still a server in a cupboard or small server room. It stores your documents, runs your case management system, and quietly does its job in the background.

When it's looked after properly, this can work well. But it does mean somebody is responsible for checking it, updating it, and eventually replacing it.

Other firms use cloud systems instead. In practical terms, they're doing the same job, storing files, running applications, providing access, just somewhere else.

Instead of owning the hardware yourself, you're renting space on professionally managed equipment. You connect to it over the internet and someone else takes care of the maintenance and hardware failures.

Neither approach is automatically right or wrong. What matters is that you understand which one you're using, what it can and can't do, and who is looking after it.

Case management software

Lawyers interact with this all day long, but usually only see the front end: Matter screens, contacts, notes, time entries.

Behind the scenes, it's doing a lot of organization for you. It ties documents, emails, key dates and tasks together so your team can see a complete picture of each matter.

When it's set up well, it stops people hunting through shared drives wondering where someone saved a file.

Where things often go wrong is not in the software itself, but in how little of it is used.

Firms pay for powerful systems and then only use a small fraction of the features, falling back on manual workarounds and spreadsheets. That creates duplication, inconsistency and more admin than necessary.

Email
For most firms it's still the main way work arrives and conversations happen.

Modern email platforms can do far more than send and receive messages. They can help keep data organized, reduce mistakes, and integrate with your case management and document systems.

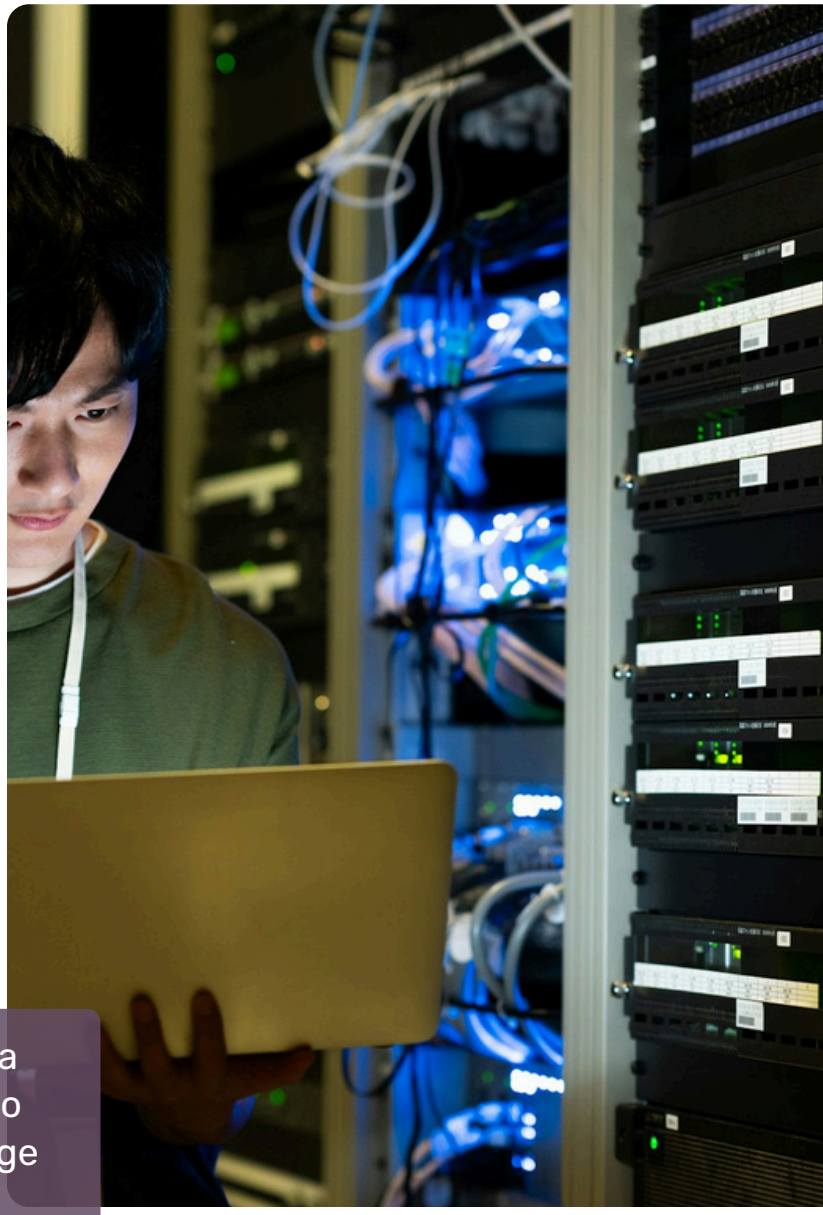
When those links are set up properly, your staff spend less time copying, pasting and filing, and more time doing legal work.

