Progress® ShareFile®

Modern Data Security for Small and Mid-Sized Law Firms

E-BOOK

A Guide to Safeguarding Your Clients' and Your Firm's Data with Secure Document Sharing

Law firms are increasingly turning to document workflow technology to streamline the creation, management and collaboration of legal documents. These solutions automate repetitive tasks—such as drafting, approvals and filing—enabling teams to produce documents faster, with fewer errors and less administrative overhead.

While increasing the use of document workflow technology offers clear operational and business gains, it also introduces a new set of security considerations.

Law firms are prime targets for cybercriminals—not just because they handle sensitive data, but because they're frequently targeted. Since 2018, there have been 138 publicly confirmed ransomware attacks on law firms globally, resulting in exposure of over 2.9 million records. In 2023 alone, 45 attacks were reported. The threat landscape continues to evolve—even as the pressure to digitize accelerates.

Despite this, many firms, especially small and mid-size ones, still aren't implementing the necessary security precautions. In the ABA 2022 Legal Technology Survey, only 40% reported using any standard cybersecurity practices—and almost one in five revealed they employed no security measures at all.

The good news is that small to mid-size firms can safeguard documents and the sensitive information they contain if they choose a platform wisely. To effectively safeguard firm and client information, it's essential to choose a document workflow solution with integrated security features that work—whether there's a dedicated IT team in place or not.

In this eBook, we'll clarify essential features that document workflow tools must have to help secure your firm and client data, as well as strengthen your firm's overall security posture.

Why Document Security Matters

Legal teams are responsible for gathering, sharing and securing thousands of legal documents. But without the proper support from document workflow technology, they could face risks:

- Law firms store large volumes of highly sensitive client and case data—making them a prime target for hackers seeking valuable information.
- Non-secure file sharing practices by users can inadvertently expose the firm to data breaches and unauthorized disclosures.
- Unauthorized access to documents not only jeopardizes client confidentiality but can also result in regulatory violations and compliance penalties.
- Relying on third-party platforms introduces additional risk, as vulnerabilities in those systems can directly impact the firm's security posture.

Given their exposure to cyberattacks, how can they use document workflow technology to support safe exchanges of files and information?

"The continuing lack of attention to confidentiality, security, and due diligence issues remains a serious and disturbing concern."

2022 American Bar Association Cloud Computing Report, Legal
Technology Survey

Many law firms are adopting document workflow technologies to boost revenues and better respond to the increasing online demands of both courts and clients. These solutions give legal teams a fast, scalable way to leverage the latest technology tools without the need for substantial upfront capital investment. Plus, they value having anytime, anywhere access to their data, predictable monthly expenses and reliable data backup.

Law firms are prime targets for cybercriminals—not just because they handle sensitive data, but because they're frequently targeted. Since 2018, there have been 138 publicly confirmed ransomware attacks on law firms globally, resulting in exposure of over 2.9 million records. In 2023 alone, 45 attacks were reported. The threat landscape continues to evolve—even as the pressure to digitize accelerates.

Despite evident warning signs, many firms, especially small and mid-size ones, still aren't implementing the necessary security precautions. In the ABA 2022 Legal Technology Survey, only 40% reported using any standard cybersecurity practices—and almost one in five revealed they employed no security measures at all.

Law firms often assume that strong security requires enterprise-level IT resources. Others simply underestimate their risk or believe comprehensive protection is out of reach. In many cases, smaller firms don't even realize their current security measures fall short. But in reality, even small firms handle highly sensitive data and face the same threats as large organizations. To effectively safeguard firm and client information, it's essential to choose a document workflow solution with integrated security features that work—whether there's a dedicated IT team in place or not. Legal teams are responsible for gathering, sharing and securing thousands of legal documents. Given their exposure to cyberattacks, why are some failing to take the proper steps to secure sensitive data? And just how safe are they from potential lawsuits themselves?

It's possible that law firms are selecting solutions without vetting them for the appropriate security features. Another reason could be that their existing tools don't include the necessary security features that employees can self-manage easily, without the need for robust IT.

In this eBook, we'll clarify essential features that document management and automation solutions must have to help secure your firm and client data, as well as strengthen your firm's overall security posture. It also offers a practical framework for you to compare different options and make a confident, informed purchase decision.

Three Impacts Resulting from Poor Docment-Sharing and Security Practice

1. Exposure to cyberattacks

Cybercriminals know that legal files often contain valuable data: financial records, Social Security numbers, patent specifications, M&A plans, personally identifiable information and more. Because of this target-rich environment, approximately one in every 40 cyberattacks is directed at the legal industry.

Attackers search for—and often find—weak links in a firm's document storage and sharing processes. Sadly, most weaknesses are due to human error.

For small and mid-sized firms without a dedicated IT team, those weak links can be:

- For small and mid-sized firms without a dedicated IT team, those weak links can be:
- Easy-to-guess passwords (such as Password123)
- Employees reusing the same password across multiple tools and platforms
- Employees keeping the same password for an extended period
- No multi-factor authentication to confirm that only authorized recipients are accessing the data
- Employees unknowingly engaging with phishing emails that compromise firm data

One in every 40 cyberattacks is now directed at the legal industry.

2. Reputation damage

Because of the potential damages and widespread publicity that often accompany a data breach, law firm clients are taking notice and taking action.

According to the 2025 Integris Law Firm Cybersecurity Report, 52% of firms say their clients have asked about their cybersecurity practices, and 8% have experienced a breach themselves. The risks aren't just hypothetical: 37% of clients said they would warn others about a firm's breach, and 39% would consider ending the relationship. In today's climate, cybersecurity transparency is a business necessity—not an optional investment.

