softwerx
The Microsoft Security Specialists

The Secure Legal Practice

How UK law practices with lean in-house IT teams can strengthen protection, credibility and operational continuity with Microsoft Security® and Managed XDR solutions from Softwerx

Table of Contents

Foreword:

Legal practices are being judged on more than just legal expertise. Clients, regulators and insurers now expect clear evidence that sensitive matters, privileged data and client funds are properly protected against cybercrime. For many practices, that expectation is rising faster than internal resources can keep up with.

The legal sector sits in a demanding middle ground. Many small and medium-sized legal practices below enterprise scale rely on lean internal IT and security teams. However, they face a similar level of threat intensity and compliance pressure as the largest global practices but without equivalent budgets, staffing or specialist skills. Running a fully staffed 24x7 Security Operations Centre (SOC) is unrealistic for most, and even well-run in-house teams cannot monitor every access attempt or e-mail all the time. However, cybercriminals operate round the clock and regulators do not relax security standards for smaller organisations.

This is why a predictable and affordable operating model matters. For legal practices with stretched IT resources, it makes sense to treat cybersecurity as a managed operating expense rather than a open-ended capital spend. This approach provides ongoing specialist cover, continuous monitoring and response, and a modern security capability that can scale with the practice without needing to build and fund a large internal security team.

At the same time, the threat environment is becoming more complex. While the wider cybersecurity industry is adapting, Microsoft® stands out for the scale of its security investment. A $20 billion commitment is broadening and deepening the effectiveness and integration of its security technologies, powering a global security ecosystem within Microsoft 365® – the business ecosystem that most legal practices already rely on.

For many practices the real opportunity is not to add more tools but to implement and optimise the Microsoft Security technologies they already own within their Microsoft 365 licences, and to reinforce them operationally with **secure365®**, the Managed eXtended Detection and Response (XDR) solution from Softwerx.

The Secure Legal Practice guide shows how Softwerx helps law firms use Microsoft Security to improve hygiene, compliance and resilience while preparing for AI and tougher client due diligence. Breaches are inevitable. What matters is how quickly you can detect, contain and mitigate their impact, and how professionally you protect your own reputation and that of your clients. With Microsoft Security and **secure365**, cybersecurity is monitored and improved by specialists 24x7 so in-house teams can focus on the wider needs of the practice.

David Smart, CEO, Softwerx

Over half of cyberattacks with a known motive are now driven by extortion and ransomware, and data theft is present in approximately 80% of incidents investigated by Microsoft's security teams (Microsoft Digital Defence Report 2025, microsoft.com). For legal practices, this reinforces a simple truth: criminals go where valuable data and operational pressures meet.

1. The reality of risk:
Why every legal practice must assume a breach

With a small internal IT team supporting a growing, multi-site firm, we have had to be honest about what we could manage ourselves. Continuous monitoring and incident response cannot sit alongside day-to-day legal operations. Through our partnership with security specialist Softwerx we have access to expert advice which enables us to stay up to date with current and emerging threats and maintain effective risk management strategies.

Jack Fairweather, Director,
Fairweather Law Limited

Legal practices handle precisely the kinds of information that cybercriminals can monetise fast: personal data, health and family details, M&A papers, dispute strategy, IP filings, funds held on account and privileged communications. This makes law firms consistent and potentially lucrative targets.

The UK legal sector is being constantly targeted for phishing, ransomware, business email compromise and password attacks (NCSC Cyber Threat Report for the UK Legal Sector, ncsc.gov.uk). Identity compromise remains the most common attack vector, reflecting how modern cybercriminals focus on access and users rather than on network perimeters.

What makes the legal sector different to many other business markets is its necessary attitude to risk – the consequences of getting cybersecurity wrong in the legal space are simply worse. For example, consider the following aspects:

1. Regulations that must be met

Both stringent legal regulation and professional codes obligate practices to heavily protect data, confidentiality and client funds and to report cyber incidents promptly (SRA Cybersecurity and IT Guidance 2025, sra.org.uk).

2. Operational fragility

A serious cyber incident can bring a legal practice to a complete stop: halting casework, delaying court deadlines, preventing conveyancing, billing and client communications. Most practices are mid-market-scale organisations lacking the financial resources to deal with outages of more than a few days without severe, potentially existential cashflow consequences for their business.