Wi-Fi
Poorly planned networks lead to slow systems, dropped calls and frustration.

Good Wi-Fi design supports your software, keeps traffic flowing, and helps separate staff devices from guest access so you're not accidentally exposing systems you want to protect.

The cloud
The cloud is a secure, professionally managed place to store and run your systems, which you access via the internet.

It doesn't mean you lose control of your data. When used properly, it often makes things simpler, more flexible and more resilient.



Understanding these components at a high level gives you enough context to ask sensible questions and to challenge decisions that don't feel right.

Getting the basics of cybersecurity right

Cybersecurity can feel intimidating. But most of the protection you need as a law firm comes from doing a handful of things consistently well.

The first is controlling who can see what.

That starts with good authentication. Strong passwords, backed up by multi-factor authentication (MFA). MFA means that logging in needs not just a password, but also a second proof - often a code or prompt on a phone.

If someone steals or guesses a password, they still can't get into your systems without that second factor. It's a small inconvenience for staff, but it blocks a huge number of common attacks.

Encryption is another important building block. It's a way of scrambling information so that if someone gets hold of a device or intercepts data, they can't read it.

Modern systems can encrypt laptops, phones and stored files so that if a device is lost or stolen, your client information isn't exposed. It's often available but not always switched on or properly configured.

Firewalls and web filtering quietly protect you in the background.

A firewall acts like a gatekeeper between your network and the internet, checking traffic and blocking anything suspicious.

Web filtering stops staff being able to visit known dangerous sites or fake login pages, even if they click on a bad link.

Staff still need training and awareness, but these tools give you a safety net. Device security matters just as much as what happens on the server or in the cloud.

Work now happens across laptops, phones and tablets, often on the move. Those devices should be kept up to date, protected with passwords or biometrics, encrypted, and monitored by your IT support partner.

Allowing staff to use personal devices for convenience, without proper controls, is a common way for data to end up in places it shouldn't.

Then there's phishing. The tried-and-tested method attackers use to trick people via email.

These messages might look like delivery notifications, bank alerts, shared document links or urgent requests that seem to come from colleagues. The goal is always the same: Get someone to click, enter login details, or open a dangerous attachment.

Training staff to pause, check and ask before acting on anything that feels the slightest bit off is one of the cheapest and most effective defenses you can put in place.

None of these measures are particularly glamorous. But together, they create a strong shield around your firm's data.

Treating data protection as part of daily practice

Data protection shows up in small, everyday decisions about where you store things, who has access, and how long information is kept.

One of the simplest and most important ideas is access control.

Not everyone needs to see everything. If you deliberately limit access so that people only see what they need for their role, you automatically reduce the damage that can be done by a mistake, a hacked account or a disgruntled employee.

Retention is another area where many firms quietly drift into risk.
Old matters are kept “just in case” for far longer than needed. Over time, that builds a larger pool of data that could be exposed if something goes wrong.

Clear rules about how long you keep different types of information, and a process to delete or archive it, keep your footprint sensible.

Where you store data matters too.

Firm documents should live in secure, approved systems. Not scattered across personal email accounts, USB sticks, or unsupervised cloud folders. As soon as data leaves the systems

your IT support partner can monitor and protect, you lose visibility and control.

When something does go wrong (and eventually, something will) it’s far better to have thought ahead.

An incident response plan doesn’t need to be complicated. It can simply set out who is responsible for what, what gets done first, who is informed, and how decisions are recorded.

The aim is to avoid panic and guesswork at the worst possible moment.

Documentation underpins all of this. When you write down how things should be done, and keep those notes up to date, you make it easier for people to act consistently.

New staff understand expectations faster, and if your state regulatory board or clients ever ask how you protect data, you have something concrete to point to.

Using email, documents and file sharing safely

Most of the day's work flows through email and document systems.

That's why many incidents start there. Not because the tools are bad, but because they are used for almost everything.

One common mistake is treating email as the answer to every situation. It becomes the way to send documents, share drafts, get approvals, send confidential updates and trade sensitive information.

