No Way Out

What Happens When a Professional Services Firm Gets Hit — And Can't Pay, Can't Hide, and Can't Recover

INNOSEC SECURE SIMPLIFY SUCCEED

A Special Report by Alan McBurney, Founder of INNOSEC

Most firms don't think about ransomware until it happens. By then, the three things they'd rely on — paying the ransom, keeping it quiet, and recovering from backups — have already been taken off the table.



It's Monday Morning. Your Devices Are Locked.

It starts with a phone call before 7am. Nobody can log in. Every laptop and desktop in the office shows the same message: your files have been encrypted, a copy of your data has been taken, and if you want it back — or want to prevent it being published — you need to pay. The amount is in Bitcoin. The deadline is 72 hours.

Nobody can work. No case files. No documents. No accounts system.

But this didn't start this morning.

They've been inside your systems for weeks. Reading client correspondence. Copying files. By the time you see the ransom note, they've already taken what they came for.

You ring your IT provider. They're looking into it. They'll get back to you.

Now the clock starts running — and it's running against obligations your firm already carries under existing law.

Personal data has almost certainly been compromised. Client records. Case files. Financial information. Correspondence. You must notify the Information Commissioner's Office within 72 hours. Not "when you've figured it out." Within 72 hours of becoming aware.

You don't know what was taken. Your IT provider is still trying to work out how they got in.

If individuals are at high risk, you must notify them directly. Your clients. The people who trusted you with their conveyancing documents, their wills, their financial records, their personal injury claims.

If you're a solicitor's practice, the SRA expects to be informed. If you're handling regulated financial work, there may be additional reporting obligations to your professional body.

And if you're thinking about paying the ransom to make it all go away?

The Exit **That Isn't There**

Paying a ransom to a sanctioned entity is a criminal offence under UK law. Not a regulatory breach. A criminal offence.

The gang behind this is almost certainly Russian-affiliated. The UK government has sanctioned 36 ransomware criminals to date. The infrastructure these gangs operate from is linked to sanctioned entities. In 2025 alone, the UK, US, and Australia imposed coordinated sanctions on the providers behind LockBit, BlackSuit, and Play.

The Office of Financial Sanctions Implementation (OFSI) — the arm of HM Treasury that enforces UK sanctions — operates on a strict liability basis. "We didn't know" is not a defence.

They've already fined organisations for exactly this — including a £300,000 penalty in July 2025 for a single payment to a designated individual.

So now you're sitting in your office on a Monday morning. Devices locked. Client data in the hands of criminals. A legal obligation to report within hours. And the one option that might have made the problem disappear is potentially a criminal act.

Where are your backups?

Not whether you have backups. Whether they cover what matters. Whether they're isolated from the environment the attackers have been living in. Whether anyone has actually tested a restore. And how long it takes — because every day without case files is a day of missed court deadlines, stalled completions, and clients you can't serve.

If your IT arrangement is reactive — a helpdesk that fixes things when they break — the honest answer is probably: you don't know.
That's not a hypothetical. That's where a growing number of firms are going to find themselves.

You can't pay. You can't hide. And you may not be able to recover.

Cyber risk is an IT problem that happens to others

Most managing partners at professional services firms think of cyber risk as an IT problem.

Something the provider handles. Something covered by the insurance. Something that happens to other people.

The Obligations You Already Carry

The legal obligations your firm carries are not new, not optional, and not someone else's responsibility. They exist right now, under current law, and they apply to every firm holding personal data — which means every law firm, every accountancy practice, every architectural and engineering consultancy, every financial services provider.



UK GDPR — Breach Reporting

Under the UK General Data Protection Regulation, every organisation that processes personal data must report a notifiable breach to the ICO without undue delay and no later than 72 hours after becoming aware of it. A breach is notifiable if it's likely to result in a risk to individuals' rights and freedoms. A ransomware attack on a firm holding client records, financial data, case files, medical information, or personal correspondence will almost always meet that threshold.

You must also document every breach — even the ones you don't report to the ICO. And if the risk to individuals is high, you must notify those individuals directly. That means telling your clients.