3. Client perception

Clients generally assume their practice is secure – it's implied by the fact they were engaged in the first place. As a result, they can be unforgiving when this turns out not to be the case or, more accurately, when a breach is unprofessionally or ineffectually dealt with or mitigated. A poorly handled cyber breach can change the trust equation overnight, especially regarding sensitive matters.

A managing partner in our research expressed the stakes plainly: "*Fire and flood we can recover from. A cyberattack could end the business. We could only survive a short outage before the financial pressure became existential and clients would not be sympathetic if the failure was ours.*"

43% of UK businesses experienced a breach or cyberattack in the last 12 months, and the rate rises with organisation size, showing the pressure on legal practices is real and persistent

(Cyber Security Breaches Survey 2025, gov.uk)

What legal leadership should be asking:

- *Do we understand the risks the practice is exposed to from potential cyber events?*
- *What level of business risk is the practice willing to take and what risks are unacceptable?*
- *If our business infrastructure was compromised, how long could we keep serving clients?*
- *If our network was compromised, how long could we survive as a business?*
- *How quickly would we know an attacker was inside our systems?*
- *What evidence could we show regulators or insurers within 72 hours?*
- *What happens if we are breached outside business hours – at 2am or a weekend?*
- *Are we confident that privileged information would stay protected under pressure?*

Breaches are not hypothetical. They are a certainty in the current threat landscape. The question is how prepared a legal practice is to **limit impact, contain exposure and recover fast.**

Cyber threats are now a fact of doing business and they force very real conversations at leadership level. They sharpen focus on how sensitive data is protected, how disruption is managed and how quickly client confidence can be lost if an incident is mishandled. That reality has reshaped our risk appetite and elevated cyber security as a board-level responsibility. Awareness is key. Constant monitoring, early detection and an ongoing understanding of emerging risks is a necessity. It is very much a living process as the cyber security landscape continues to evolve on a rapid basis.

Jack Fairweather, Director,
Fairweather Law Limited

2. **Assumed trust is no longer enough:** Why firms must prove their security hygiene

Better cybersecurity will not make clients choose us over another firm. But without it, we cannot get into the building. It is part of modern legal DNA.

Trust in the legal sector has long been assumed – if you are a lawyer, then by definition you are trusted.

Clients expect law firms to protect their data, apply sound controls and uphold confidentiality as a matter of course – it's implicit in the relationship. That assumption is starting to harden into the need for proof. Corporate clients now invariably enter detailed due diligence activity when engaging new legal counsel, insurers want clear evidence of business controls and processes and regulators are issuing penalties when basic security safeguards are missing or breaches are mishandled.

But this does not mean having the best cybersecurity on its own will win you business. It does, however, mean that having poor security will stop you from even competing for it in the first place.

Three forces are driving this change:

1. Insurance requirements have hardened

Professional indemnity cover in the legal sector now routinely includes strict requirements in terms of cyber hygiene, with insurers increasingly mandating the implementation of technologies such as multi-factor authentication (MFA), Zero Trust endpoint controls, patching discipline, secure backups and incident response readiness (Law Society Cyber Insurance Guidance 2025, lawsociety.org.uk).

2. Regulatory enforcement is tightening

In the UK, the Information Commissioner's Office (ICO) has fined law firms in 2025 for late breach notification and technical breaches such as missing MFA, reinforcing a much stricter benchmark for professional competence (ICO Enforcement Notices 2025, ico.org.uk).