The more you use it for, the more likely it is that something goes wrong. An attachment goes to the wrong person, a draft is sent instead of the final version, or a long email thread contains more than the recipient should see.

Safer alternatives exist and are widely available.

Secure client portals, or secure messaging features built into your practice management system, allow clients to log into a protected area to view documents and updates. Information stays in one place, access can be controlled, and documents aren't constantly being copied and forwarded.

Good document management also means knowing which version is the right one.

When files live in inboxes, desktop folders and shared drives all at once, it's easy to send something out using the wrong draft.

Systems that keep a single master copy with a clear history of changes solve this problem and quietly prevent a lot of confusion.

Consumer messaging apps, like chat tools designed for personal use, are another area where firms slip up.

They're attractive because they're quick and familiar, and clients often suggest them. But they're not designed for legal confidentiality, record-keeping or controlled access.

Messages may be backed up to personal cloud accounts, phones may be shared with family members, and there is no central way for the firm to retain or review the conversation.

It's far safer to politely steer clients towards approved tools that you can manage properly.

Finally, many data leaks are simply human mistakes. The wrong recipient chosen from an autocomplete list, a file saved to a personal device "for convenience", an old email forwarded without noticing what's lower down the thread.

Sensible systems, gentle warnings, and a culture that encourages people to slow down and double-check go a long way here.

Choosing where your systems live

A frequent question for law firm owners is whether systems should live on servers in the office, in the cloud, or a mixture of the two.

Running your own server gives you a tangible asset and a sense of control. But it comes with responsibility.

You need to budget for replacements, power and cooling, monitoring, backup solutions, and someone to keep everything updated and healthy.

When it works, it can be fast and reliable.

When it isn't maintained properly, problems often appear suddenly and at the worst times.

Cloud systems swap that capital expense for a subscription model. You pay monthly to use infrastructure that someone else maintains. Capacity can usually scale up or down more easily as your firm grows or changes.

For teams that work across locations or rely heavily on remote access, the cloud's "anywhere" functionality feels natural.

In terms of security, both approaches can be safe or unsafe. It depends on how they're set up and maintained.

Cloud providers invest heavily in physical security, redundancy and monitoring that most individual firms simply couldn't replicate on their own.

Local servers can be highly secure too, but only if someone is actively taking care of them.

Whatever you choose, one principle remains the same: You must not assume that the system will take care of everything by itself. Backups, updates and monitoring still need to be planned and checked.

Planning for bad days

Nobody likes thinking about things going wrong, but it's far less painful to plan ahead than to improvise during a crisis.

A backup is an extra copy of your data, stored somewhere safe, that you can restore if needed.

If there is only one copy of a document, on a laptop, on a server, or even in a cloud system, it isn't really protected. Hardware can fail. Files can be deleted. Accounts can be compromised.

A simple way to think about backup is the 3-2-1 idea. Have **three** copies of your data, on **two** different types of storage, with **one** copy kept off-site.

That might mean your main system, a secondary backup device in the office, and a further backup in the cloud. The point is to avoid a single point of failure.

Ransomware brings this into sharp focus.

When ransomware hits, it locks your files and demands payment to unlock them. If you have recent, clean backups that haven't been touched by the malware, you can erase the infected systems and restore your data.

Firms that end up paying are often those whose backups weren't working, weren't recent, or were stored on the same systems that got infected.

But backups only solve part of the problem.

They protect your data, but not your ability to keep working while things are broken.

That's where business continuity comes in.

Continuity planning answers questions like: ***"If our main system went down today, how would we keep serving clients?" and "How quickly do we need to be back online before it starts causing serious damage?"***

There isn't a single right answer.

Some firms can cope with a day's interruption. Others can't.

The important thing is to decide your own tolerance for downtime and data loss and then make sure your backup and continuity setup matches that.

Using technology to save time, not just avoid risk

So far, much of this has focused on stopping bad things from happening. But technology should do more than protect. It should make your life easier.

Many legal processes follow predictable patterns. New matters are opened in similar ways. Clients receive similar updates at certain stages. The same types of documents are drafted repeatedly.

When these steps are handled manually, they eat up a lot of time and create opportunities for errors or missed steps.

Workflow automation allows your systems to take care of the repetitive parts. Opening a matter can automatically create the right folders, tasks and initial documents. Reaching a particular stage in a case can automatically trigger a client update.

Staff still use their judgment and expertise, but they're no longer bogged down in avoidable admin.

