softwerx

The Microsoft Security Specialists

# The Secure Legal Practice

## Your Security Checklist

Future reputational crises facing law firms will not begin in a courtroom. They will start with a security breach. Cyber attacks are inevitable and law practices are increasingly judged on how they manage the fallout of an incident as much as on their legal expertise.

Most UK law firms operate as LLPs. When a breach occurs, it is not an abstract corporate event. It directly affects partner drawings, firm valuation, professional indemnity excesses and long-term client retention. In this model, security is not simply an IT issue. It is a balance sheet issue and a governance issue.

Clients, regulators and professional indemnity insurers expect clear cyber hygiene, incident response readiness and demonstrable oversight of security controls. SRA scrutiny is increasing and client security questionnaires are becoming more forensic. At the same time, AI now sits firmly within everyday legal workflows, amplifying weaknesses in identity management, data governance and endpoint security. Shadow IT and consumer-grade AI tools can quietly bypass safeguards where governance is weak.

Ransomware has evolved into data exfiltration and double extortion. Reputational damage now extends beyond downtime to public leak sites and client notification obligations. Add to that growing supply chain exposure across chambers, expert witnesses, e-disclosure providers and SaaS legal platforms and the threat landscape is broader than many mid-sized firms appreciate.

When data and trust are your currencies, protecting them demands a clear view of threat exposure, regulatory duties and client expectations. This checklist sets out 10 critical cybersecurity steps UK law practices should take in 2026 – plus one often overlooked essential. Each is designed to reduce risk, strengthen resilience and maintain operations when incidents occur.

# Checklist

## 1. Right-Size Cybersecurity for Your Law Firm

When a key client asks for evidence of your cyber controls during a panel review, or your insurer increases your excess following a market-wide breach, the financial impact lands directly on the partnership.

It is no longer a question of if, but when. Determined attackers will find a way into your network. Law firms must shift from a breach prevention mindset to informed risk management. The key question is how much damage a breach would cause to clients, compliance obligations, continuity and professional reputation.

Security investment should be proportionate to the level of business risk the practice can tolerate. Overspending diverts resources. Underspending exposes unacceptable consequences, including higher PII excesses and lost panel appointments. Define risk tolerance, assess your posture against recognised benchmarks such as Cyber Essentials Plus or ISO 27001 where appropriate and align spend accordingly.

## 2. Prove Cyber Resilience Before It's Too Late

If a ransomware attack encrypts active matter files the week before completion, the real test is not whether you had a plan but whether you can restore systems and reassure clients within hours.

An incident response plan on paper is no longer sufficient. Firms must demonstrate that response processes are practical, rehearsed and capable of containing and recovering from an incident within hours, not days.

Regularly test and refine response measures through structured simulations and recovery exercises. These should include board-level tabletop exercises involving managing partners, verification of backup integrity and full restoration testing. Untested plans create avoidable exposure. When response is rehearsed and recovery proven, downtime reduces, client disruption is limited and confidence increases.

## 3. Identity Control Is the First Line of Defence

When a fee earner's credentials are compromised and used to access privileged correspondence, the breach is not just technical - it becomes a professional conduct issue.

Microsoft continues to report that most breaches involve compromised identities. Weak authentication remains one of the easiest paths into a network. In a profession built on people, identity security is critical because human behaviour remains a primary attack vector.

Multi-factor authentication should be standard across all systems without exception. Access should be tightly governed, over-privileged accounts identified and corrected and departing partners or staff removed promptly. Apply Zero Trust principles to reduce exposure, limit lateral movement and protect sensitive matter data. Identity must be treated as a continuously monitored control point, not a one-off configuration.

## 4. Secure Every Device

A partner reviewing documents from home on a personal device, or a solicitor working on a transaction over public Wi-Fi, can unintentionally extend the firm's attack surface.

Lawyers work across multiple devices and locations, often using home networks or personal equipment. This expands the attack surface and increases risk around privileged correspondence, deal rooms and litigation bundles.

Traditional antivirus is no longer sufficient. Firms require modern detection and response capabilities that identify ransomware, credential theft and suspicious behaviour early, wherever a device is located. In Microsoft environments, Defender for Endpoint, Intune and Entra ID work together to enforce consistent controls across identities, devices and data without disrupting productivity.

## 5. Lock Down Email and Collaboration

A fraudulent completion statement sent at the right moment in a property transaction can move client funds within minutes, breaking a house purchase chain and diverting a deposit to a criminal account instead of the intended bank.

After identity, email and collaboration platforms remain the most common entry points for social engineering. Business Email Compromise, fraudulent completion statements and invoice redirection scams continue to affect conveyancing and corporate transactions.