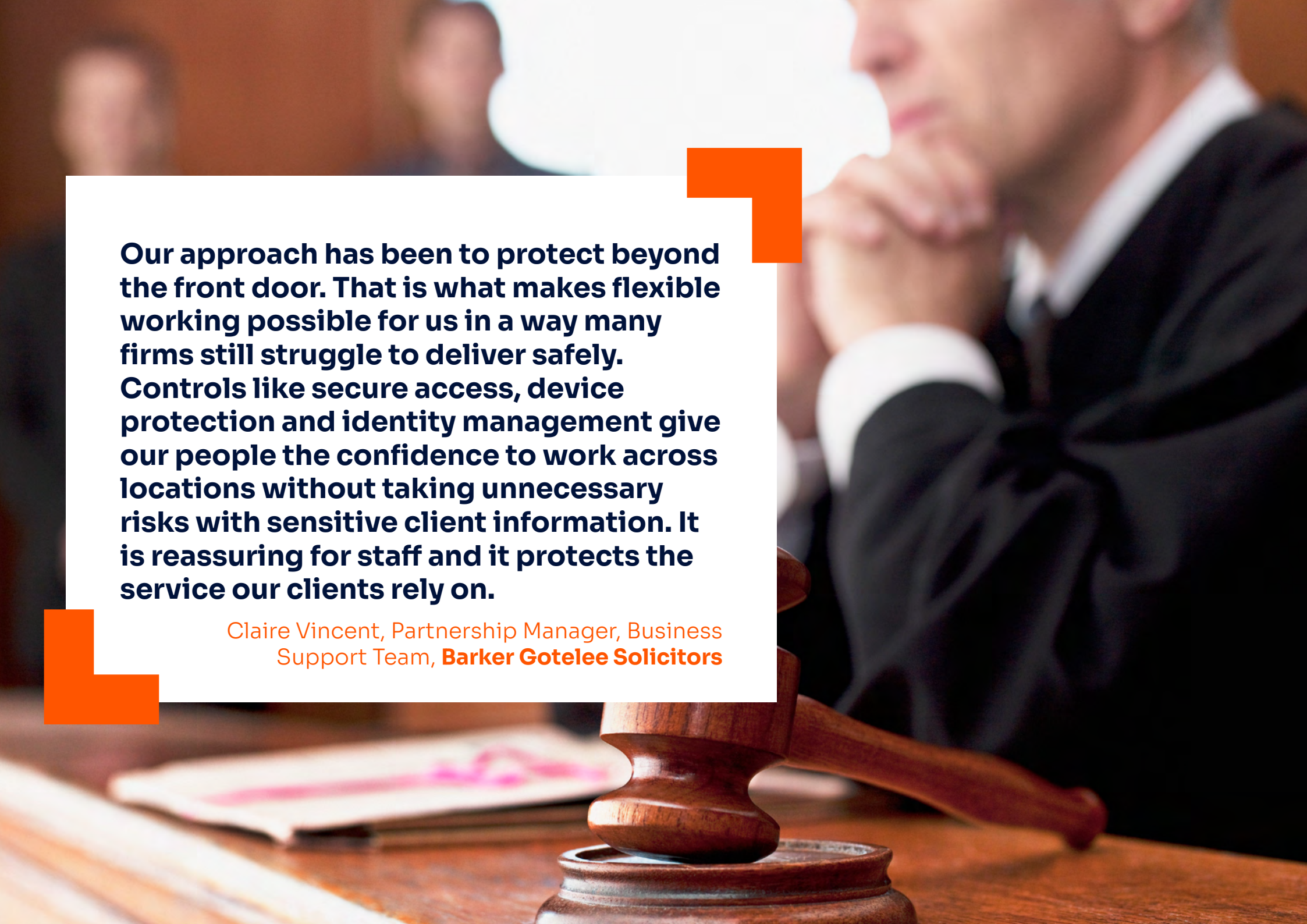
3. Client due diligence is growing

Legal firms entering larger tenders are already seeing security questionnaires and evidence requests become routine – requiring the provision of proof to a sufficiently high level of cyber hygiene, not as a commercial differentiator but as table stakes to even participate in the tender at all.

What a Microsoft 365 business stack means for a Secure Legal Practice

According to the Law Society of England and Wales, 78% of UK law practices now use cloud computing services, with the majority explicitly using Microsoft 365. This has direct cybersecurity implications. Microsoft 365 is available in several licence bundles aimed at different segments, each with a different security capability.