Templates are another powerful but often underused tool.

Standardizing engagement letters, common forms, recurring clauses and standard communications means people aren't constantly reinventing the wheel.

It also keeps your branding and tone consistent and reduces the chance of someone using an out-of-date version.

Newer tools like AI assistants can help with summarizing long documents, suggesting wording for routine correspondence, and surfacing relevant information faster.

Used inside secure, controlled systems and with clear rules about what they're allowed to see, they can be useful "junior helpers", speeding up tasks without making legal decisions.

Smart search tools can index your documents and emails so staff can find what they need quickly, rather than scrolling through long lists of files or digging through inboxes.

Remote collaboration tools and e-signature platforms can remove delays caused by geography, printing and scanning.

Voice dictation is another simple win. Many lawyers think and speak faster than they type. Being able to dictate notes or draft content and have it converted to text can be a real productivity boost, especially for busy fee earners.

None of these tools are there to replace people. They're there to free them from low-value admin so they can focus on work that genuinely requires their expertise.

Controlling devices and access

As your firm grows and people come and go, it becomes harder to keep track of who has access to what, and on which devices.

Mobile Device Management (MDM) systems give your IT support partner a central view of all the phones, tablets and laptops that connect to your systems.

They can make sure security updates are applied, enforce encryption, and remotely lock or wipe a device if it goes missing.

This is especially important if staff use their own devices for work. Without MDM, firm data can end up mixed into personal apps and storage with no easy way to remove it.

On the access side, the safest approach is to give people the minimum permissions they need to do their job well.

Over time, access tends to grow "just in case". If nobody ever reviews it, you end up with staff who can see far more than they should, and with old accounts that were never properly closed when someone left.

Off boarding is critical too.

When a person leaves the firm, their accounts should be disabled promptly, their company-owned devices collected or securely wiped, and any shared passwords changed.

Leaving accounts active "for now" because they might be useful later is an easy way to create hidden vulnerabilities.

Regularly reviewing accounts and permissions is one of the simplest ways to cut risk. If an account doesn't have a clear owner or purpose, it's better to remove it than leave it quietly sitting there.

Working with the right IT partner

Even the best designed systems will occasionally have problems. What matters is how they're managed.

And that largely depends on the IT support partner you work with.

Good IT support is proactive.

Instead of waiting for things to break, they look for early warning signs and fix issues before they interrupt your day.

They keep your systems updated, monitor key services, and talk to you about improvements rather than just reacting to emergencies.

They also make sure your systems and data security meet the standards set out by your state regulatory board.

You don't need technical knowledge to judge whether your IT support partner is doing a good job. Ask yourself a few simple questions:

- Do they explain things in plain language?
- Do they understand how a law firm works, not just how computers work?
- Do they talk to you about planning and improvements, or only appear when something has gone wrong?
- Do you feel confident that they know what's happening in your systems?

Regular reviews help keep everyone on the same page. They're an opportunity to ask questions like:

- "Are there any parts of our setup that worry you?"
- "What should we be planning for over the next year or two?"
- "Are our backups and continuity plans still appropriate and tested?"

Warning signs include outdated systems that never seem to get replaced, backups that are taken but never tested, access that hasn't been reviewed in a long time, and a general sense that your provider is always on the back foot.

Perhaps the biggest indicator of all is communication.

> ***If your provider makes you feel silly for asking questions, drowns you in jargon, or leaves you unsure about what's been done and why… you may be relying on the wrong support. A good IT support partner should leave you feeling more in control, not less.***

Bringing it all together

Technology touches every part of your firm. How you communicate, how you store information, how your team works, how secure you are, and how clients experience your service.

You don't need to master the technical detail, but you do need to make sure the basics are in place.

If you keep systems up to date, protect client data with sensible, well-chosen security measures, give your team tools that make their lives easier, control who has access to what, and work with an IT support partner who understands your world and speaks plainly, you'll avoid most of the mistakes that cause law firms pain.

The goal is to reach a point where your systems quietly support your firm, rather than constantly demanding attention.

When that happens, technology stops being a source of stress and becomes one of the most valuable assets in your practice.

If you're interested in working with an IT support partner that truly understands your business and the tech challenges you face, we'd love to help.

Get in touch.

CALL: 509-956-4916
EMAIL: sunderwood@nexgen.tech
WEBSITE: www.nexgen.tech

nexGen TECHNOLOGY SERVICES