VansonBourne

Rethinking SaaS resilience in the legal sector

Research Report

The legal sector is embracing a bold digital transformation, with many rapidly moving to cloud-based SaaS platforms run by Independent Software Vendors (ISVs), like iManage Cloud, Microsoft 365, and DocuSign. In the US, the percentage of attorneys using cloud computing for work-related tasks has jumped **from 60% in 2021 to 75% in 2024**. In the UK, nearly **two-thirds (64%)** of law firm leaders expect their core business systems to run entirely in the cloud by 2027.

But as firms shift away from legacy infrastructure, many overlook a critical reality: ISVs provide availability—not recoverability. Under the **Shared Responsibility Model**, firms are responsible for their own data. Yet **85%** of business and professional services' IT leaders are unaware of this, mistakenly believing that their native SaaS tools provide sufficient data protection (Vanson Bourne, 2025). Without the appropriate safeguards in place, firms are left vulnerable to cyberattacks, insider threats, accidental deletion, and even supply chain compromise. All of which have severe consequences.

In this paper, we explore why SaaS adoption is outpacing the legal sector's preparedness for data disruption, and how low awareness of the Shared Responsibility Model is exposing firms to serious but avoidable operational, reputational, and regulatory risk. Through real-world data we'll explain what protection is essential, and how to ensure your cloud-first future is secure, complaint, and under your control.

Percentage of US attorneys using cloud computing for work-related tasks

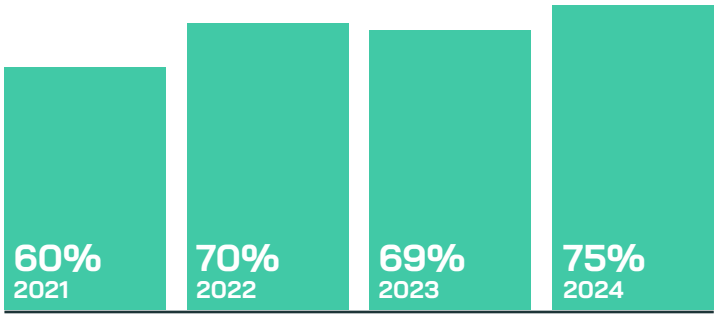


Figure 1. Cloud computing in modern legal practice, 2024 ABA Legal Technology Survey

The evolving landscape of legal infrastructure

With global **SaaS revenues reaching $218.5 billion in 2024**, it's no surprise that SaaS now dominates the modern workplace tech stack. In fact, **Business and Professional Service firms use an average of 99 SaaS applications today** (Vanson Bourne, 2025), with **72% of firms using Microsoft 365 (OneDrive) and 54% leveraging Dropbox**. Amongst other apps such as iManage Cloud, DocuSign and Atlassian Cloud, SaaS is readily becoming the digital foundation of modern casework.

The rise of SaaS in the legal sector has not been driven by enthusiasm, but by inevitability. As ISVs pursue scalable cloud-first delivery models, law firms are being steered towards platforms that offer convenience and remote access, but also demand an evolved approach to data sovereignty and protection. However, many have yet to recognize this need, with **85%** of ITDMs in business and professional services organizations believing that **native SaaS tools are sufficient for data protection** (Vanson Bourne, 2025).

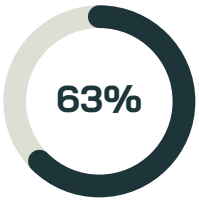
This misconception leaves firms dangerously exposed, over-relying on embedded features such as recycle bins or version histories to protect critical data, and unaware that in the event of a deletion, corruption, or attack, the responsibility for protecting or restoring data rests squarely with the firm themselves.

> *With all of the lessons learned that people have seen over the years between disasters, having multiple copies of that data on multiple mediums, including some sort of Backup outside of the software solution at hand is critically important.*
>
> Will Fulmer, Chief Technology Officer, Helient Technologies LLC.

