Sponsored by

BlackBerry

File Sharing and Collaboration Leads to Security Gaps in Financial Services Firms

EXECUTIVE BRIEF

Introduction

Financial services organizations, including banks, brokers, insurance, and wealth management advisors, are generally considered the most secure enterprises. According to an April 2015 study by Accenture, 86% of people in the U.S. and Canada said that banks and financial institutions were the companies they trusted most with managing their data securely, far ahead of mobile phone providers, tech firms, and social media platforms.[1]

Trust and financial services go hand in hand. Not only do customers trust financial institutions with their assets, but with their personal information as well. The very nature of the business involves a great deal of sensitive information, from account balances to personal identifiable information (PII) like Social Security numbers.

There are a number of regulatory regimes imposed on financial services firms at the international, federal, state, and local levels. Many of these regulations govern data security, making financial institutions subject to a great deal of scrutiny over their cybersecurity efforts. Among the better-known regulations are the Federal Information Security Management Act (FISMA), the Gramm-Leach-Bliley Act (GLBA), the Payment Card Industry Data Security Standard (PCI DSS), the EU's General Data Protection Regulation (GDPR), and New York State's NYCRR Part 500 regulations.

With hefty fines, strategic and operational impacts, and exposure to legal action, the failure to adequately protect sensitive information is costly for any organization. According to the 2017 Cost of *Data Breach* Study by the Ponemon Institute and IBM, the average total cost of a data breach is $3.62 million.[2] In financial services, the cost is particularly high. The study found that breaches cost financial firms $336 per compromised record. Only healthcare – another highly regulated industry – suffers a higher per-record cost at $380.

In this Paper

- Regulatory scrutiny makes data breaches particularly costly for organizations that operate in the financial services industry
- Data breaches can come from any number of sources, including mistakes from well-intended employees, rogue employees, and international crime organizations
- Solutions exist today to help financial services organizations better protect their unstructured data and avoid costly breaches

Information security discussions often focus on perimeter security and intrusion prevention, which is understandable. Many high-profile breaches, including the 2017 Equifax incident, involve intruders gaining access to databases full of records stored as structured data. This Research Brief, however, focuses on two areas that receive less attention: unstructured data (such as Microsoft Office files, PDFs, and image files), and the security risks present in many of the internal business processes that use it.

The same regulatory scrutiny and fines that apply to a breach of structured data also apply to breaches that result from flaws in file sharing (which usually involves business files – i.e., unstructured data). Sometimes these breaches are subject to higher penalties because they highlight greater flaws in internal operations and processes.

Data Protection Policies Covered by Financial Industry Regulations

	NYDFS 500	GLBA/ FFIEC	PCI DSS	GDPR
Protection of Customer Info	✓	✓	✓	✓
Encryption	✓	✓	✓	✓
Access Controls	✓	✓	✓	✓
Compliance Logging and Reporting	✓	✓	✓	✓
Oversight of External Users	✓	✓	✓	✓
Incident Monitoring and Reporting	✓	✓		✓

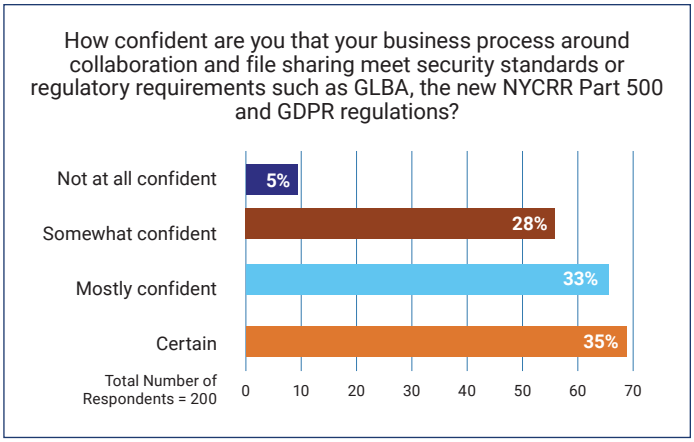
The findings in this Research Brief are based on a survey of 200 IT professionals who work in financial services. The survey was conducted in September 2017.