The penalties for serious failures are up to £17.5 million or 4% of annual turnover. For failure to report — up to £8.7 million or 2% of turnover.

UK Sanctions Compliance

Every UK business must screen against the UK Sanctions List before making payments or entering business relationships. For solicitors and accountants, the SRA, Law Society, and CILEx Regulation require screening of clients, counterparties, and beneficial owners — across all practices, not just those regulated for anti-money laundering.

Making funds available to a designated person carries civil penalties of up to £1 million or 50% of the transaction value, and criminal prosecution for deliberate violations. As the opening scenario illustrates, this obligation collides directly with ransomware — where paying the demand may itself be the criminal act.

Professional Body Requirements

Cyber Insurance Policy Conditions

Most firms that hold cyber insurance assume it will be there when they need it. But insurers are tightening policy conditions across the board. Many policies now require evidence of tested backups, multi-factor authentication, endpoint detection, and documented incident response plans — as preconditions for coverage, not as recommendations.

Marks & Spencer made a £100 million claim on its cyber insurance following its 2025 attack. Co-op confirmed it did not have comprehensive cyber cover in place and would not be claiming.

And even when policies are in place, ransom payment coverage is being capped, conditioned, or excluded entirely. Insurers are not going to pay a ransom to a sanctioned entity on your behalf. That would make them complicit in the same offence.

The SRA, LSNI, ICAEW, and equivalent bodies increasingly expect firms to demonstrate adequate security controls, incident response capability, and data protection compliance. This isn't a separate requirement from the above — it's an additional layer of accountability. A firm that suffers a serious breach and cannot demonstrate it had reasonable controls in place faces not just regulatory penalties, but professional conduct implications.



The Escape Routes Are Closing

For years, firms that suffered cyber incidents had a playbook that worked well enough. Pay the ransom. Restore quietly. Lean on the insurer. Keep it out of the press. Move on.

The damage was financial and temporary. Reputations survived because nobody found out.

That playbook is being dismantled — systematically and deliberately — by the UK government.

You Can't Pay

The ransomware economy is dominated by Russian-affiliated gangs operating from infrastructure that the UK, US, and Australia are actively sanctioning. The UK has sanctioned 36 ransomware criminals. Coordinated designations in 2025 targeted the hosting providers — ZSERVERS, Media Land, Aeza Group — that these gangs depend on. Every new designation makes the payment landscape more dangerous for victims.

Even if a specific gang isn't yet designated, the Home Office is building a payment prevention regime that would require all ransomware victims to notify authorities before making any payment. Authorities would then check for sanctions exposure and could block the payment entirely. 72% of consultation respondents supported a targeted payment ban for public sector and critical national infrastructure. 63% supported mandatory incident reporting economy-wide.

The direction of travel is unmistakable: the government wants to make paying ransoms harder, more visible, and in many cases, illegal. The days of a quiet payment through an intermediary are ending.

You can't hide.

UK GDPR already requires breach reporting to the ICO within 72 hours. The Cyber Security and Resilience Bill — currently in committee in the House of Commons — introduces 24-hour initial notification requirements for regulated entities and their supply chains. The Home Office ransomware proposals include mandatory reporting for all ransomware incidents within 72 hours, regardless of whether you intend to pay.

Layer these together and there is no scenario in which a serious cyber incident at a professional services firm stays private. The ICO will know. Your professional body will know. Under the incoming reporting regime, law enforcement will know. And once you've notified the ICO, you may be required to notify affected individuals — which means your clients find out.

> *In a tight-knit professional community — the kind where law firms, accountancy practices, and AEC firms build their reputation on trust — reputational damage from a single incident compounds. It affects every conversation at every networking event, every referral, every tender.*

INNOSEC SECURE SIMPLIFY SUCCEED

You can’t rely on insurance

Cyber insurance premiums are projected to rise 15–20% in 2026. Insurers are demanding evidence of security controls as preconditions for coverage — validated backups, tested incident response, multi-factor authentication, endpoint detection. Only 17% of UK organisations hit by ransomware in 2025 actually paid the ransom, down from 44% in 2023. 24% now have a formal policy never to pay.

