TIP SHEET: FIVE SOLUTION FEATURES TO CONSIDER

Prioritize Document Control and Security

A law firm IT administrator needs to wear a lot of hats to be successful. Network maintenance, third-party vendor management, and data security are just a few of the responsibilities.

Data security is a common top priority due to the volume and nature of information that is handled during legal review. A workflow solution designed for document control and security can help law firms limit access to private client data without adding a lot of work to overwhelmed IT teams.

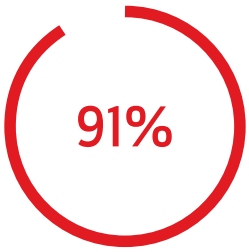
Choosing the right solution for your firm can be time-consuming. Here are five important features to consider when implementing a secure, easy-to-manage document control solution.

1. DOCUMENTS ARE STORED, MANAGED, AND ACCESSED WITHIN THE PERIMETERS OF A SECURE ECOSYSTEM.

Leverage a secure content ecosystem with regulated workflows, defined access perimeters, and comprehensive oversight. Authorized employees can access documents based on their assigned privileges, and content interactions should be logged for accountability. A comprehensive ecosystem should provide users with a means to securely interact with their clients' sensitive materials (even those that originate in paper form), minimize its productivity footprint, and give administrators workflow oversight and management controls.

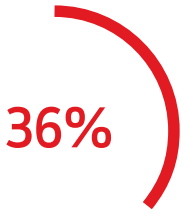
Security policies related to documents are common among law firms, and there are different solutions in the market. Not all of them meet the above criteria.

With the growing focus on cloud computing, extranets are a classic example of a secure cloud tool that can help clients collaborate on projects with external parties. While clients potentially benefits the most from extranets, they show the least amount of access to firms' projects:



Allow access to their lawyers

Allow access to their staff



Allow access to clients

Source: American Bar Association 2019 Cloud computing technology survey

2. EASY-TO-USE SECURITY FEATURES.

Technology, document-workflow solutions, and office equipment that has easy-to-use, built-in security features (such as badge scanners on printers) can help enhance security efforts because user compliance tends to be higher.

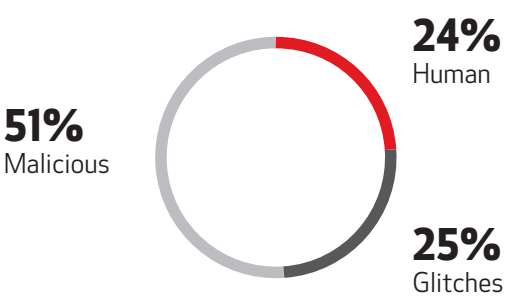
If security requirements are cumbersome—or there is no time or resources to train employees—people may be tempted to use less secure workarounds. It's especially important that office equipment has security features that are transparent to the user and are not distruptive.

A DATA BREACH COULD COST MORE THAN

$8.19 MILLION

average cost of breach of private data for U.S. organizations in 2019*

ROOT CAUSES OF A DATA BREACH IN 2018*



Source: 2019 cost of a data breach study by the - Ponemon Institute and IBM Security

3. FAST AND EXTENSIVE ACCOUNTABILITY.

Activist groups, disgruntled employees or clients, and cyber criminals have many means of accessing client information. They could take client documents from anywhere at any time: a desktop, a laptop, a mobile device, a table in a copier room, or during a file-sharing session.

An effective document management and security solution should provide quick access to details about a document, such as who accessed it last, what they did with it, and when.

Even if no private client information is in jeopardy, having fast and extensive document traceability can be an important capability for helping to limit accidental exposure because it can provide quick insight on what happened when a document is misfiled or missing.

TODAY'S TOP 10 CYBER SECURITY THREATS

In no particular order, here are today's top 10 threats:

1. Lack of Pervasive Security Mindset
2. Security Issues With Third Party Providers And Cloud Systems
3. Ransomware
4. Rogue Employees
5. Hactivists
6. Nation-State Espionage
7. Accidental Exposure By Well-Intentioned Employees
8. Technology Obsolescence
9. Password Management Being Weak Or Non-Existent
10. Reduced Security Standards For Remote Workers

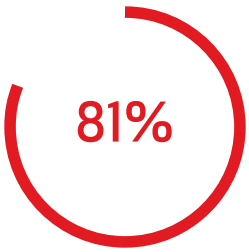
Source: Source: Logicforce, "Top 10 Law Firm Cyber Security Threats Right Now"

4. SECURE AUTHENTICATION FOR EXTERNAL ACCESS TO SENSITIVE CONTENT.

You can require user authentication when documents will leave or will be accessed from outside of the ecosystem; for example, when documents are shared with outside counsel and are viewed on a mobile device, or when copies are ready for output at a printer.

This can be a key capability as both clients and law partners expect on-the-go document accessibility as mobile device use increases.

SMARTPHONE USAGE IS EXPLODING



of Americans own smartphones

Source: Pew Research Center, "Mobile Fact Sheet"

5. LAW FIRMS' NEEDS TODAY AND TOMORROW.

In a new question in the 2019 survey, firm leaders were asked what they have done to effectively lead change in their firms. The two most effective tactics reported were to create a culture of collaboration at all levels in the firm and to put forward-looking leaders in key roles.

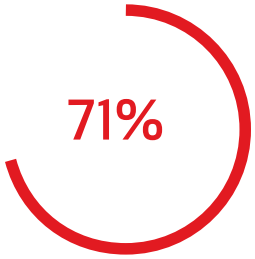
Finding a solution that can grow with a firm can minimize the need to change technologies as their needs change. Look for solutions that:

- Can integrate with existing hardware and software
- Can easily allow you to add new users and delete old users as needed
- Come with robust service and support
- Are easy for new users to learn without dedicated training
- Have a longstanding history of serving the legal vertical
- Have consistent user experience across device models

MORE USERS TO MONITOR AND TRAIN?

In the Altman Weil 2019 Law Firms in Transition Survey, they found:

of firms will pursue organic growth in 2019



of firms are looking to acquire groups in 2019

DOCUMENT SECURITY DOESN'T HAVE TO HURT.

IT administrators don't need to take on a painful project to help limit access to private client information. Easy-to-implement managed document workflow systems can provide a consolidated ecosystem for documents with a variety of security options that can be configured to align with firm security and compliance policies offer single-view visibility into what's happening with client documents and give control to IT or office administrators to help limit and manage document access and activities.

Learn how **Canon Solutions America** can help provide security surrounding your document management.

Canon
CANON SOLUTIONS AMERICA

1-800-815-4000 CSA.CANON.COM

01/19-1049-3910