azured

5 things IT leaders in the legal sector should know about cloud security.

If you're an IT leader working in the legal sector, chances are you're probably feeling pretty overwhelmed right now. The constant threat of cyber-attacks, the rise of hybrid and home working, increasing demands from digital-savvy clients, rigid compliance requirements, and an open letter from the Solicitor's Regulation Authority (SRA), have put immense strain on the industry – and those working within it.

With the UK legal sector being such an attractive target for cyber attackers, we look at how working in the cloud can improve the security and efficiency of businesses.

A **2020 review by the SRA** found that for firms who had been the victim of a cyber-attack, the results "were often catastrophic", with the National Cyber Security Centre's (NCSC) report on cybersecurity in the UK legal sector reporting that more than **£11million of client money was stolen by cybercriminals.**

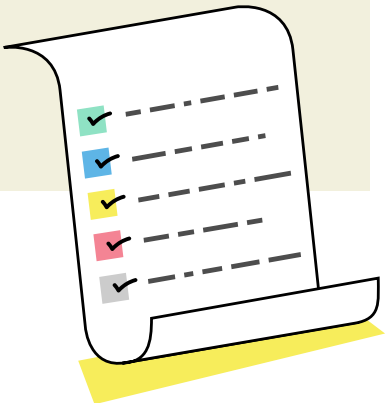
The pressure is on. **Workloads are increasing and increasing in complexity**, and the worker demographic is changing, with younger 'tech savvy' staff entering in to the legal industry with an expectation of what the modern workplace looks like. And while absolutely necessary to thrive in the modern workplace, tech savvy staff are almost pointless if the technology isn't there to support them. The Law Society believe the "movement to the cloud will act as a **competitive advantage for law firms looking to improve security, accessibility, and collaboration".**

Different **legal businesses will all be at different stages in their journey to cloud-based working.** The **Law Society report** that collaboration tools, document management, e-billing and IP management have been largely adopted, and that areas of growth include legal analytics, legal project management, governance and compliance, and contract management. While the larger, more mature law firms are already adopting AI and machine learning. But if AI seems a far cry from where you are right now, don't be alarmed!

Wherever your business is on its journey to cloud adoption, we know that IT leaders in the UK legal sector are facing some big challenges.

Top five things IT leaders in the legal sector should know about improving their cloud security:

1. Implementing secure home and hybrid working practices
2. Meeting the requirements of SRA and GDPR compliance
3. Meeting the digital expectations of clients
4. The growing sophistication and level of cyber attacks
5. Varying levels of awareness and confidence around new technology



azured

1. Implementing secure home and hybrid working practices.

As a sector slow to embrace cloud technology, the reason often cited is concerns over security. Partners, directors and employees needing to access documents, calendars and business-critical apps in and away from the office – with office staff also needing to access those very same documents, calendars and business-critical apps. But of course, this just isn't any old data. This is important, highly confidential data entrusted to you to care for.

It's easy to see that any potential gaps in your security (of which there could be many), whether that's down to devices, data, apps, or networks – accessed at home and in the office, could be financially and reputationally catastrophic.

Enter cloud security. Modern cloud security is pretty serious stuff – in fact, Microsoft are so serious about it that they've even **published guidance specifically for the legal sector.** So, it's fair to say they know a thing or two about keeping legal organisations working securely in the cloud – including modern cloud security features like **strong encryption,** third-party verification, **data loss prevention**, **intrusion detection** and rapid response.

Securing data in the cloud

Storing large volumes of data for long periods of time is standard for any legal business. The sheer volume can feel overwhelming and, with high server and data storage costs, expensive too. But, once all that data is stored, processed and managed correctly in the cloud, everything else becomes much easier – and easier on the purse strings (this might be a good opportunity to earn some points from the finance department).

Network security in the cloud

When the office was kept in the office, life was a much simpler time. A secure network that everyone joined at 9am and left at 5pm (if you were one of the lucky ones). But now even a small team will spend their time on the office network and, potentially, multiple unsecured public and home networks in a single day. The opportunity for a weakness in the security is almost inevitable.

Once a cybercriminal has gained access to an unsecured network, they can attack every other device connected to that network. On unsecured public WiFi, for example, a hacker can slide in between a device and the network – so the innocent victim unwillingly passes all their data to the hacker, no questions asked. Suddenly sending a quick work email via the wi-fi at your local coffee house doesn't sound so appealing…

Securing devices in the cloud

In the chain of cloud security, the device (of which there are many millions in the world), is often the weakest link. So much can go wrong. Out of date software and operating systems, inadequate protection...user error, perhaps? In fact, **85 percent of security breaches involve the human touch.** This often happens when someone in the organisation doesn't know the difference between a legitimate email and a phishing email. And from here, it can all go very wrong, very quickly. Compliance, anyone?