Security is Top of Mind, But Risks Remain

The survey results confirm that financial services organizations put a great deal of effort into their security plans for structured and unstructured data, as well as for sharing sensitive files. They also confirm that financial services firms believe their security policies cover unstructured data such as business files. However, the survey also confirms the presence of significant security risks involving unstructured data and file sharing.

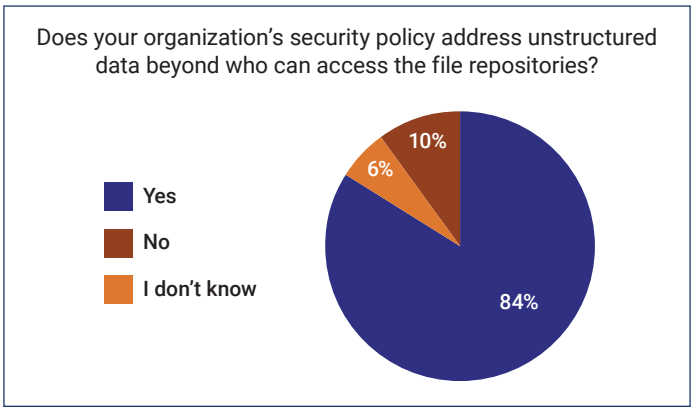
> "Email was created for the fast, easy distribution of information, but it was not developed with security in mind."

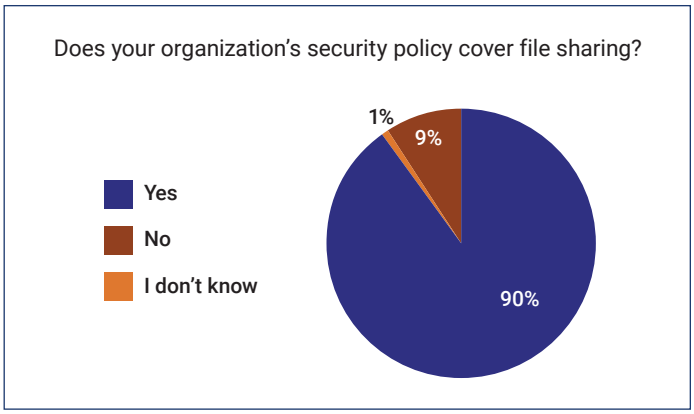
Despite the fact that the vast majority of respondents said that their firms had security policies covering unstructured data, only 35% of survey respondents reported they were certain that their business processes around collaboration and file sharing meet their regulatory requirements. One-third of the respondents said they were only "somewhat confident" or "not at all confident" about their ability to meet regulatory requirements. Most of the survey's respondents indicated plans are in place for addressing the security of unstructured data.



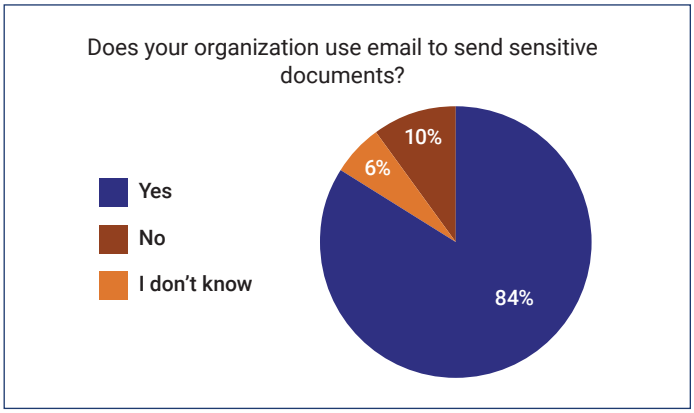
Email is a Problem

The survey results uncovered areas where the business processes used by financial services institutions were exposing them not only to risks, but to inefficiencies as well. The most prominent example involves email.





