

File Sharing Without Fear: 5 Key Requirements for Law Firms When Choosing a Content Collaboration Platform

Executive Brief

Summary

Law firms have received two dramatic wake-up calls about the vital importance of data security in the last two years. First, there was the leak of 11.5 million documents from offshore law firm Mossack Fonseca, known as the Panama Papers, which became public in 2016.¹ Then came the massive cyberattack on prominent global law firm DLA Piper in the summer of 2017.² As we will explore, despite the industry's aversion to media coverage of such attacks, less-visible breaches involving the legal profession are being reported worldwide in ever-increasing numbers.

Law firms of all sizes have become appealing targets for hackers for multiple reasons. They are one-stop shops for valuable confidential information such as trade secrets, business transactions, insider information, social security numbers, financial information and more. Cyber criminals are also attracted to law firms' large trust accounts. Add to this the fact that law firms are known for relatively lax data security compared to financial institutions, which have long been prime targets, and the urgent need for coordinated, firm-wide cybersecurity practices becomes obvious.

In today's mobile, collaborative legal environments, any workforce productivity or cybersecurity strategy is incomplete without a secure content collaboration platform (also referred to as Enterprise File Sync & Share (EFSS) solutions). Attorneys need anytime, anywhere document access and collaboration across all their devices – especially for the most sensitive files – to keep pace with the demands of their profession. They also need to keep those files safe.

Table of Contents

Collaboration culture and the legal profession	4
Current threat landscape for law firms	5
Why content collaboration matters to law firms	6
5 non-negotiable requirements for content collaboration platforms in law firms	6
BlackBerry® Workspaces: the most secure file sharing and collaboration solution	7

Collaboration culture and the legal profession

Employees share files across more endpoints – both mobile and desktop – than ever before. This culture of digital collaboration presents unique challenges for law firms because they have an added ethical and professional duty to safeguard their clients’ proprietary and confidential information.

Legal associations are establishing new policies and practices to make attorneys more accountable in the digital age. The American Bar Association (ABA) has amended its Rules of Professional Responsibility to include attorneys’ duty to stay informed of changes in the law and its practice, “including the benefits and risks associated with relevant technology.”³

Apart from the professional ramifications of data breaches, there are potentially disastrous implications for the bottom line. Law firms’ reputations hinge on protecting client confidentiality. According to an article in the Canadian Bar Association magazine, class-action lawsuits are becoming more common for breaches of privacy, presenting another potential for liability.⁴



Current threat landscape for law firms

Law firms not only face malicious cyberattacks launched from the outside, but also confront internal threats.

External threats

A survey of more than 200 law firms published in Law.com found 40% had been breached without knowing it.⁵ The same poll found an average of 10,000 intrusions occur every day at law firms, with large and small firms equally at risk. Overall, more than 80 per cent of American law firms have had some type of breach, according to a 2015 Bloomberg article.⁶



Internal threats

Data leakage by employees and third parties associated with law firms happen for diverse reasons. Some employees may lack adequate security awareness. While others may use unapproved collaboration and file-sharing apps that are familiar and convenient tools to get work done. Other causes include basic human error, lost devices, negligent data sharing and, quite commonly, internal bad actors who use a data breach to damage the organization.

Despite the headline news about data breaches at law firms and the alarming statistics, however, an astounding 95% of law firms are not compliant with their own data security policies, according to the same survey of 200+ firms.⁷

Why content collaboration matters to law firms

Collaboration and the exchange of sensitive files are essential to daily activities at law firms. Many firms still fax and mail documents for security reasons, which obviously hinders productivity. Yet attorneys also store and exchange critical files (with content ranging from private client information to intellectual property and M&A documents and spreadsheets) on all types of devices for ease of access and productivity – which compromises security. A secure content collaboration platform or EFSS solution delivers both data protection and mobile productivity.