Bring-Your-Own-Device (BYOD) is fraught with security issues, like insufficient visibility and control. But, of course, lots of organisations will be encouraging staff to use their own devices – which is a particular problem when **67% of security professionals say remote workers using their own mobile devices has decreased their organisations' security posture.**

azured

2. Compliance in the Cloud

Compliance with the Solicitors Regulation Authority (SRA) and General Data Protection Regulation (GDPR) is absolutely crucial – yet generally touted to be a rather unfortunate and painstaking task. But with the right tools and applications, working in the cloud can make it easier.

SRA compliance for legal teams working in the cloud

The SRA have published a list of **compliance tips for solicitors.** It's comprehensive, practical advice – and a great place to start if you're unsure about any aspect of compliance. Their guidance covers:

- appropriate leadership and oversight
- undertaking risk and impact assessments
- creating policies and procedures
- undertaking training and awareness
- monitoring and evaluating the impact of technology

GDPR for legal teams working in the cloud

According to the **Information Commissioner's Office** (ICO), data security incidents occur when organisations don't have the "appropriate technical or organisational measures" to protect the personal data they hold. This is a requirement of the **GDPR Principle (f): Integrity and confidentiality (security).** Personal data is big business for legal firms in the UK. And failing to meet GDPR requirements means big problems.

Organisations are also required to **report breaches within 72 hours of discovery** under Article 33 of the GDPR. Of course, if it takes 72 hours to discover, there's a whole lot of damage that could be done (potentially irreversibly).

Cyber Essentials for the legal sector

Working to an industry-standard like Cyber Essentials, as a minimum benchmark in cybersecurity, can really alleviate a lot of the pain that comes with managing and mitigating risk and compliance in the cloud. **Cyber Essentials is a UK Government backed scheme** that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.

Cyber insurance for the legal sector

The Federation of Small Business reported that **38% of small businesses with cyber insurance don't actually know what their policy includes.** Which, if you ask us, has disaster written all over it… take the time to take it seriously. If you don't know your policy inside out, have a chat with someone who does. If they enjoy talking about cyber insurance policies as much as we enjoy talking about tech, you're probably in safe hands.

In August 2022 the SRA **revised its minimum terms and conditions for solicitors' professional indemnity insurance (PII)** – to explicitly exclude first-party losses that result from a cyber attack, i.e. those affecting the firm rather than clients. This is a big step-change, with even more responsibility piled on to the folk over in IT.

As former **Law Society president, I. Stephanie Boyce, says,** "Protection and prevention should be a firm's priorities to guard against damaging cyber attacks. Insurance is not a substitute for good protection, but an additional safeguard to cover certain costs and losses in the event of a cyber-attack."

azured

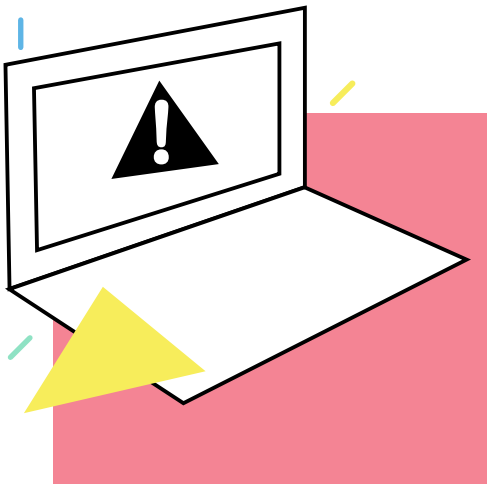
3. Meeting client's digital expectations.

Compared to other sectors, the legal sector has been slow to embrace and adopt cloud technology – and it hasn't gone unnoticed. Indeed, when customers are sending you encrypted files and you're printing them off and chucking them through the fax machine to leave on someone's desk, the security cracks begin to appear…

Technology adoption research by The Law Society revealed an **increasing pressure for UK firms to use or enhance the use of technology to improve efficiency.**

Clients are often drivers to change – and it's no different in the legal space either. Law firms will have clients who have undergone digital transformation projects spanning many months or years. They've been educated in the modern working environment and know what is possible in the world of slick, secure cloud experiences. They've had a taste of the good stuff. Forcing clients to login to outdated systems with unsecured login details isn't the best way to keep your now tech-savvy clients on the books. We've seen government-approved legal businesses with unsecured websites. So it does happen, but it doesn't make it right.

azured



4. The growing sophistication and level of cyber attacks.

The UK cyber threat report by the Law Society and the NCSC identified four key cyberthreats to the legal sector: ransomware, phishing, data breaches, and supply chain compromise.

Ransomware

Ransomware is a form of malware that prevents victims accessing their files or data until a ransom has been paid. Ransomware is the biggest online threat to UK businesses – and the legal sector appears to be very attractive to hackers that excel in this particular line of cybersecurity. It's important to note here that the cybercrime industry is a professional one – any images of hackers in hoodies should be replaced with suits, boots and a Board of Directors.