As with most businesses, file sharing via email is a very common practice at financial institutions. The survey found that more than four out of five respondents said their organization sends sensitive files via email as part of their business process.



Email was created for the fast, easy distribution of information, but it was not developed with security in mind. That makes email a poor choice for sending sensitive information. More recent advances in email security, such as encrypted email, are not practical for day-to-day communications with external parties due to low adoption rates for this technology.

Using email to send sensitive information exposes financial services firms and their partners to a great deal of risk. When a copy of an email and any associated information (like an attachment) is sent from one user to another, multiple copies of the message are also stored on servers and devices, some of which are beyond the control (and security policies) of the organization where the email originated.

Consider that a copy of each email message is saved:

- On the outbound email server
- On the inbound email server
- On each recipient's hard drive
- On each device that the sender and each recipient uses to access their email.

Even in a simple scenario where an email is sent from one sender to one recipient, where each party uses a single device, that's four copies of the message on various machines. Now consider that each of those machines or devices is vulnerable to attack, misuse, or in the case of mobile devices, they may be stolen or lost.

There's no way for organizations to guarantee that an outside device or email server is secure, which means any information sent via email needs to be treated as if it will be exposed at some point, whether it's sensitive business information — a lesson Salesforce.com learned the hard way in 2016 — or the private musings of a public official, like former U.S. Secretary of State Colin Powell whose personal email was made public by hackers in 2016.

Mistakes Happen

One of the biggest missteps reported by survey respondents was the accidental sharing of sensitive files. More than one-quarter of respondents indicated they had a security breach caused by a simple mistake.

Typos, busy people trying to multitask, and new employees are just some of the ways human error can lead to the release of sensitive information. In addition to better technology solutions for securely sharing unstructured data, the survey findings suggest that better training on the handling of business documents, which is repeated on a regular cadence, could help reduce costly mistakes. Better security practices also need to extend beyond employees to include partners and consultants as well.

Audit trails are particularly useful for instances where sensitive information is accidentally shared. The ability to see who

received the information, viewed the file, downloaded it, or made edits is an important feature of enterprise-grade file-sharing and collaboration solutions. An audit trail can be used to understand the extent of a mistake and help contain the damage.

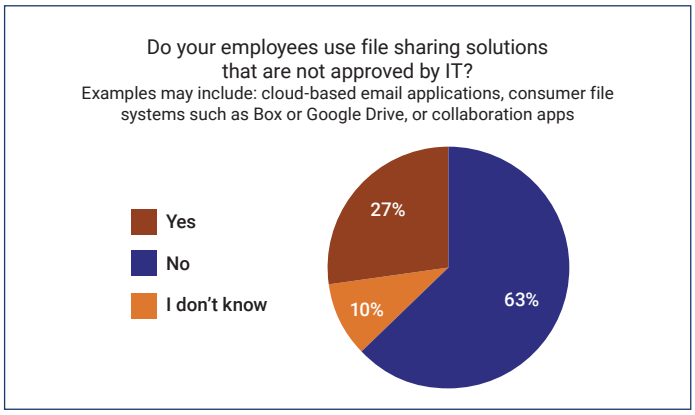
When an outside counsel representing a large U.S. bank turned over documents as part of a routine discovery process related to a lawsuit in 2017, more than a gigabyte of sensitive information unrelated to the matter in question was accidentally released, including financial information on as many as 50,000 individuals. The information was sent by the bank to its outside counsel, and was then burned onto a CD and delivered to the plaintiff's lawyers. Once the information left the bank's network, there was little that the financial institution could do to stop it from being shared further. This example demonstrates how the ability to revoke access to information after it has been shared can help prevent a mistake from becoming a very costly problem.