The insurance industry is repricing risk and tightening conditions precisely because the threat landscape has changed. If your firm can’t demonstrate basic controls, your coverage may be inadequate, conditional, or void when you need it most.

And the nature of the threat itself has shifted. As the opening scenario describes, modern attackers exfiltrate data before encrypting devices — and in more than half of extortion cases, encryption isn’t even part of the attack. When the threat is data exposure rather than locked systems, backups don’t help. The damage is the leak itself.

> *There is no technical fix for confidential client files being published on a criminal’s website.*





The Direction of Travel

The obligations described above already exist. But the regulatory pressure behind them is building — and it all points the same way.

The Cyber Security and Resilience Bill brings managed service providers into regulation for the first time — with security obligations and enforcement powers to match. The Bill doesn't create a new expectation — it removes any remaining ambiguity about who is accountable and how fast they must act.

In October 2025, the Chancellor and senior ministers wrote directly to all FTSE 350 companies reinforcing that board-level oversight of cyber risk is essential — placing it alongside financial reporting and health and safety as a governance responsibility.

The Home Office ransomware consultation received overwhelming support for a targeted payment ban, a payment prevention regime, and economy-wide mandatory reporting. The government confirmed in July 2025 it intends to proceed with all three.

None of this is theoretical. And the pressure flows downhill. Regulated clients push compliance requirements onto their suppliers. Insurers demand evidence of controls. Professional bodies tighten expectations. Public sector procurement requires demonstrated cyber resilience. The Bill accelerates that cascade — what was informal becomes enforceable, what was best practice becomes baseline.

A 15-person law firm in Belfast doesn't need to be directly in scope of any of these measures to feel their full force. All it takes is one client questionnaire you can't answer, one insurance renewal you can't pass, or one incident you can't report within the required timeframe.

The Questions You Should Be Able to Answer

Here's a test. Not a technical test — a business one. These are the questions that surface in the first hours of an incident, in the middle of an insurance renewal, or when a client asks "how do you protect our data?" If you can answer them clearly, with evidence, your firm is in a defensible position. If you can't, you're carrying risk that could end careers.

On backups and recovery

Your practice management system — LEAP, Clio, Osprey, whatever your firm runs on — holds your client matters, your time records, your billing, your case history. If it was encrypted tomorrow morning, what happens? Not "we have backups." Backup of what, exactly? The practice management database? Your email? The documents in your DMS or shared drive? Your accounts package? Your phone system? Are those backups isolated from the network that just got compromised — or are they sitting on the same system the attackers walked through?

Has anyone actually tested a full restore? Not checked that the backup job completed. Tested it — rebuilt the system from scratch, restored the data, confirmed the firm could function? If your IT provider says "yes, backups are running," ask them: when did you last prove you could bring this firm back from nothing? If the answer is vague, your backups are a hope, not a plan.

And how long does recovery take? A day? A week? Can your firm survive a week without access to client files, email, and accounts? What happens to court deadlines, completion dates, tax filings, project milestones? What do you tell clients in the meantime?

On incident response

It's 7am and your systems are down. Who do you ring first — and what do they actually do? Not "our IT provider." What's the plan? Who assesses whether personal data has been compromised? Who makes the call on whether to notify the ICO? Who tells the partners? Who speaks to clients? Who deals with the insurer?

If the answer is "we'd figure it out at the time" — that's not a plan. That's a scramble. And scrambles don't complete ICO notifications in 72 hours. They don't produce the structured, evidence-based account your insurer will require. They don't give clients the reassurance that protects the relationship.

In a 15 or 20-person firm, the managing partner ends up doing all of this. While also being the person who's supposed to be fee-earning, managing staff, and keeping the practice running. That's not a plan either. That's one person absorbing a crisis alone.

On obligations

Your firm holds personal data — client names, addresses, financial records, case details, medical information in personal injury files, commercial secrets in M&A transactions, family details in matrimonial work. The ICO expects you to protect it. If it's compromised, they expect you to report it. Could you?

Could you explain to the ICO what data was held, how it was protected, and what went wrong — within 72 hours? Could you tell affected clients what was taken and what risk they face? Could you demonstrate that your firm had reasonable security measures in place — or would the investigation reveal gaps you didn't know existed?