In July 2022, the National Cybersecurity Centre (NCSC) and the Information Commissioner's Officer (ICO) wrote to the Law Society asking them to "remind solicitors that the payment of a ransom won't keep data safe or be viewed by the ICO as a mitigation." This follows a massive rise in the increase of ransomware payments made by solicitors (and in some cases, their clients). Whether it's naivety or lack of knowledge, when you get a letter from the NCSC and ICO, it's time to buckle up.

Phishing

Phishing is where an attacker takes on the role of a trusted identity and tricks employees into opening emails, texts or instant messages. For UK businesses in 2021, phishing was responsible for 83% of cyber attacks. Exchange Online Protection, Microsoft 365 Defender and Microsoft Defender SmartScreen can all help protect legal businesses against the threat of phishing attacks. Of course it needs to be configured and deployed correctly – but that's for another day.

Data breaches

Data breaches through theft of data and hacking of office or client accounts are also on the Law Society's list of cybersecurity concerns.

According to data and analysis from the Information Commissioner's Office (ICO) and NetDocuments over two thirds of data breaches at UK legal firms were, for want of a better phrase, an inside job. The 2021 data identified 68% of data breaches in the UK legal sector (those where the origin could be identified) were caused by insiders – with 32% caused by malicious actors on the outside.

- 52% of data breaches in the legal sector occurred from sharing data with the wrong person (via email, post or verbally).
- 25% of data breaches in the legal sector occurred from phishing attacks.
- 10% of data breaches occurred from losing data (i.e., loss/theft of device containing personal data, or of paperwork or data left in insecure location).

Supply chain compromise

Notoriously difficult to spot (especially if you don't really know what you're looking for), supply chain attacks are on the rise by a massive 430%. Supply chain attacks target a trusted third-party supplier or vendor who offers services or software vital to the supply chain.

CrowdStrike's 2021 Global Security Attitude Survey of 2,200 IT decision-makers found that:

- 84% believe that software supply chain attacks could become one of the biggest cyber threats.
- 45% experienced at least one software supply chain attack in the last 12 months, compared to 32% in 2018.
- 59% that suffered their first software supply chain attack didn't have a response strategy.

azured

5. Varying levels of awareness and confidence around new technology.

As previously mentioned, **52% of data breaches in the legal sector occurred from sharing data with the wrong person.** There's always a small margin for human error... but this figure is too high given the sensitive nature of the data that we're talking about.

Of course, this is just one example – but with the right education to the right people, teams can work securely in the cloud. And as we know, with knowledge comes great power. Educating and empowering teams to embrace and feel confident using new tech should sit at the heart of any IT project. Creating a culture of honesty and transparency where identity and access management is implemented across the organisation, and teams are able to raise security concerns before they arise, will be crucial for any business and its data.

How Azured can help legal teams embrace the cloud:

- Identity and access management
- Architecture and configuration
- Risk management
- Engagement and training
- Asset management
- Vulnerability management
- Data security
- Logging and monitoring
- Incident management
- Supplier security

azured

So, to recap, here are our top five things IT leaders in the legal sector should know about improving their cloud security:

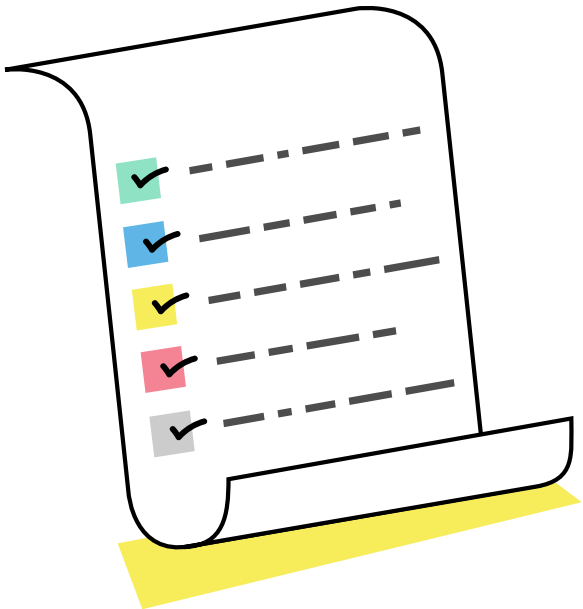
1. Secure home and office working practices across devices, data and networks.
2. Work to an industry-standard security benchmark to reduce the burden of compliance.
3. Embrace new cloud-based technology to improve efficiency of teams, and relationships with clients.
4. Take proactive steps to reduce the risk of attacks, including phishing, data breaches, ransomware and supply chain compromise.
5. Educate (non-tech) teams to increase awareness and confidence for staff using new cloud-based tech.

Cloud security for the legal sector

If you have either one or both feet in the cloud, and think we can help improve your security posture, please consider our baseline security review as a first step.

Know your phishing from your ransomware? **Download our free guide to cloud identity and access management in the cloud to find out more.**

Confused by the mirage of tech-speak? Head over to our **A-Z of cloud security.**



azured

azured

Azured UK Ltd
www.azureduk.com
hello@azureduk.com