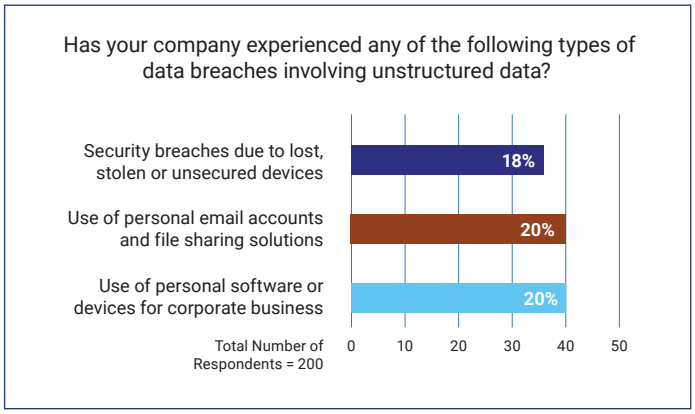
Rogue Employees: Consumer-Grade File-Sharing Applications

The widespread availability of web-based file-sharing systems also presents a risk to financial services firms. Employees use file-sharing applications as shortcuts to try to get their jobs done, but in doing so they are exposing their company, other employees, customers, and partners to an enormous amount of risk, including compliance issues.

More than one-third of respondents to the survey said their organizations either have employees using file-sharing applications that are not approved by IT (and one assumes, therefore, not covered in the existing security plan) or they aren't sure about the use of such applications. Twenty percent of respondents indicated that their firm suffered a data breach involving unstructured data as a result of its employees using personal email accounts or file-sharing solutions.

Many companies report that employees are using non-approved file sharing apps.





> "Many financial institutions that lack confidence in modern technology or tools to mitigate risks related to unstructured data are still using legacy technologies as an alternative."

What if financial institutions used the appeal of consumer-grade file-sharing and collaboration tools to help create an experience for employees that is both secure and easy to use? Many of the freely available tools employees turn to in place of authorized applications or processes are simple, increase employee productivity, are accessible from multiple devices and locations; however, enterprise-grade security is not a built-in capacity.

When it is difficult for employees to access business email or other applications because they are off the corporate network, they are more likely to turn to web-based applications like email to send, receive, and store information because it's available wherever there's a working Internet connection. The same can be said of web-based file-sharing applications, which can be used to access documents when an employee cannot access their business computer.

Bad Actors

Many of the well-publicized data breaches in recent years involve bad actors: people or groups that intend to do harm by accessing information left exposed by organizations of all types. More than one-quarter of the survey respondents reported their organizations suffered a data breach because of an external attack, which could include hackers that are part of organized crime networks, lone actors or small groups that probe networks to see what they can find, or attackers sponsored by nation-states looking to create havoc and steal data.

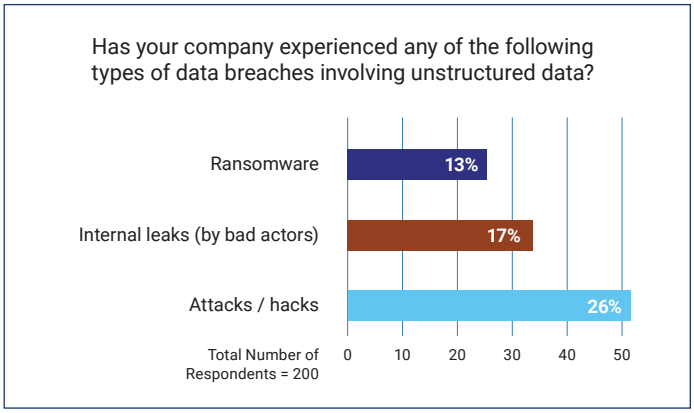
Seventeen percent of survey respondents reported their organizations suffered a data breach at the hands of internal bad actors. This includes disgruntled employees and others, who either attained access to sensitive information or had access all along and simply distributed the data to unauthorized parties.

A smaller but still significant percentage (14%) of respondents said their organizations were the victims of a ransomware attack, where data is taken and held hostage until the attacker is paid off and releases it (although payment doesn't always guarantee its release). The most noteworthy ransomware attack of the past several years is the WannaCry attack, which struck the Internet in the spring of 2017.