Because these tools sit at the centre of legal work, they require both robust technology and informed people. End-user awareness training remains essential, particularly for staff handling client funds or sensitive data. Technical controls must operate continuously in the background. Microsoft Defender for Office 365 blocks phishing and malware, Sentinel flags unusual patterns and Purview supports Data Loss Prevention, classification and controlled sharing.

## 6. Build Data Governance That Reflects Legal Reality

When sensitive merger documents are overshared or retained long after a matter closes, the exposure is not just regulatory - it can undermine client trust.

Client information is the lifeblood of a law firm. Protecting it is non-negotiable and must align with confidentiality obligations, GDPR, SRA standards and insurer expectations.

Effective governance includes classification, access control and disciplined retention. Legacy matter archives and unmanaged data stores increase exposure and inflate breach impact. Microsoft Purview can classify documents automatically and enforce policies that restrict sharing and reduce accidental disclosure. Technology must be matched with process and culture, including regular data reviews and clear retention policies. When governance reflects how lawyers actually work, firms reduce risk and demonstrate accountability.

## 7. Put Guardrails Around AI Use

If a fee earner pastes privileged advice into a public AI tool to "sense check" drafting, the risk is immediate and potentially irrecoverable.

AI can amplify existing weaknesses. Over-privileged accounts, poor classification and unmanaged devices become higher-impact risks when AI tools are layered on top.

Governance must separate firm-sanctioned AI from consumer AI platforms. Clear policies should address prompt hygiene, client confidentiality and the risk of inadvertent disclosure of privileged information. Clients are increasingly asking whether public AI models are being used in the delivery of legal services. Guardrails must therefore cover both technical and reputational risk. Microsoft Security Copilot can accelerate investigation and mitigation but it must sit within a controlled, well-governed environment.

## 8. Manage Cloud Apps, Third Parties and Data Sprawl

When an outsourced e-disclosure provider or SaaS legal platform suffers a breach, clients will still look to your firm for answers.

As firms adopt cloud platforms and specialist legal SaaS tools, sensitive data spreads across drives, collaboration spaces and third-party systems. Each integration creates another potential exposure point.

Supply chain risk is now a material concern. A breach in an outsourced provider can quickly become your problem. Apply Zero Trust principles, strong identity governance and continuous monitoring across internal and external environments. Use classification so protection follows information wherever it travels. Periodically retire unused workspaces, review third-party integrations and assess supplier security posture. This reduces blind spots and strengthens compliance.

## 9. Ensure Continuous Threat Detection and Response

An attack that begins at 02:00 on a Sunday will not wait until your IT provider opens on Monday morning.

Cyber threats do not keep office hours. For most small to mid-sized law firms, building an in-house 24×7×365 Security Operations Centre is unrealistic.

A Managed eXtended Detection and Response service such as secure365® from Softwerx provides continuous monitoring and automated containment using native Microsoft Security technologies. This approach delivers predictable operational expenditure, scalable protection and consistent response capability. Governance oversight remains with the firm but operational vigilance is maintained around the clock.

## 10. Build Trust Through Demonstrable Security

When a major client issues a 200-question security assessment as part of a tender, reassurance alone will not secure the work.

In legal services, security underpins every client relationship. Regulators, insurers and panel clients expect evidence of cyber hygiene, monitoring maturity and incident readiness through structured reporting, not verbal assurance.

Microsoft Defender XDR and Sentinel provide telemetry and analytics to evidence real-time detection and response. Combined with Purview controls and managed 24×7×365 operations such as secure365, firms can demonstrate measurable resilience. This evidence supports client tenders, panel reviews and indemnity renewals, shifting conversations from reassurance to substantiated assurance.

## And Number 11 of 10 – Don't Forget the Front Door

Confidential bundles left in a taxi or an unauthorised visitor tailgating into the office can undo even the most sophisticated cyber controls.

The strongest cyber controls are undermined if physical security is weak. Smart cards, office access, home printing, document disposal and tailgating risks must be treated as part of the same discipline. Digital and physical controls should operate as one joined framework to safeguard clients, people and the firm.

## The Bottom Line for Legal Leadership

Cyber resilience is not about buying more tools. It is about governing what you have properly, aligning it to legal risk and pairing it with continuous monitoring and response.

The firms that will remain trusted in 2026 will detect threats early, contain incidents professionally and demonstrate control under scrutiny from clients, regulators and insurers alike.

Want help applying this checklist to your Microsoft Security environment? Softwerx can identify gaps and implement enterprise-class 24×7×365 Managed XDR monitoring with secure365.

# 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