ABERDEEN

RICOH
imagine. change.

Documents in the Digital Workplace:

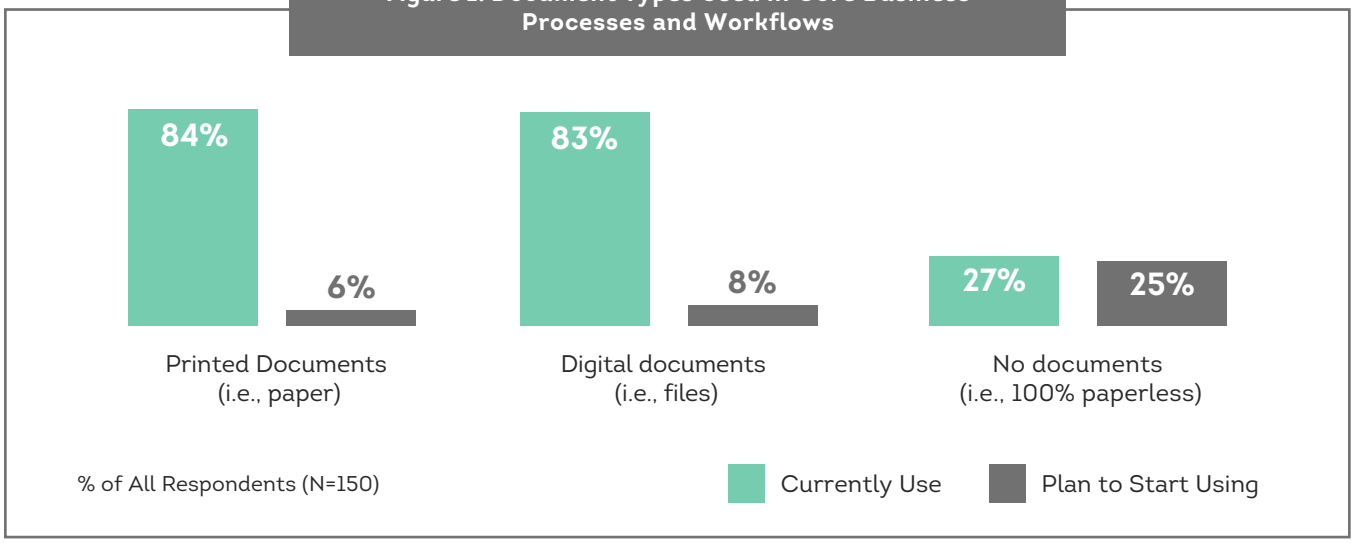
Enable the Opportunities, and Manage the Risks of Ransomware and Data Breaches

Introduction: Documents in the Digital Workplace

Documents – whether paper-based, or fully digital – are an integral part of the core business processes and workflows for virtually every organization.

Aberdeen's research found that a growing number of organizations have at least one initiative for a core business process / workflow which is 100% digital (i.e., paperless) … and also confirms that digital documents (i.e., files) continue to be everywhere.

Figure 1: Document Types Used in Core Business Processes and Workflows



To enable the sharing of their essential documents between the users and / or systems that need them, approximately 4 out of 5 organizations in Aberdeen's study are currently using a complex, hodge-podge mix of multiple "do it yourself" mechanisms, including:

- Postal services (i.e., "snail mail")
- Express delivery services (e.g., couriers, FedEx)
- FAX or FAX services
- IT-level tools (e.g., FTP, custom scripts)
- Email attachments
- Messaging app attachments (e.g., Skype, Slack)
- File sync / file share apps (e.g., SharePoint, OneDrive, Google Drive, DropBox, Box)

Larger, more mature organizations with a wide variety of use cases have also invested in purpose-built, enterprise-class mechanisms for storing, managing, sharing, and safeguarding their digital documents, such as:

69%
Managed File Transfer

69%
Content Management Systems

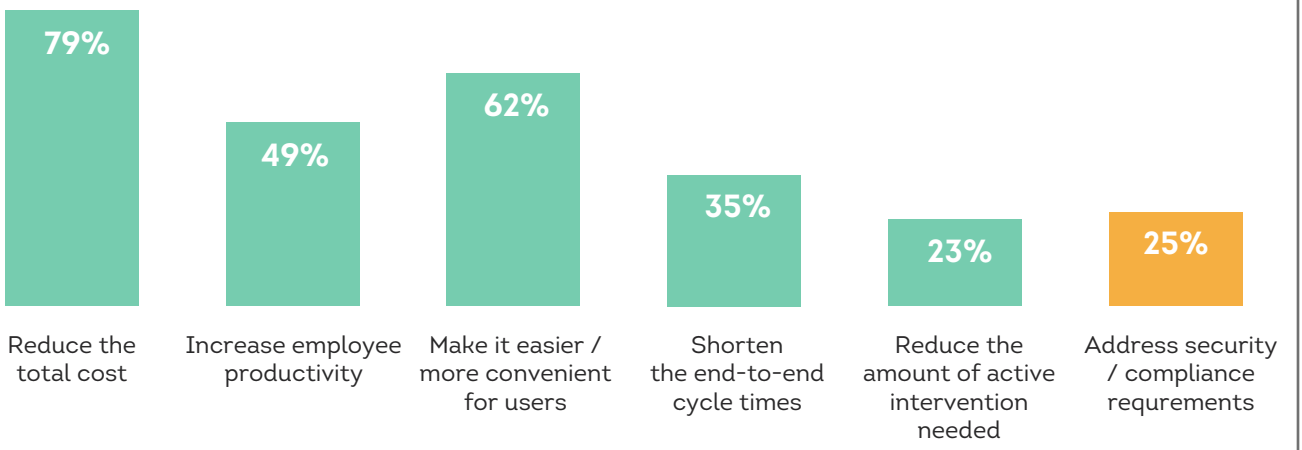
71%
Document Management Systems

81%
Data Backup and Recovery

When it comes to the top drivers for making investments in technology-based capabilities to improve the business processes and workflows that involve digital documents, it's not surprising that saving time and money dominate the list. Organizations are pretty clear about what they're looking for: cost savings, productivity, convenience, speed, and efficiency – while at the same time, addressing their requirements for security and compliance (see Figure 2).