"More than one-third of respondents to the survey said their organizations either have employees using file-sharing applications that are not approved by IT."

By implementing controls that give them complete control over their files, financial institutions gain the ability to neutralize attacks by bad actors that take place despite their best efforts and existing defenses to prevent them. Every organization that was affected by WannaCry was protecting its network using tactics such as intrusion prevention, but they became victims nonetheless. If access control for files, including the ability to revoke access to sensitive information, were as widely used as firewalls and perimeter defense strategies, attacks by bad actors would be less lucrative and potentially less common.

Internal leaks trail external attacks, but remain a significant threat



Cumbersome Process and Inefficiencies

Many financial institutions that lack confidence in modern technology or tools to mitigate risks related to unstructured data are still using legacy technologies as an alternative. Nearly 80% of respondents said their companies are sending sensitive documents via old-fashioned snail mail and faxes. Three-quarters of the respondents cited security reasons or legacy processes that have not yet been modernized as the reason for using postal mail and faxes. More than 40% indicated their use was the result of technological or hardware constraints.

Why does your organization mail or fax documents?

Security reasons	77%
Legacy process	71%
Technology/hardware constraints	42%
Other	8%

Whatever the reason for using mail and faxes, two things are clear: first, these forms of communication carry security risks of their own (e.g., you don't really know who receives the information once you send it); and second, they create significant inefficiencies in the way that financial services firms are conducting business. There is a substantial opportunity to increase productivity, speed, and customer satisfaction by adopting new technologies for communicating sensitive information if it can be done in a secure manner.

Improving the Security of Unstructured Data and Related Processes

There's often a tension between productivity and security in adopting enterprise software technologies. The ability to send documents via email, for example, is faster and less expensive than using postal mail or fax. But, mail and fax are often perceived as being more secure.

When organizations invest in the right tools and processes, there doesn't have to be a tradeoff. Modern file-sharing tools exist today that are built around the concept of increasing security, regulatory compliance, and productivity. They are developed to provide the same level of service and ease of use as the consumer-grade products in the market, while also offering enterprise-grade security, administration, and reporting features. The following requirements can help financial services institutions identify a solution that meets their needs.

Security and compliance requirements include:

- **File encryption:** With FIPS 140-2 certified crypto-modules. Files encrypted at rest, in transit, and in use.
- **File access and usage controls:** Ability to restrict access to authorized users and restrict the redistribution of files. Support for Digital Rights Management (DRM), water-marking and online view-only mode.
- **Administrative controls:** Fine-grained user and policy management. Ability to change or revoke access manually or automatically, even after files have been shared.
- **Logging and auditing:** Ability to capture and log all data access events. Support for flexible compliance reporting. Integration and support for data loss prevention (DLP) solutions.

> "It's important that financial services institutions have a way to respond to these breaches and minimize the damage when they occur."

Productivity requirements include:

- **Collaborative workspaces** accessible via browsers and apps.
- **A platform-agnostic approach** that supports secure access, productivity and file synchronization. Must support the most important OS in the enterprise – Windows, MacOS, iOS, Android, and HTML 5.0 browsers (for any device that runs them).
- **The ability to extend and secure existing repositories** to protect files in place and enable access and sharing without the need for data migration
- **Support for existing workflows and systems,** with a robust integration architecture and development APIs and SDKs.

Conclusion

For many institutions in the financial services industry, their current security policies, applications, and business practices they rely on when working with unstructured data may not be sufficient for protecting them from security risks or meeting compliance requirements. This creates a great deal of risk for these firms because of the high costs of a data breach -- in terms of customer trust, restitution, and penalties -- can ruin a business.

