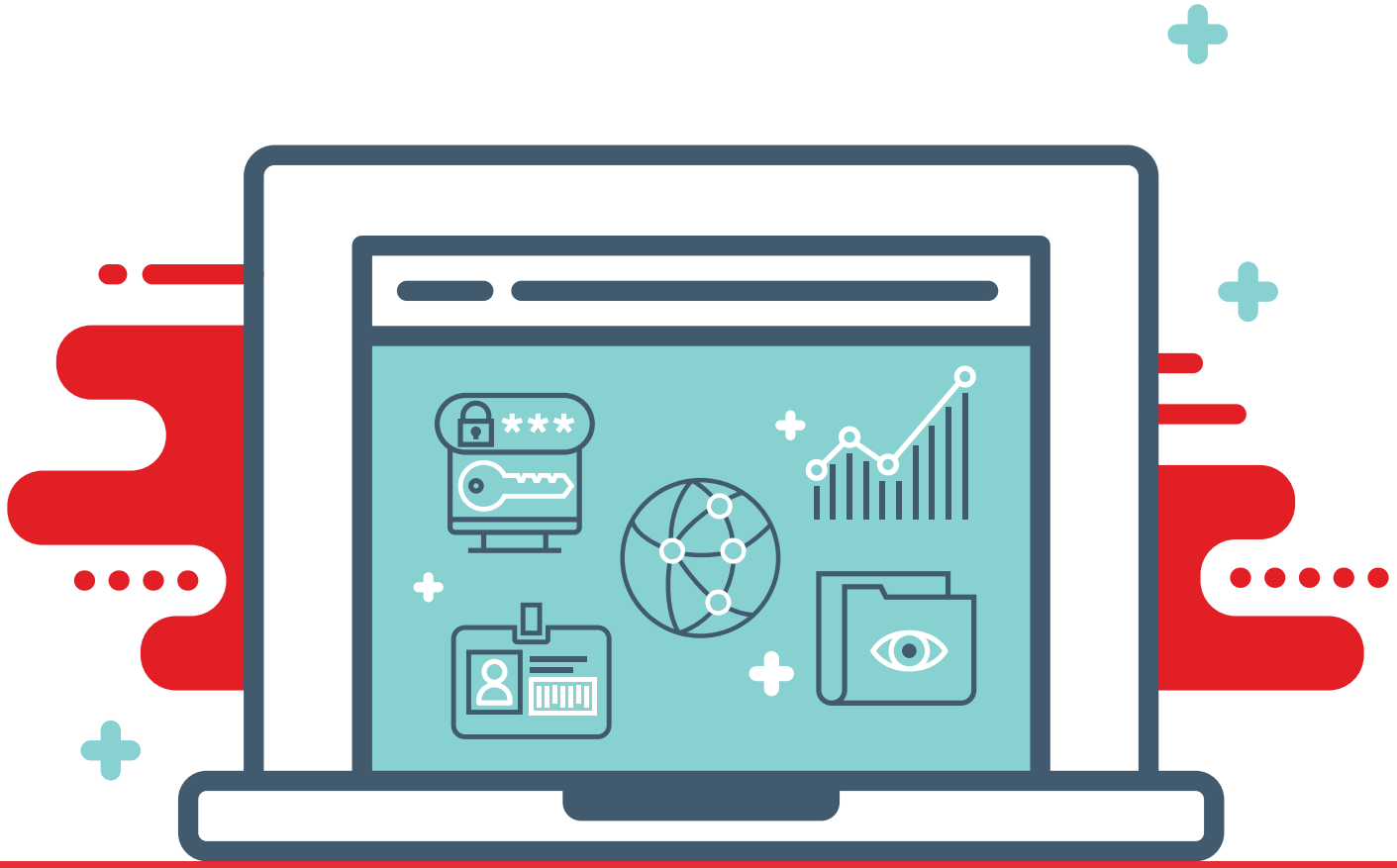

FIVE SIGNS YOUR OFFICE TECHNOLOGY MAY BE PUTTING YOUR FIRM AT RISK

Technology has increased the capabilities of organizations to gather, manage, and store vast amounts of information and data. Law firms are no exception. The practice of law has always been a paper-driven profession. As such, the large volume of documents and files accumulated within the legal workflow represents a significant responsibility. Due to the sensitive nature of the entrusted information, it can increase a firm's exposure to risk if those trusted materials are compromised.

As law firms face greater pressure to ensure data security thanks to increasing legislation ranging from the European GDPR to the California Consumer Privacy Act, evaluating office technology to ensure that information is secure on all fronts is paramount.

According to the 2019 Legal Technology Report from the American Bar Association, more than one-quarter of law firms have experienced a data breach in the U.S.—an increase from previous years.[1] According to a 2019 study by the Ponemon Institute, the current average cost of a data breach in the U.S. is $8.19 million.[2] More than half of those breaches in the professional services sector are considered to be small and mid-sized businesses.

Is your client's data secure? Here are five signs your office technology may not be as secure as you thought it was:

1 Processing paper is a full-time job.

The traditional method of storing client records for most law firms has been an on-site storage room with shelves or cabinets filled with files and documents. Older records were boxed and trucked to an off-site storage facility.

Advances in technology and the introduction of digital media have improved the way in which many firms handle documents and client records, but the emphasis may have been on production and storage rather than the security of those documents.

A secure document ecosystem can automate some processes, helping to create security advances that aren't possible with paper. Electronically capturing sensitive data as it enters your firm, filing it in a secure repository, and routinely purging unnecessary or outdated documents can save your firm significant amounts of time and money.

Does your office technology allow you to seamlessly capture, route, and store information so that it is searchable and accessible to only those who are authorized to view it? Is your firm's staff responsible for manually policing your firm's record retention policies?

2 Digital and paper files are left idle and accessible.

If yours is like most firms, digital files are routed from a laptop or workstation to a printer, where they can sit and wait to be retrieved by the person who printed them. For example, instead of a document being sent from a workstation to a remote printer to wait in a bin where anyone can access it, a document ecosystem can store the document, providing access and authentication controls for content. Processes can be set up so that a person wishing to print must enter a code into a keypad on the printer or swipe an access card for the document to be retrieved and printed.

3 Client documents are not monitored and tracked.

If a data breach happened at your firm, how quickly could you confirm it? Even after you realize there has been a breach, how quickly could you respond or remediate using your current content workflow solutions? Some solutions can provide integrated mechanisms for defining and controlling document access privileges, which can make it easier to identify and trace document distribution within the system. Knowing who handled sensitive, privileged, and/or protected information—and what they did with it—can help a firm remediate problems and respond to audits more effectively.

4 Attorneys and other personnel are accessing firm files remotely without authentication.

Accessing documents remotely is essential for clients and firm partners, but it can come at a risk when mobile-device users are accessing law firm files without authentication and authorization. Implementing individualized release codes is an example of an available security feature. When someone wants to access files within the firm's ecosystem, an individual PIN code is sent to them that must be utilized to access the files.

5 Employees are using printers, scanners, and other devices that are not part of the secure document ecosystem.

Utilizing non-approved, unsecured devices can pose a risk, because it can leave sensitive information vulnerable to data loss. Learn how Canon Solutions America can help by implementing security measures surrounding your document management and imaging devices as well as by providing cybersecurity testing and training services.

Endnotes

[1] *2019 American Bar Association Technology Report*

[2] *Ponemon Institute 2019 Cost of Data Breach Report – Courtesy of Ponemon Institute & IBM Security*

Canon

CANON SOLUTIONS AMERICA

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

01-04/19-1054-3907