Microsoft 365 Business plans are designed for organisations with up to 300 users, while Enterprise (E3 or E5) plans are for organisations larger than that. Microsoft 365 Business Standard and Microsoft 365 E3 are unlikely to be appropriate choices on their own for legal firms, since they are designed mainly for productivity and lack the necessary security capabilities. Legal practices with fewer than 300 users should be using or considering Microsoft 365 Business Premium as a minimum baseline, adding Microsoft Defender and Purview Suite licence upgrades for full enterprise-class compliance and security if required. Larger practices with more than 300 seats should plan to implement Microsoft 365 E5 if they have not already done so.



Our approach has been to protect beyond the front door. That is what makes flexible working possible for us in a way many firms still struggle to deliver safely. Controls like secure access, device protection and identity management give our people the confidence to work across locations without taking unnecessary risks with sensitive client information. It is reassuring for staff and it protects the service our clients rely on.

Claire Vincent, Partnership Manager, Business Support Team, **Barker Gotelee Solicitors**

Microsoft 365 Business Premium and Microsoft 365 E5 are bundles of productivity, management and security products. However, the security content is only of value if fully implemented, configured and monitored. A common problem for smaller organisations without a critical mass of operational security expertise is that, sometimes, this doesn't happen. The security value is there in the Microsoft 365 licence being paid for, but it is not always activated or managed.

This under exploitation of bundled Microsoft Security technologies creates a gap between what firms believe is protected and what clients, insurers and regulators can evidence. Microsoft Security is an industry-leading, integrated portfolio of AI augmented, enterprise-grade tools that includes identity protection, endpoint detection and response, threat intelligence and compliance solutions. Used well, it supports both hygiene and higher levels of assurance, helping practices raise standards, demonstrate control and prepare for AI safely. Since legal firms are almost certainly already paying for it in their Microsoft 365 licences, it makes strong business sense to extract full value from what is already in place.

In practical terms, Microsoft 365 E5 (or Microsoft 365 Business Premium plus Defender and Purview Suite upgrades) strengthens a Secure Legal Practice by enabling:

Stronger identity control so every lawyer, assistant and contractor is verified, access is conditional and risky sign-ins are blocked early.

Higher assurance endpoint protection for laptops and mobiles, with faster detection of ransomware, credential theft and suspicious behaviour.

Better protection for email and collaboration which remain the most common entry points for phishing, impersonation and invoice fraud.

Improved data classification and governance so privileged and sensitive client data is labelled, protected and shared only with trusted users.

Clearer evidence of hygiene through reporting and auditing that supports tender due diligence, insurer renewals and regulatory scrutiny.

Safer AI adoption because strong identity, device and data controls reduce the chance of AI tools exposing confidential material.

The message for legal leadership is simple. If Microsoft 365 licences (E5 or Business Premium) are already owned, there's a clear opportunity to optimise existing investments by upgrading if necessary, and by ensuring that any bundled Microsoft Security technologies are being correctly configured, managed and 24x7 monitored. This may even lead to cost savings if additional third-party tools are being used to deliver capabilities that might be better provided by underutilised Microsoft Security technology included in the Microsoft 365 licences.

Softwerx helps legal practices strengthen baseline hygiene by optimising the available Microsoft Security technologies across identities, devices, email, cloud and data, and then enforcing those controls through 24x7 monitoring and response via the **secure365** Managed XDR service. Softwerx can also help you determine whether additional upgrade licences are advisable for your organisation to implement true enterprise-grade security.

Overall, this makes the resulting cybersecurity capability fully optimised, transparent, credible and measurable in the moments that matter for legal practices such as tenders, audits, insurer renewals and incident response.

3. The pressure to adopt AI safely

We realised early on that AI was coming into the legal workplace, whether we were ready or not. Trying to block it or ignore it was never going to work, so we put an AI policy in place early which continues to evolve, to take control in a measured way. The priority is always in protecting client confidentiality and making sure staff have clear boundaries on what is acceptable, so we can explore the benefits of AI without putting trust or compliance at risk.

Claire Vincent, Partnership Manager, Business Support Team, **Barker Gotelee Solicitors**

AI has already made huge inroads into legal work. Email summarisation, contract parsing, matter search, drafting support and knowledge retrieval are already mainstream use cases. The risk comes from deploying AI without the right security guardrails.