Data breaches are going to happen. They happen at the hands of well-meaning employees who make mistakes, rogue employees who fail to follow policies and procedures designed to protect

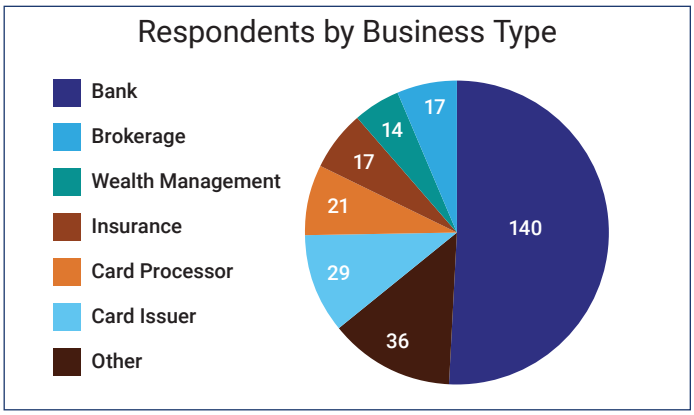
the organization, and bad actors that hope to profit from gaining access to sensitive information. It's important that financial services institutions have a way to respond to these breaches and minimize the damage when they occur.

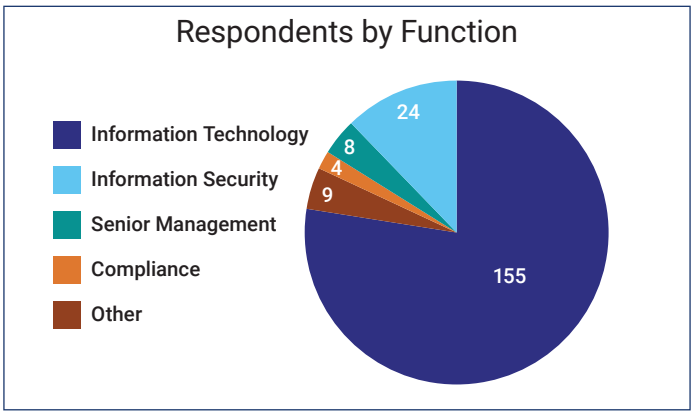
Secure file-sharing and collaboration applications can help financial services institutions protect themselves and their customers. Applications with the ability to restrict and revoke access to business documents, for example, can prevent the dissemination of information that is stolen or accidentally released. Audit trails can help more quickly uncover rogue employees and assist in meeting regulatory requirements.

But modern technology will only be widely adopted by employees if it improves productivity. Security must be a core feature of the workflows. Barriers created by applications that complicate processes and make it difficult to access or find information will drive employees to the consumer-grade applications that introduce risk. Collaboration and file-sharing solutions designed with security, productivity, and compliance in mind will go a long way toward reducing the risks associated with unstructured data.

BlackBerry Workspaces

BlackBerry Workspaces makes enterprises more mobile and collaborative, while reducing the risk, complexity, and cost of sharing information across and beyond your organization. Workspaces provides file-level encryption and user access controls, so you maintain control over your content even after it leaves your firewall. Workspaces also embeds digital rights management (DRM) protection in your files, so you can control what the recipient is able to do with the file once they gain access to it. Learn more and sign up for a free trial at blackberry.com/workspaces.





About the Survey

The survey of 200 IT professionals in the financial services industry was conducted in September 2017. Respondents received an email invitation to take the survey. The respondents include a number of job functions and business types within financial services.

About BlackBerry®

Today, BlackBerry is a transformed company. Building off decades of innovation in secure communications, BlackBerry continues to be a trusted technology provider for financial institutions the world over. BlackBerry's secure file sharing solution, BlackBerry Workspaces, received the highest score in two of five use cases in the 2017 Gartner Critical Capabilities for Content Collaboration Platforms Report.

[1] https://newsroom.accenture.com/industries/banking/north-american-consumers-overwhelmingly-trust-banks-to-securely-manage-their-personal-data-according-to-accenture-report.htm

[2] https://www.ibm.com/security/data-breach/index.html