3. Revenue loss

Once a firm becomes a cyberattack victim, the road to recovery is long and expensive.

According to IBM, in 2024, the average time (across all industries) to identify a data breach was over 200 days, and the average time to contain it was 70 days.

That's valuable time, effort and expense that legal and IT teams must spend on data recovery and remediation—time that should be spent on servicing clients and generating billable hours.

"The global average cost of a data breach [has] surged to $4.88 million."

IBM Cost of a Data Breach Report 2024

Three Key Capabilities Every Law Firm Needs to Safeguard Their Data

As cybercriminals deploy more sophisticated attacks using artificial intelligence, larger firms are turning to tools such as managed detection and response, SIEM systems and advanced identity and access management (IAM) solutions to protect themselves. However, smaller law firms typically don't have the same level of financial and technology resources available.

To help protect your firm and client data, smaller firms should invest in a document workflow technology that provides the following security capabilities:

1. **Secure document management controls** – Enables your firm employees—without IT involvement—to create security and sharing guidelines and permissions for clients and third parties to control who can view, edit and share data.

2. **Secured collaboration** – Safely transmits documents using encrypted files and email communication.

3. **Security threat alerts**—This feature provides real-time alerts when a security threat is detected so admins can respond swiftly.

Secure document management controls

Teams can also be geographically dispersed or operate in remote/hybrid work environments. Yet, they still need solutions that facilitate seamless access and the ability to exchange documents from anywhere. A chief concern among legal teams is accidentally sharing protected documents with opposing counsel or not redacting sensitive information within documents and correspondence.

Secure document management platforms provides an efficient process for protecting your information and allowing only authorized users access throughout a case.

Look for a platform that provides:

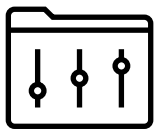
Strong password hygiene - Creates and sets guidelines for password complexity and periodic password changes (usually every 90 days) to allow access to authorized individuals.

Watermark features - Quickly applies unique identification marks to deter downloading and printing of sensitive documents.

Download restrictions and sign-in requirements - Restricts document sharing and viewing by limiting the number of individuals who can download and view documents.

Multi-factor authentication (MFA) - Enforces a second form of validation—such as text link or email authorization—to confirm that client documents are only accessed by your desired recipients.

Remote wipe - When laptops are stolen or misplaced, IT admins can quickly “lock” them or erase their data to prevent data theft or unauthorized access.



Secure communications and file storage - Automatically helps protect shared documents and email communications with AES-256 encryption—one of the most secure encryption algorithms available—without human involvement.

Secure collaboration

A strong legal strategy depends on effective client communication and collaboration. However, it can't jeopardize the security of your data. An effective solution provides the protection your organization and clients require without changing how people prefer to work.

Look for a platform that provides:

- **Sharing permissions and authentication –** Enables the setup of authentication access on a document level to control who can access, edit and share documents.
- **Use of links instead of email attachments –** Reduces restrictions imposed by email size limits and facilitates secure email practices.
- **Secure client portal -** Creates a single, secure location where everything related to a case—documents, communications, workflows, contacts, etc.—is stored and easily accessed by all authorized users.
- **Seamless co-editing -** Allows users to provide immediate feedback, edits and approvals within documents to eliminate the need for separate, unsecured email correspondence.
- **Secure data transfer -** Automatically encrypts documents and communications shared with clients and third parties.
- **Activity reporting -** Tracks legal workflow progress, assigns tasks and deadlines and monitors all document activity—including unauthorized or suspicious actions.

Security threat alerts

Security threat alerts notify your team of unauthorized document access or sign-in attempts. Look for a solution that provides:

Unusual sign-in threat alerts - Delivers real-time notifications of unauthorized access from suspicious devices or user locations, such as access from a foreign country.

Multiple failed sign-in alerts - Provides real-time alerts when a person or entity is making various attempts to gain unauthorized access.

Malware upload alerts – Helps block and alert you to malware uploads to prevent widespread damage or data loss.

The average daily cost of a data breach in the US is $8,640 per day.

Security threat alerts

Every law firm strives to put clients first—and part of that customer centricity is making every effort to safeguard their data. With ShareFile products, legal, small and mid-size firms finally have a secure, easy-to-use workflow solution that allows team members to streamline document-heavy workflows, enhance security protection and offer seamless client experiences—without compromises.

Discover how ShareFile software can give your firm:

- **Peace of mind –** Gives clients confidence that their content is secure from the initial exchange through project completion.
- **Proactive security –** Enables team members to quickly address security risks when handling client documents.
- **Threat identification –** Helps locate threats related to unusual access and malware uploads based on events.

Visit **ShareFile.com** to learn more.

About Progress Software

Progress Software (Nasdaq: PRGS) empowers organizations to achieve transformational success in the face of disruptive change. Our software enables our customers to develop, deploy and manage responsible AI-powered applications and digital experiences with agility and ease. Customers get a trusted provider in Progress, with the products, expertise and vision they need to succeed. Over 4 million developers and technologists at hundreds of thousands of enterprises depend on Progress. Learn more at www.progress.com

Worldwide Headquarters

Progress Software Corporation
15 Wayside Rd, Suite 400, Burlington, MA 01803, USA
Tel: +1-800-477-6473

facebook.com/progresssw
twitter.com/progresssw
youtube.com/progresssw
linkedin.com/company/progress-software
progress_sw_

Progress