CYBERREADY
The Human Readiness Company

Confidentiality Fortified:

Cyber Resilience for Legal Guardians

The practice of law has always played a key role in technology innovation, from issuing patents to facilitating high-profile data protection lawsuits. While the tech industry would not exist without law as its partner, the law industry doesn't return the favor with such vigor.

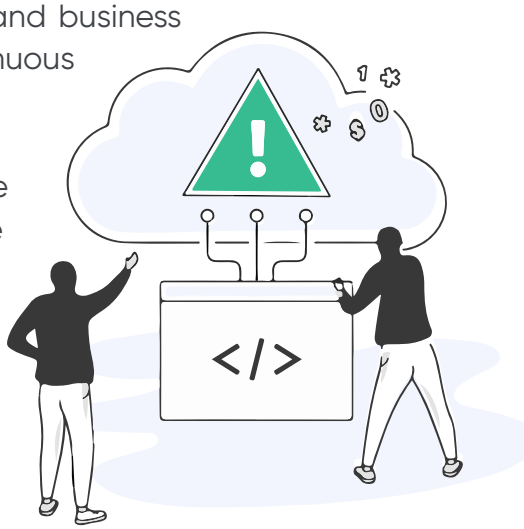
Legal firms are adopting cloud technology at a slower pace than other industries. But despite being risk-averse, they clearly see the ***benefits of scalability, flexibility, and cost reduction.***

Unfortunately, in 2023, **one in forty law firms** faced a ransomware attack in which hackers held confidential client information under siege. Client confidentiality is the center of the universe in the legal industry— and even though the cloud offers built-in security features, ***the possible data privacy and security risks linger in law firms' minds.***

The challenge is to ensure that technological adoption does not compromise the sacrosanct duty of protecting the client and their information by any means possible.

The Push Towards Cloud Adoption in Legal Practices

Despite legal firms' trepidation, digital transformation is accelerating, and **cloud migration** is steaming ahead. ***Over 90% of organizations already use cloud computing, and the security benefits are clear.*** Most cloud vendors provide built-in security and business continuity features like encryption, automatic backup, MFA, continuous monitoring, and robust disaster recovery.



The security benefits for law firms align with modern workflows. The rise of ***hybrid working*** has increased the need for collaborative work environments in which legal software and documents are accessible via cloud-based systems. For example, case management software provides client updates and file management on demand, helping legal teams improve productivity through enhanced collaboration.

Similarly, cloud-based software supports organizations in meeting the requirements of tech-savvy clients and fostering better client engagement. Cloud platforms like cloud intake tools and document management software enable legal teams to provide clients with secure access to documents, portals, automated forms, and virtual lawyer services.

When all the benefits of cloud computing are tallied, it becomes clear that on-premises infrastructure ***no longer meets the growth requirements of modern law firms.*** More efficient and flexible collaboration between teams helps law firms overcome headwinds and hurdles in expansion.

The standout feature of the cloud is the ability to work from anywhere, which also enables lawyers to eliminate physical barriers to clients. Local practices can expand regionally, or personal injury lawyers can visit clients in hospitals.
So, why are law firms still nervous to dip their toes into cloud computing?

The Paramount Importance of Client Confidentiality

Client confidentiality is the fundamental pillar on which the practice of law is built. In addition to the industry-wide ethical obligations, there are now **data privacy laws** to consider, such as GDPR and CCPA. All businesses are concerned with data breaches, but the stakes are even higher when your duty to protect client information is centuries old.

The legal industry must learn that **cloud security** can sufficiently and efficiently protect customer data. Yet, despite the positive outlook, complexities remain when it comes to cloud adoption in law. For example, international and expanding law firms must understand how data privacy laws differ between geographical locations and whether they can store data overseas.

The Threat Landscape: Phishing Attacks and Cloud Vulnerabilities

The lock-and-key confidentiality of legal data makes it a hot target for hackers. Data managed and stored by law firms can encompass contact information, medical data, and personal characteristics. Information and documents from high-profile cases are the ultimate trophies for cybercriminals—because they can sell and leak this data to media outlets for lucrative prices.

Despite the slow adoption of cloud technologies, law firms must prioritize phishing protection measures before, during, and after the cloud migration process.

Law firms might expect a barrage of phishing threats, including:

Email phishing: Bad actors will send an email to employees that appear to have come from senior management, such as a high-ranking partner.

Malicious links and attachments: A single legal case can incur thousands of documents. In the flood of digital paperwork, receiving a malicious attachment from a colleague wouldn't draw suspicion, and employees will likely open it without scrutiny.

Spear phishing: In spear phishing attacks, hackers target victims with a personalized approach. For example, they might contact a paralegal claiming to be the client, asking for an update on their case.

Whaling: Sometimes called 'CEO fraud,' whaling attacks aim to trick high-ranking partners in the firm into urgent action, such as approving a fraudulent payment for the 'accounts department.

Deepfakes: AI makes phishing attacks alarmingly realistic, which is especially dangerous in law firms that rely on video or phone calls to identify clients. A hacker could easily use deepfake technology to replicate the client's voice or likeness.

Any data breach has reputational, financial, and legal consequences, not to mention the threats to business continuity. In a law firm, there is another layer to the reputational damage because any leaked data instantly breaks the ancient principle of client confidentiality. In that case, clients' loss of trust in the firm will be two-fold: They will be frustrated by the data breach—and feel betrayed by the disruption to attorney-client privilege.

How to Fortify Law Firms Against Cyber Threats

Many cloud vendors automate security, which helps the legal industry meet compliance and data privacy obligations. While law firms can trust vendors to do some of the legwork for them when it comes to protecting data, there is one critical area that cloud vendors cannot control: Employees.

As the legal industry makes the cloud migration leap, firms need to understand their unique security gaps. Law firms must take steps to mitigate easily avoidable phishing attacks by focusing on the identification and avoidance of scams.

Senior management, such as high-ranking partners and the C-suite, must factor staff-wide cybersecurity awareness training into their defense arsenal to help everyone do their part to protect client data. This builds a robust human firewall that boosts data security and enhances client confidentiality.

Our Solution

CybeReady's innovative approach leads you to achieve an exceptional combination of risk reduction, engaging learning experience, and cultural impact while addressing compliance challenges. This is facilitated through our SaaS platform, which runs a comprehensive awareness training program ensuring effectiveness.

Book a demo today to discover how CybeReady can fortify your law firm's data defenses while moving to the cloud and beyond.

info@cybeready.com | www.CybeReady.com