> The use of AI features within Microsoft 365 is rising in legal workflows, especially in firms seeking efficiency without compromising confidentiality.
> (Legal sector AI adoption analysis 2025)

Legal teams are already asking hard questions:

- *If AI sees a document, who else might see it?*
- *Where is client data that is passed through AI tools processed and stored?*
- *How do we stop staff using unapproved consumer AI tools?*
- *What does AI mean for privilege, confidentiality and regulatory reporting?*
- *How can we provide paper trails where required for AI-processed documents?*
- *How do we ensure AI outputs are professional and auditable?*

Shadow AI is a growing issue. Staff often experiment with consumer AI tools without considering the consequences for confidentiality. According to the 2025 Microsoft Work Trend and AI Risk commentary report, there is a steep rise in unapproved workplace AI use, with 71% of UK employees having used unapproved consumer AI tools at work, creating unmanaged exposure for sensitive data.

Microsoft has responded directly to data-sensitive sectors by committing to the enablement of in-country processing for their AI technology, Copilot, for UK Microsoft 365 customers by the end of 2025, supporting data residency expectations (Microsoft 365 UK processing update 2025). This is a major step forward for sensitive market sectors such as legal but it's only significant if the underlying cyber hygiene resulting from an optimal Microsoft Security implementation is strong.

AI can be transformational for business, but it can also magnify operational weaknesses, particularly related to security. If identities are over-privileged, if data is unclassified or if devices are unmanaged, poorly secured AI can actually magnify the effects of those flaws.

Softwerx helps legal practices adopt AI securely by:

- Strengthening foundational identity and access hygiene.
- Ensuring sensitive data is governed and classified.
- Tightening control of unmanaged apps and data sprawl.
- Continuous monitoring for misuse and leakage.

Maintaining 24x7 oversight and response through Managed XDR helps to keep firms compliant and confident in their security posture while allowing them to benefit from AI-driven efficiencies.

4. For legal practices, resilience is reputation: Why response speed determines survival

The trusted relationship with Softwerx is pivotal. Their security knowledge and skillset are genuinely reassuring, especially as new threats emerge all the time. Whether it's keeping on top of market developments or seeing practical demonstrations of risks such as deepfakes, it helps us stay proactive and aware, rather than being caught off guard. Their guidance is invaluable.

Claire Vincent, Partnership Manager,
Business Support Team, **Barker Gotelee Solicitors**

For legal leaders, the business risk is not only in a breach. It is the operational and reputational risk that follows when the response to a breach is slow or ineffective.

A cyber incident can stop litigation work, delay completions, freeze time tracking, block access to case files and interrupt cashflow. Many mid-scale practices would struggle to survive a prolonged outage and insurers rarely pay interim costs before cash flow problems bite.

> Microsoft incident investigations show ransomware can move from access to major impact extremely quickly, making early detection and containment the main control that separates disruption from catastrophe.
> (Microsoft Digital Defence Report 2025)

Most law practices with lean internal IT or security capabilities simply do not have the scale to run a 24x7 SOC. That's not a failure, simply a reality. A viable in-house SOC, providing continuous monitoring and response, can cost millions of pounds in staffing and capital expense and take months or even years to set up. Outsourcing the SOC function to a specialist Managed XDR solution provider like Softwerx, with its **secure365** offering, is an efficient and cost-effective response to this problem.

Legal practices typically do not have the staffing depth or specialist security skills to run 24x7 monitoring and threat response in-house. Even strong IT teams are stretched across infrastructure, user support, compliance and digital change, and in any case the technical skills and profile of staff required to enforce cybersecurity effectively are different to those found in typical IT teams. Outsourcing round-the-clock detection and response to highly accredited specialist security analysts removes that burden while greatly raising the level of assurance.

secure365 provides continuous monitoring, rapid incident triage and high levels of assurance and response built exclusively on a foundation of Microsoft Security technologies. It delivers:

- 24x7 detection and investigation.
- Automated containment to stop spread and limit exposure.
- Rapid analysis, escalation and incident handling by cybersecurity specialists.
- Threat hunting to pre-empt potential future incidents.
- Full operational transparency.
- Reporting aligned to insurer and regulator expectations.
- Financially backed service-level guarantees and response times.
- UK-based analyst coverage.
- Improved operational continuity.