And if a client — a bank, an insurer, a public body — sends you a supplier security questionnaire next week, could you complete it honestly? Could you evidence multi-factor authentication, endpoint protection, backup testing, access controls? Or would you be ringing your IT provider and hoping they can help you fill in the blanks?

On ownership

Who actually owns IT across your firm? Not who "sort of looks after it." Not who you ring when the printer jams. Who has the authority to make decisions about technology, the visibility to see problems before they escalate, and the evidence to prove the firm is operating responsibly?
In most firms the answer is: nobody. The IT provider handles the day-to-day. A partner half-watches the bills. Decisions get made reactively — whoever shouts loudest, whatever broke most recently. Nobody has the full picture. Nobody is truly accountable.

That's fine until something goes wrong. Then the managing partner discovers they've been carrying personal responsibility for a function nobody was actually governing — and every gap that was invisible last week is suddenly the subject of a regulatory investigation, an insurance claim, or a conversation with a very unhappy client.

> *If you've read this far and recognised your firm, you're not alone. Most professional services firms with 10 to 50 staff are in exactly the same position. The difference is whether you find out on your terms — or on someone else's.*



Why Your Current Arrangement Can't Close This Gap

This isn't about vendor quality. Most IT providers serving professional services firms in Northern Ireland and across the UK are competent, well-meaning, and responsive when something breaks. The problem isn't that they're bad at what they do. The problem is that what they do isn't what the situation now demands.

> *Most firms have a managed helpdesk, not a managed service provider — despite what it says on the invoice.*

The arrangement is reactive: something breaks, you call, they fix it. You get a monthly bill. Nobody talks about risk, standards, or roadmaps unless something goes wrong.

That model was adequate when the worst-case scenario was a slow laptop or a crashed server. It's not adequate when the worst-case scenario is encrypted systems, exposed client data, mandatory reporting within hours, potential sanctions liability, and an insurance claim that depends on evidence of controls you can't produce.

The gap isn't technical. It's structural.
A reactive helpdesk isn't designed to maintain tested disaster recovery. It isn't designed to produce evidence for regulatory reporting. It isn't designed to run incident response within defined timeframes. It isn't designed to support sanctions-aware decisions under pressure. It isn't designed to give partners clean answers when regulators, insurers, or clients ask "are you covered?"

This isn't a criticism. A two-person IT shop in Belfast was never built for that. But the bar has moved. The obligations are real, the escape routes are closing, and the consequences of being unprepared have shifted from inconvenience to existential risk for a professional services firm's reputation.

The question isn't whether your IT provider is competent. It's whether your IT arrangement — the operating model, the accountability, the evidence, the capability — matches what the law now demands of your firm.



What a Defensible Position Looks Like

If the problem were technical, the answer would be better tools. If the problem were vendor quality, the answer would be a better vendor. But the problem is neither. The problem is that no one owns the outcome — and without ownership, no amount of tools or talent produces the evidence, the speed, or the accountability that the regulatory environment now demands.

That means the answer isn't a technology upgrade. It's a structural one. An operating model with a named owner, clear standards, and visible health — so that when the questions arrive, the answers already exist.

A defensible position isn't about buying more tools or spending more money. It's about having an operating model that can answer the questions that matter — before the questions arrive.

One accountable owner. Not a shared responsibility across partners, an internal "IT person," and an external provider who all point at each other when something goes wrong. One named owner with clear accountability across all IT domains — strategy, security, identity, platforms, change, incidents, vendor coordination. When a client asks "who owns this?" the answer is immediate and unambiguous.

Risk first, then tools. Start with what could damage client trust — security, uptime, confidentiality, data protection — and build controls around those risks. Not the other way around. Most firms accumulate tools and subscriptions without ever mapping them to the risks that actually matter. The result is complexity without confidence.

Standards that hold. Minimum baselines for devices, access, backups, vendor expectations, and onboarding. Not "we try to keep things consistent." Documented standards that mean every device, every user, every system behaves predictably. Standards are what turn change from a gamble into a routine.

