FIVE STEPS TO HELP AVOID WORST-CASE SCENARIOS

Law firms can't afford to have anything less than an urgent approach to protecting client data. A single case of unauthorized access to a file or page of notes could potentially cost a firm millions of dollars in recovery costs and incur a tarnished reputation. Managing data, however, is not just about security; it is also good for business. Understanding the nuances of how data flows through your law firm allows you to improve the client experience, streamline operations, and develop better business-winning outcomes. By helping your firm make document control a top priority, you can help mitigate risk and impact profits.

A good way to start the process is to create a team that can understand competing data needs within the firm and build consensus. Here are five actions to consider as you get started.

1. TO SECURE YOUR DATA, YOU NEED TO KNOW WHERE IT IS.

Review and document everything that happens with structured and unstructured data containing sensitive client information. This includes documents, videos, and photographs, as well as emails and texts, among others. Consider questions such as: *Where are they stored? How are they distributed? Are they indexed and classified? Are they secured while in use, in transit, or at rest? Who has access to them?* If you don't have a way of obtaining this information, talk to a professional familiar with document workflow security. This capability is beneficial in today's environment of increasing cybersecurity threats.

"DARK" DATA MAKES FIRMS VULNERABLE AND INEFFICIENT

"Law firms, like every other type of organization, struggle to make data capture a priority. People instinctively create new files and documents as part of their daily routine and keep them in familiar places. While this practice may be more efficient for each individual, it's the core reason data goes 'dark'".

Source: *Law Technology Today, "How to Unlock a Firm's Data Potential," January 9, 2019*

2. USE ONLY VENDORS THAT OFFER PRODUCTS AND SOLUTIONS THAT ARE ALIGNED WITH THE FIRM'S WORKFLOW SECURITY STANDARDS.

Seek vendors that can provide a system for tracking who is handling workflow documents and what they are doing with them, i.e., scanning, copying, printing, or distributing. Implement solutions that can track paper files, digital files, email attachments, and other documents that contain sensitive client information. Exposure can happen at any point during a firm's possession of the information. In the event there are questions about how a document was used and handled, you need a solution that provides fast and easy access to that information.

MOST COMMON TYPES OF SECURITY MEASURES AT LAW FIRMS

Removing Desktop Administrative Rights

Two-Factor Authentication for Remote Access

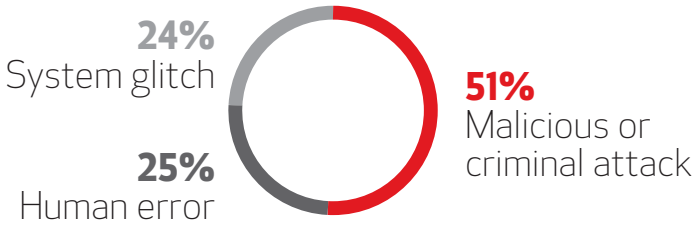
Phishing/Social Engineering Tests of Users

Source: *ILTA 2019 Technology Survey*

3. LEVERAGE YOUR OFFICE EQUIPMENT'S SECURITY FEATURES.

Using document-workflow solutions and office equipment that have easy-to-use security features (such as badge scanners on printers) can help restrict document access to authorized personnel within the firm and protect data from inside breaches. Task your IT staff or enlist a Canon certified specialist to "harden" your devices by activating the extensive security feature sets that reside within the equipment to help limit penetration from the outside. It's especially important that office equipment has security features that are transparent to users and are not otherwise disruptive to workflows. Smooth and continuous operations are important to law firm performance and financial health.

ROOT CAUSES OF A DATA BREACH



Source: *Ponemon Institute 2019 Cost of Data Breach Report – Courtesy of Ponemon Institute & IBM Security*

4. PROVIDE STAKEHOLDERS WITH SECURE AND INTUITIVE FILESHARING TOOLS.

High-risk practices that professionals may use include emailing case documents back and forth on unsecured networks and/or relying on the use of USB drives which can contain malware. By giving your firm's team easy-to-use mobile document sharing tools with user verification, you can help the firm adopt security features that still allow users to be fast and productive. This is an important capability, because transferring files with mobile devices occurs more often today. Innovative solutions employ a variety of methods for securing client data, such as using a unique release code that can be sent directly to a compatible smartphone or another mobile device. The user can then enter the release code to access a document or send a document directly to a printer or copier within the firm.

UNCHECKED BYOD (BRING YOUR OWN DEVICE) POLICIES COMPROMISE SECURITY

Nearly two-thirds (**64%**) of employees use a company-approved personal device for work. However, less than half (**40%**) of employees are subject to regulations for their personal devices.

Source: *Survey of 1,000 full-time employees by Clutch, a B2B Research Firm, May 2018*

5. LOOK FOR OPPORTUNITIES TO CONTROL COSTS AS YOU CHOOSE TECHNOLOGY INVESTMENTS.

Partners sometimes must be convinced to invest time and money in new resources, even for something as crucial as client privacy. One way to increase the likelihood of support is to identify ways to control the cost of acquiring and using security solutions, such as leveraging advanced security features within existing equipment to harden their security profile when possible. Look for a document security platform that is flexible and can be used with a wide variety of brands of printers, copiers, and other office technology. Seek out vendors that have a multi-layered approach to security by providing comprehensive security services such as penetration testing, training, and virtual CISO.

LAW FIRM DATA BREACHES CAN COST MILLIONS OF DOLLARS

$4.62 million Average cost of a data breach in the Professional Services Sector in 2019.

Source: *Survey of 1,000 full-time employees by Clutch, a B2B Research Firm, May 2018*

Learn how Canon Solutions America can help provide a unified platform that provides security, access control, and ease-of-use for document and worklfow management in tandem with a host of cybersecurity services.

Canon
CANON SOLUTIONS AMERICA

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

02/19-1058-3978