SECURING CLIENT DATA IN A DIGITAL AGE

WHY DOCUMENTS ARE AT RISK,
AND WHAT YOU CAN DO ABOUT IT.

Law firms have many priorities to manage. Protection of client data should be at the top of the list. And even if it is already, document flow and management are not usually among the highest security priorities. They should be, because private client information in any document that law teams handle is at risk of exposure, a disaster that could harm a firm's reputation and cost millions of dollars to rectify.

New Threats Move Fast

Activist groups, disgruntled employees or clients, and cybercriminals have new means of accessing client information. They could be taking 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.

Lack of standardization, outdated equipment, and innocent mistakes can put law firms at risk of exposing client data when document creation, access, and flow aren't controlled and secured.

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

SIX TOP WAYS TO SECURE CLIENT DOCUMENTS

Every day, firms handle tremendous amounts of sensitive documents containing private client information. Those documents are created, uploaded, downloaded, shared, copied, printed, and filed. This fast-moving connection of workflows must be secured, but also organized and controlled for productive operations.

Here are six ways to help secure your document ecosystem:

1. CAPTURE NEW & INCOMING FILES

Ensure every incoming client document immediately enters the same document management system. Use an encryption method to protect documents when they are in digital storage or being transferred digitally.

2. USE INTEGRATED TECHNOLOGY

Use an integrated hardware-software solution for document management so that users can share information without leaving the secure ecosystem.

3. USE SECURE ACCESS CONTROL

Require user authentication at points in a workflow where documents will leave the secure ecosystem; for example, when documents are transferred via mobile file sharing.

4. EMBED ACTIVITY TRACKING AND REPORTING

Having visibility to active document workflows can enable monitoring for abnormal activity or unauthorized access.

5. PLAN FOR USER ENGAGEMENT

Security protocols should be intuitive and easy to follow to promote user adherence to firm policies, and can help reduce firm liabilities.

6. BALANCE ACCESS WITH SECURITY

A proactive approach to security involves a balance of document availability, confidentiality, and integrity, because a security plan should be aligned to business drivers and outcomes or it won't be effective.

LACK OF PREVENTION IS COSTLY

$8.19 MILLION

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

Take a Unified Approach

Securing and controlling document workflows doesn't have to slow down day-to-day operations or impede client services. In fact, solutions like uniFLOW from Canon can help enable firms to contribute to a secure document ecosystem by providing a consolidated platform for collecting documents and managing document output.

The reality is that many points of potential exposure exist in the life of any active client document. Having visibility and control of document workflow can help law firms reduce risk while continuing to provide clients with stellar service.

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

SOURCE: *2019 Cost of a Data Breach Study by the Ponemon Institute and IBM Security.*

Canon

CANON SOLUTIONS AMERICA

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

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