In even the most well-protected networks, breaches happen (due to user error, for example). A powerful solution allows law firms to remediate the breach with remote file access controls and digital rights management (DRM) protection – so firms stay in control even after files are shared outside the firewall.



When users can safely access, share, sync and collaborate on even the most sensitive files using any device, they are more productive. Law firms need a solution that supports seamless workflows while always ensuring data security.

5 non-negotiable requirements for content collaboration platforms in law firms

The size of the EFSS market is expected to grow from USD 1.11 billion in 2015 to USD 3.51 billion by 2020, according to Markets and Markets research.⁸ The rising demand for cloud-based integration and the Bring Your Own Device (BYOD) trend are driving this growth.

As the number of EFSS vendors increases, choosing the right solution becomes more complex. Law firms should take extra care scrutinizing a potential provider because of their stringent security needs. Yet security is just part of the equation: a content collaboration platform is only valuable if it also offers functionality and ease of use. It should allow attorneys to access case files whenever and wherever they are – including from court – on their device of choice.

The following questions can help law firms assess any content collaboration or EFSS solution:

1. Does it support easy, secure file sharing on all devices?

Today’s law firms need an EFSS solution that goes beyond simple file sharing to enable teams to work effectively across the firm, as well as with all types of external partners. Attorneys must have the ability to share, edit and control confidential documents from any mobile or desktop device.

2. Does it enable customized permission profiles for internal and external collaboration?

Attorneys should have the ability to create and manage detailed security policies tailored to a wide range of file-sharing scenarios inside and outside the law firm.

3. Does it allow permissions to be managed or revoked after files have been shared?

When a sensitive file gets into the wrong hands, law firms should be able to revoke access in an instant.

4. Does it balance security with collaboration?

An EFSS solution should balance the needs of attorneys (intuitive interface for efficiency and productivity), clients (privacy) and IT (central policy management, flexible deployment, easy integrations, etc.).

5. Does it provide end-to-end file encryption?

Legal files should always be encrypted – in transit, at rest and while in use – by encryption that meets the rigorous standards of governments and financial institutions.

BlackBerry® Workspaces: The Most Secure File Sharing and Collaboration Solution

BlackBerry® Workspaces meets and exceeds the key requirements outlined above for an EFSS solution for law firms. BlackBerry® Workspaces is a secure content collaboration platform that enables multi-OS file synchronization and sharing. It promotes “anytime, anywhere” collaboration in an intuitive, user-friendly interface, while also delivering industry-leading security. With BlackBerry® Workspaces, law firms stay in control – even after files are shared outside the firm’s firewall.

BlackBerry® Workspaces achieved the highest scores in the Workforce Collaboration and Centralized Content Protection use cases versus 12 other vendors in the [2017 Gartner Critical Capabilities for Content Collaboration Platforms Report](#).⁹

How BlackBerry® Workspaces provides what law firms need:

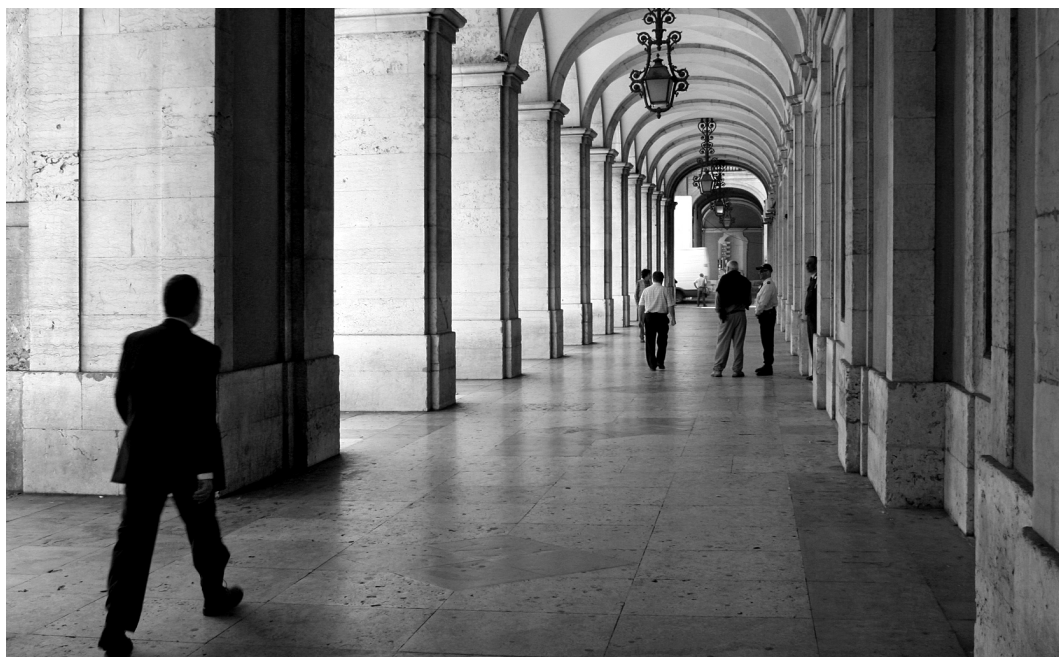
BlackBerry® Workspaces stands apart from the expanding number of EFSS and content collaboration vendors as a complete solution for law firms, delivering best-in-class data security and easy, anytime collaboration capabilities.

1. Does it support easy, secure file sharing on all devices?

BlackBerry® Workspaces is a secure choice for law firms. It builds security right into business files or unstructured data, and protects data wherever it travels. It delivers the most robust Digital Rights Management (DRM) in the market, making it easy to control users' ability to access, view, edit, copy, print, download and forward files – online and offline – on any device, even after they are downloaded from the system.

2. Does it enable customized permission profiles for internal and external collaboration?

BlackBerry® Workspaces securely connects the right people to the right content across law firms and beyond to external parties. System administrators can create customized permission profiles for unique workflows, extending mobility and collaboration capabilities while enforcing security. With BlackBerry® Workspaces, attorneys can collaborate on confidential files with outside law firms with confidence that they retain visibility and control over the content.



3. Does it allow permissions to be managed or revoked after files have been shared?

BlackBerry® Workspaces allows group administrators to set permissions to expire after a certain amount of time or on a specific date, remotely change permissions or revoke access manually at any time. When a device is lost or stolen, an employee leaves the organization, a partnership ends or an employee makes a mistake and opens the door to a bad actor, administrators can immediately revoke access to all shared, sent or synced documents. Administrators can control the data even if the employee forwarded it to their personal email address or saved it to a flash drive. When access rights are revoked, all applicable encryption keys for that user or group or device are immediately expired, leaving the user with an unusable ‘digital blob.’

4. Does it balance security with collaboration?

BlackBerry® Workspaces synchronizes documents across all devices (personal or corporate-owned) to ensure the latest file version is available on all devices (including Windows® and macOS®, or iOS, Android™ and BlackBerry® 10 mobile devices). BlackBerry® Workspaces users can create, manage, view, search, edit and annotate Microsoft® Office, PDF and image files. Members can edit from any mobile device – even offline – including the ability to make inline comments and use “@mention” to leave comments for specific people. BlackBerry® Workspaces makes collaboration simple and seamless.

5. Does it provide end-to-end file encryption?

With BlackBerry® Workspaces, files are always encrypted (via AES-256 where available, using FIPS 140-2 certified cryptographic library): in transit, at rest and – uniquely – in use. This helps to control over what can be done with the file itself – whether that is printing, editing, copying or forwarding it to someone else. By keeping sensitive data encrypted and controlled by default, BlackBerry® Workspaces reduces the risk of a breach or loss of data.