A roadmap before projects. A simple sequence of improvements — what happens now, what happens next quarter, what can wait — so every change is planned, scoped, and justified. No more reactive firefighting disguised as progress. No more projects that start because something broke and stop because something else broke louder.

Visible weekly health. A short, consistent set of signals — security posture, backup status, open issues, upcoming changes — so leadership always knows what's handled and what's next. Not a 30-page monthly report nobody reads. A weekly rhythm that takes five minutes and removes the guesswork.



What This Looks Like in Practice

A 14-person solicitors' practice in Northern Ireland. Two partners, a mix of solicitors and support staff, steady caseload across conveyancing, commercial property, and private client work. Well-regarded locally. The kind of firm where clients come through referrals and stay for years. The partners were protective of their reputation — it was the practice's most valuable asset.

They had an IT provider. Monthly invoice, reactive support. When the internet dropped or a laptop played up, they rang and someone fixed it. Occasionally the provider recommended a new tool or upgrade. The partners said yes or no based on cost and disruption. Nobody asked deeper questions because the IT seemed to work.

Now map that to the obligations in this report.
The firm held client data across conveyancing files, wills, powers of attorney, commercial leases, and litigation matters. Personal names, addresses, financial details, bank account information, medical records in personal injury cases, family details in matrimonial work. All subject to UK GDPR. All requiring 72-hour breach notification to the ICO if compromised. All requiring direct notification to affected individuals if the risk was high.

The firm also had SRA obligations — including sanctions screening for clients and counterparties. But the screening was informal, inconsistent, and undocumented. Nobody had considered what would happen if the firm was hit by ransomware and faced a demand from a Russian-affiliated gang. Nobody had thought through whether paying would constitute a sanctions offence.

Their backups? The provider said they were running. But nobody at the firm — or, it turned out, at the provider — had tested a full restore of the practice management system. Nobody could confirm how long recovery would take, or whether the backup data included everything the firm needed to function: the case management system, email, documents, accounts, and the phone system.

Their incident response plan? There wasn't one. No defined roles, no communication plan, no documented steps for assessing a breach, notifying the ICO, or informing clients. If something serious happened, the managing partner would have been making it up in real time — while simultaneously trying to reassure staff, deal with the provider, and work out which clients were affected.



Their cyber insurance? The policy existed, but the last renewal had come with new conditions — evidence of MFA, endpoint protection, backup testing — that the firm had ticked "yes" to on the assumption the IT provider had it covered. Nobody had verified whether that was true.

The transformation took 60 days. Not because the technology was complex, but because the problem was never technology. It was ownership.

One accountable owner was named across all systems and vendors. Risks were mapped — starting with what could hurt client trust and trigger regulatory obligations, not with what tools were available. Standards were set for devices, access, backups, and vendor expectations. A simple roadmap sequenced improvements so nothing felt like a gamble. A weekly health rhythm gave the partners visibility without requiring them to understand the technical details.

The sanctions screening process was documented and made part of standard operating procedure. Backups were tested — actually tested, with a full restore — and the recovery timeframe was established and communicated to the partners. An incident response plan was written with named roles, so the managing partner wasn't carrying the entire burden alone.

By the end of the second month, the partners could answer the questions that matter. What's in place? Who owns it? What happens if something goes wrong? What evidence do we have?

The next cyber insurance renewal was straightforward — because the evidence existed. The next client security questionnaire was completed in two days. And when a minor incident occurred — a compromised email account detected and contained within hours — the firm had a clear, structured account ready for the SRA and the affected client the same day.

> **"They didn't become more technical. They became more certain.**

Common Objections

At this point you usually have two worries, even if you agree the current setup is fragile. First: "We don't have time for an IT change." Second: "This sounds expensive—let's just patch it." And there's a third, more practical one that often sits underneath both: "Even if we wanted to change, we're mid-contract with our current provider." All three are rational when things are still "manageable enough." The problem is that "manageable" is where most professional services firms quietly build exceptions, dependency, and risk—until a client questionnaire, an outage, or a security scare forces change on the worst possible timeline.

"We Don't Have Time To Deal With It Changes Right Now"

I hear you. In a small-to-mid professional services firm, every disruption hits delivery, and partners don't get spare capacity.