Cloud growth outpacing security

For now, the pace of SaaS adoption continues to outstrip firms' ability to secure it, with hackers increasingly drawn to the legal sector for the high-value rewards that come with access to privileged, case-critical information. Unfortunately, these attacks are no longer rare or speculative.

- In the US, Ransomware attacks on law firms rose by **30% in Q1 2024**, with average ransom demands now **exceeding $500,000**.



of business and professional services ITDMs report having experienced a security breach involving SaaS application data within the last 12 months (Vanson Bourne, 2025).

The rising risk of a data compromise

The risk from ISVs is also growing rapidly across industries. In 2024, **36% of data breaches were linked to third-party vendors, marking a 6.5% increase from the previous year**. These risks aren't limited to configuration errors or weak integrations either. Attackers are directly targeting SaaS providers and cloud platforms, with UK law firm **cyberattacks surging by 77% in just one year**, according to Lubbock Fine. External vendor risks are also only half the picture. ICO data from 2022 to 2025 shows that, on average, **60% of data breaches in the UK legal sector stem from internal, non-cyber incidents**, including accidental alterations or misdirected communications.

> *All of these cloud providers, whether it be a Microsoft…or anybody else out there, no one is immune to…potentially malicious actors out there.*
>
> Will Fulmer, Chief Technology Officer, Helient Technologies LLC.

Critically, the response to these rising threats are far from immediate. Gartner predicts that **it will take until 2028 for 75% of enterprises to make SaaS backups a critical requirement**. For now, many appear to overestimate the data protection capabilities of cloud-based tools, with **one in three (33%)** law firm leaders citing data security as a key reason for moving to the cloud, a sign of misunderstood responsibility.

The mechanics of the problem

In legal practice, **regulatory frameworks such as the GDPR, NIS2, and HIPAA demand not only strong data governance, but clear disaster recovery and business continuity plans**. As highlighted by global law firm Clyde & Co, regulations such as DORA – primarily aimed at financial institutions – go further by holding ICT providers accountable for operational resilience. This marks a broader regulatory shift from aspirational policy to enforceable accountability across interconnected service ecosystems. For legal firms, especially those advising regulated industries or reliant on third-party platforms, this underscores a vital learning: **safeguarding data is no longer just an IT concern, it is a matter of professional integrity**.

However, the more ISVs a law firm relies on, the more exposed it becomes. The *Shared Responsibility Model* compounds this risk by dividing responsibility between provider and customer, creating a dangerous data protection gap if customers do not take data protection into their own hands.

- **Here's how Microsoft addresses this model in their policy: *"For all cloud deployment types, you own your data and identities. You're responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control."***

By aligning data protection and recovery strategies, law firms can contain disruption and avoid costly consequences. In the UK, **the ICO can issue fines up to 4% of global turnover, or £17.5 million, for mishandling client data**. According to IBM, the impact of a breach is also significant, with professional services **firms facing an average breach cost of $5.08 million, exceeding the global average of $4.88 million**. To meet rising compliance standards and ensure continuity, legal IT leaders must adopt a resilient and unified SaaS-ready data protection strategy that safeguards client trust and strengthens firm-wide resilience.

Methodology

The legal and professional services research was conducted by independent research firm Vanson Bourne as part of the soon-to-publish, "State of SaaS Resilience 2025" study. More than 500 global IT decision-makers were surveyed, including 40 from the legal and professional services sector.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit www.vansonbourne.com

About HYCU

HYCU is the fastest-growing leader in the multi-cloud and SaaS data protection as a service industry. By bringing true SaaS-based data backup and recovery to on-premises, cloud-native, and SaaS IT environments, the company provides unrivaled data protection, migration, disaster recovery, and ransomware protection to thousands of companies worldwide. The company's award-winning R-Cloud platform eliminates complexity, risk, and the high cost of legacy-based solutions, providing data protection simplicity to make it the#1 SaaS Data Protection platform. With an industry leading NPS score of 91, HYCU has raised $140M in VC funding to date and is based in Boston, Mass.

Learn more at: www.hycu.com