BlackBerry® Workspaces features that safeguard legal files while boosting productivity:

- *Custom watermarks* splash a user’s email or IP address across a document or in the viewer to deter leaks and increase accountability
- *DocuSign* integration enables users to obtain legally binding signatures
- *Read acknowledgement* tracks and stores employee uptake of official policies and procedures
- *Spotlight* feature blurs out the screen in presentations, except where the mouse or pointer is hovering
- *File locking* allows only one user at a time to edit a document, reducing duplication of effort

Three reasons IT teams love BlackBerry® Workspaces:

1. Single pane of glass

No matter where documents are stored, group members have a unified view of all the files they have access to within BlackBerry® Workspaces. Administrators have a single, centralized console for extending mobility and collaboration capabilities, while also managing and enforcing security/auditing policies. Granular logging and reporting tracks individual document activities, providing essential information for an investigation into potential security issues. BlackBerry® Workspace administrators can also create customized permission profiles for unique users, enabling collaboration with multiple players.

2. Full integration with business apps and existing solutions

BlackBerry® Workspaces readily integrates with most leading file repositories, enabling law firms to protect vital assets without investing in additional infrastructure. From BlackBerry® Workspaces mobile and web interfaces, employees can access and share files that exist within these repositories. BlackBerry® Workspaces supports a wide range of authentication systems, and integrates with existing security solutions, including firewalls and data loss prevention systems. Users can also open files and save from within the Microsoft® Outlook user interface.

3. Flexible deployment

Law firms can deploy BlackBerry® Workspaces in whatever way best suits their IT environment. There is an on-premises option for firms that want complete control, end to end, and have the IT resources to manage or maintain the deployment. The cloud-hosted solution is quick and easy, avoiding the hassles associated with an on-premises application. There is also a hybrid option. Regardless of the deployment type, law firms get a single, secure view of their content from any device.



Today's collaboration culture is here to stay. In law firms, file-sharing across devices with multiple partners can support new workflows and enhanced productivity, but it also introduces considerable risk. While network security is crucial, breaches happen in even well-protected systems because people make mistakes, get fooled or betray trust – not to mention the growing number of malicious cyberattacks from outside. With BlackBerry® Workspaces, file-level security and powerful DRM deliver an additional level of security. It empowers employees to achieve seamless collaboration and efficiency, while keeping law firms in control of critical files – even after they have been shared.



Next Steps:

To find out how BlackBerry® Workspaces can improve collaboration and data security at your law firm, please contact us at <https://global.blackberry.com/en/enterprise/contact-us>



© 2017 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BES, BBM and EMBLEM Design are the trademarks or registered trademarks of BlackBerry Limited. All other trademarks are the property of their respective owners.

¹The Guardian (<https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers>)

²American Lawyer (<http://www.americanlawyer.com/id=1202791614770/Ransomware-Attack-on-DLA-Piper-Puts-Law-Firms-Clients-on-Red-Alert?slreturn=20170917205046>)

³American Bar Association (https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html)

⁴Canadian Bar Association Magazine (<http://nationalmagazine.ca/Articles/May-2016-Web/Is-your-data-safe.aspx>)

⁵Law.com (<http://www.law.com/sites/almstaff/2017/06/29/dla-piper-isnt-alone-40-percent-of-law-firms-unaware-of-breaches/?slreturn=20170911104118>)

⁶Bloomberg (<https://www.bloomberg.com/news/articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security>)

⁷Law.com (<http://www.law.com/sites/almstaff/2017/06/29/dla-piper-isnt-alone-40-percent-of-law-firms-unaware-of-breaches/?slreturn=20170911104118>)

⁸Markets and Markets (<http://www.marketsandmarkets.com/Market-Reports/enterprise-file-sharing-and-synchronization-market-149308334.html>)

⁹Inside BlackBerry (<http://blogs.blackberry.com/2017/09/blackberry-workspaces-achieves-highest-scores-for-two-use-cases-in-gartners-critical-capabilities-for-content-collaboration-platforms-report/>)