But consider this: you're already spending the time—you're just paying for it in fragments. It shows up as interruptions, slow systems, one-off fixes, "who owns this?" loops, and senior people making technical calls they shouldn't be making.

A controlled change isn't "extra work." It's converting random disruption into a planned sequence with clear ownership.

When there's no single owner or operating model, decisions resurface, priorities swing, and providers run unchecked. That drains senior time and keeps the firm dependent on individuals.

The fastest path is rarely a big bang project—it's setting a stable baseline and a simple roadmap so changes stop feeling like gambles.

"This Sounds Expensive — We'll Just Patch It For Now"

I hear you. Nobody wants a blank cheque, and "patch it" feels like the cheapest, least disruptive choice when nothing is on fire.

But consider this: "patching" is rarely cheaper—it just hides the cost in risk and repeat work. You don't avoid spending; you lose control over when you spend, how urgently you spend, and what it does to the firm's reputation if it goes wrong.

In professional services, the real cost isn't the invoice—it's the exposure: client trust, confidentiality, delivery downtime, and leadership stress when you can't confidently answer "are we safe and stable?"

Firms that let the provider set the agenda or allow exceptions to become the real standard end up with more complexity and less confidence—more logins, more one-off setups, and more brittle systems.

That's why "cheap-first" decisions tend to create recurring issues, urgent spend, and growing compliance/cyber exposure.

We Can't Change Right Now — We're Mid-Contract With Our Provider.

I hear you. If you're locked into a contract, the last thing you want is a messy switch, duplicated cost, or a political fight with the current provider.

But consider this: you don't need to wait for renewal to understand what's missing. Starting mid-contract doesn't mean running operations alongside your current provider or bolting on a second relationship.

It means building the decision framework you're missing: a short diagnostic to see what's actually underneath, a risk-first view of what could hurt trust, clear standards for what "good" looks like, and decision criteria for what should change and what shouldn't.

That gives you two things immediately: first, you stop guessing — because you can finally see your real exposure in plain English.

Second, you stop drifting into another auto-renewal — because you'll have a transition plan ready well before the contract ends. When you do decide to transition, the timing is driven by your risk and your constraints — not by vendor pressure or a last-minute surprise.

If after the diagnostic you decide your current provider is truly delivering the outcomes you need, you'll know that too — and you'll have a clearer way to manage them. Either way, you walk away with clarity and a path forward.



Two Paths

Every professional services firm will face these obligations. The only question is whether you meet them on your terms or someone else's.

Path one leads to exposure.
An incident occurs — or a client questionnaire arrives, or an insurance renewal gets complicated — and you discover the gaps under pressure. You can't report within the timeframe. You can't evidence controls. You can't confirm whether backups work. Every option costs more, takes longer, and carries more reputational risk than it would have six months earlier. And the escape routes you might have relied on — a quiet payment, a discreet resolution — are no longer available. The managing partner absorbs the crisis alone, making it up in real time, hoping the damage is survivable.

Path two leads to certainty.
You understand where your firm stands — what's in place, what's missing, and where the real exposure sits. You put a simple operating model in place so that when the questions arrive — from a client, an insurer, a regulator, or an attacker — you answer calmly. With evidence. Without drama. The partners know what's handled, what's being watched, and what's next. The firm operates from a position of control, not hope.

> *The lesson from every firm that's made this transition is the same: it was never technology. It was ownership.*

TWO CLEAR NEXT STEPS:

OPTION 1

Book the 25-minute IT Ownership Diagnostic

In 25 minutes you'll have a clear picture of your firm's position against the obligations in this report, the specific gaps that need closing, and a practical sequence for addressing them. Whether you stay with your current provider or not.

OPTION 2

Not ready to talk yet? Take the Self-Assessment

Not ready to talk yet? The short IT Ownership & Risk Self-Assessment takes a few minutes and gives you a clear read on where accountability is breaking down and where your real exposure sits — so you can decide if and when a conversation makes sense.

INNOSEC

SECURE · SIMPLIFY · SUCCEED

© INNOSEC · Modern Practice Operating System™
Calm, secure operations. Owned — not hoped for.