This gives legal practices the best possible chance to handle a breach professionally, limiting sensitive data exposure and minimising recovery time while protecting both the client and the firm's reputation.

5. How Microsoft Security meets the sector's regulatory and insurance obligations

We've always looked at security from the outside in: what could go wrong and what would that mean for clients. GDPR sharpened our focus and rising fraud and phishing kept us proactive. Cyber Essentials Plus was our baseline but we chose to go beyond minimum standards to protect our reputation.

Adam Waumsley, IT Manager, Business Support Team, **Barker Gotelee Solicitors**

Legal, regulatory and professional requirements for cybersecurity are governed by several overlapping rule sets:

- SRA professional standards on confidentiality and client funds protection (SRA guidance 2025, sra.org.uk).
- UK GDPR and Data Protection Act expectations on appropriate safeguards and breach notification within 72 hours (ICO guidance 2025, ico.org.uk).
- NCSC guidance on phishing, business email compromise, ransomware and supply-chain risk for legal services (NCSC legal sector report, ncsc.gov.uk).
- Professional indemnity cyber controls and insurer mandates (Law Society cyber insurance guidance 2025, lawsociety.org.uk).

Microsoft Security aligns with these obligations by providing layered controls across identity, endpoints, email, cloud apps and data governance, with auditability and reporting suited to regulatory and insurer evidence demands. In many cases, the stated regulatory requirements map directly onto the feature sets found with the Microsoft Security portfolio and reinforced by the operational outcomes delivered by **secure365**.

How the Microsoft 365 E5 licence supports legal regulation and insurance controls

Microsoft 365 E5 bundle capabilities map directly to the controls the legal sector is now expected to evidence. Optimising these capabilities in a legal practice's infrastructure is a practical route towards compliance and insurance readiness:

- **SRA confidentiality and client funds obligations** are supported through stronger identity governance, access control and continuous monitoring of suspicious activity.
- **UK GDPR security requirements** are supported through encryption, classification, data loss protection and audit trails that show sensitive information handling.
- **Professional indemnity cyber controls** are supported through mandatory MFA, endpoint monitoring, rapid incident response and proof of active oversight.
- **NCSC and Cyber Essentials baseline expectations** are supported through phishing protection, identity safeguards, endpoint control and response readiness.
- **Tender and client due diligence demands** are supported through reporting that demonstrates hygiene, monitoring and response capability rather than informal assurance.

The Microsoft 365 Business Premium licence (plus added Microsoft Defender and Purview Suite upgrade licences), in conjunction with a secure365 Managed XDR implementation, also addresses these controls but for smaller organisations.

The resulting security posture should be audited against your practice's attitude to risk and the regulatory and reputational standards that you wish to apply. Consultancy from Softwerx can help you with this, including our comprehensive Cybersecurity Assessment (CSAT) service.

None of this is about technology alone. It is about using the Microsoft Security investment already in place to meet legal standards in a measurable and repeatable way.

secure365 strengthens this further by making sure your controls are actively monitored and incrementally improved every day. It catches misconfigurations early, detects attacks quickly and ensures response is consistent, not improvised.

6. What the Secure Legal Practice looks like

The Softwerx vision of a Secure Legal Practice is defined by:

- Implementing and optimising whatever Microsoft Security is already owned through existing Microsoft 365 licences.
- Accepting that the investment required for an internal 24x7 SOC is unrealistic for most mid-scale firms.
- Transforming cybersecurity provision from a capital investment to a predictable, scalable OpEx model.
- Partnering with industry-expert Microsoft specialists whose only job is leading-edge cybersecurity.

We already had Microsoft licences but moving from Business Standard and Basic to Business Premium licenses unlocked far more of Microsoft's built-in security capability. Layering secure365 on top brought structure, visibility and 24x7 oversight that we could not achieve on our own. It closed gaps and significantly strengthened our confidence in our security foundations.

Jack Fairweather, Director,
Fairweather Law Limited

secure365 was the final piece of the puzzle for us. Hackers do not sleep and I do not want to wake up to chaos in the office. What has changed is the speed at which hacking threats emerge and evolve. With Softwerx monitoring in real time, we know issues are spotted early and dealt with fast, not hours later once the damage is already done. That level of proactive alerting and response is hugely reassuring and it means I can genuinely sleep soundly.

Adam Waumsley, IT Manager, Business Support Team, **Barker Gotelee Solicitors**

The Secure Legal Practice includes:

1. Identity discipline

MFA everywhere, privilege tightly controlled using Zero Trust principles, risky behaviour spotted early.

2. Data governance

Client information labelled, protected and access governed. Confidentiality strengthened by design, not reminders.

3. Device and cloud control

Managed endpoints, secure hybrid work and visibility across cloud apps.

4. AI-readiness

AI deployed only where identity and data controls make it safe, supported by UK data sovereignty commitments.

5. Continuous monitoring and response

secure365 provides the operational capability that mid-scale legal practices cannot realistically build alone, with Softwerx specialists monitoring your Microsoft infrastructure 24x7 so your internal teams do not have to.

6. Evidence and assurance

Security hygiene can be objectively demonstrated to insurers, regulators and clients through credible, transparent reporting and dashboards, not just vague, informal claims.

Microsoft 365 is the dominant IT infrastructure platform for UK legal practices, so the fully integrated Microsoft Security technology bundled with it is already the natural foundation for cyber resilience in the legal sector (UK legal IT adoption analysis 2025). The opportunity is to get full value from what firms already own by optimising it and exploiting it fully with 24x7 Managed XDR operations.

Softwerx can help you with this optimisation and suggest ways to improve your security posture in line with your attitude to business risk. Through the adoption of industry-leading 24x7 Managed XDR solution **secure365**, Softwerx can give law practices enterprise-grade cybersecurity capabilities at a cost and level of complexity that fit their scale and business.

In summary

Protection, credibility and operational continuity

Good cybersecurity is not a stand-alone differentiator for law practices. It is table stakes. Having it will not win work on its own. However, lacking it risks exclusion from tenders, from client due diligence failures, a loss of credibility and serious operational harm if an incident is poorly handled.

The Secure Legal Practice insights in this guide help firms with lean in-house IT and security teams implement a cybersecurity infrastructure that delivers the required level of assurance efficiently and visibly. Adopting its recommendations will strengthen cyber hygiene, support compliance, build resilience into daily operations and prepare firms for an AI-enabled future without compromising confidentiality or client trust.

It recognises a hard truth. Cyber breaches will happen. The winners will be the firms that acknowledge this: how quickly they detect them, how effectively they contain and mitigate their impact, and how professionally they protect sensitive data and maintain service continuity when under pressure.

Softwerx supports this by optimising the Microsoft Security capabilities firms are already paying for and operationalising them through the enterprise-class 24x7 Managed XDR protection delivered by its **secure365** solution.

The result is a practice that safeguards every matter, sustains trust under scrutiny and operates with confidence in a legal market where credibility underpins everything.

About Softwerx

At Softwerx, we empower mid-market organisations to unlock the full potential of Microsoft Security. Through expert consultancy, strategic guidance and hands-on support, we help businesses optimise their Microsoft infrastructure, security posture and licensing. Our UK-based 24/7 Security Operations Centre (SOC), alongside our flagship Managed eXtended Detection and Response (MXDR) service, **secure365®**, leverages Microsoft 365 Defender and Microsoft Sentinel to deliver real-time threat detection, rapid incident response and intelligent security event management.

We make enterprise-grade cybersecurity both **accessible and affordable** – tailored specifically for the needs of security-conscious mid-market organisations.

Our approach guides you on a clear, tailored security journey – from initial audit to actionable outcomes – all shaped around your business's unique needs. Powered by Microsoft technologies and enriched by deep domain expertise, we take you through a structured process of discovery, assessment and expert advisory.

We transform insight into measurable impact – helping you build a resilient, future-ready security posture with confidence, clarity and the ability to protect what matters most while driving innovation forward.

Get in touch to explore how Softwerx can help secure and strengthen your business.

softwerx
The Microsoft Security Specialists

Merlin Suite, Middle Court, Copley Hill Business Park, Babraham, Cambridge, CB22 3GN Cambridgeshire

www.softwerx.com
+44 (0) 1223 834 333
info@softwerx.com