Said another way: They not only want to enable the opportunities for leveraging documents in the Digital Workplace, but also to manage the risks.

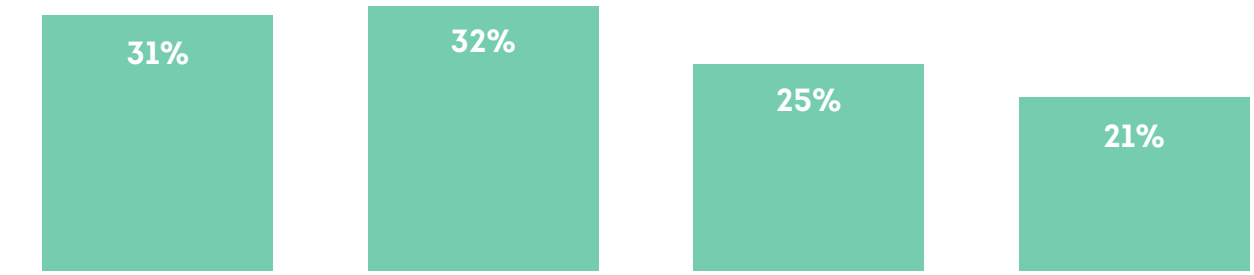
Figure 2: Leading Drivers for Technology Investments



% of All Respondents (N=150)
Multiple responses accepted; does not add to 100%.
Source: Aberdeen, October 2021

As a counterbalance to the drivers, the top inhibitors to making investments in these areas include the challenge of making a clear business case, concerns about security and ease of use, and lack of technical staff (see Figure 3).

Figure 3: Leading Inhibitors for Investments



Difficulty of making a clear business case, to prioritize the allocation of resources

Concerns about security-related risks (e.g., data breaches, unplanned disruption)

Lack of technical staff (e.g., for deployment, training, administration, support)

Concerns about convenience / ease of use for users

% of All Respondents (N=150)
Multiple responses accepted; does not add to 100%.
Source: Aberdeen, October 2021

Making a Clear Business Case: Your Digital Documents Represent Valuable Data, and Your Valuable Data is at Risk

Files are being used extensively in support of your organization's strategic initiatives for the Digital Workplace, e.g., *productivity, collaboration, digital transformation, intelligent automation,* and so on.

Without having visibility into your company file movements, however, the process of making business decisions about security-, privacy-, and compliance-related risks is based primarily on mere intuition and gut instinct. How can we make the business case more clear and quantifiable, to help justify and prioritize the allocation of resources to address these risks?

The Valuable Data in Your Digital Documents at Risk

Files represent between **46%** and **51%** of all enterprise data movements

The number of file exposure events averages **6 to 34** (median: 13) per user, per day

Data breaches are **1.1-times to 4.5-times** more likely to occur on end-user endpoints than on back-end servers

Ransomware is on the rise: more than **300M ransomware attacks** were recorded in 2020, about the same as in the first half of 2021 alone

Data breaches involving files generally relate not to records (databases), but to intellectual property (IP) – a topic that most people would instinctively defer to their legal department, because the term IP is so strongly associated with:

- **Patents** (e.g., inventions and discoveries)
- **Trademarks** (e.g., brands, logos, designs, packaging)
- **Copyrights** (e.g., written or recorded works)
- **Trade secrets** (e.g., processes, formulas, methods)
- **Confidential information** (e.g., sales and marketing plans, production forecasts, merger and acquisition activities, pricing, customer lists, procurement data)

However, what's important to realize is that a significant percentage of your organization's IP is captured in its digital data, in the form of files. And as we have seen, for the typical organization there's a lot of it!

As an example of how to communicate more effectively with senior business leaders about the risk to digital data in the form of files – in a way that actually helps them to make better-informed business decisions regarding what to do about it – Aberdeen developed a quantitative Monte Carlo analysis based on two different likelihood factors, and one Impact factor:

- **Likelihood:** How likely for a data breach to occur, on an annualized basis? How likely for a data breach to involve digital files?
- **Impact:** How much business impact from a file-related data breach that involves your most valuable IP?

To illustrate, consider three examples that reflect an organization in the private sector with the following characteristics, as summarized in the following table:

Illustrative Example	Annual revenue	Annual revenue from "crown jewels" IP	Annualized risk of a file-related data breach
1	**$10B**	**$1B**	Median (50% likely to exceed) **$3.4M** "Long tail" (5% likely to exceed) **$200M**
2	**$100B**	**$10B**	Median (50% likely to exceed) **$94M** "Long tail" (5% likely to exceed) **$6.3B**
3	**$100M**	**$100M**	"Long tail" (5% likely to exceed) **$8M**

In this type of analysis, risk is properly described as a range of possible values, along with the associated likelihood for each point on the range – as opposed to a falsely precise and highly misleading fixed-point value – which is also known as a risk exceedance curve. Generally, business decisions about risk are made at the "long tail" end of the curve, i.e.,:

1. For a **$10B enterprise** with $1B in revenue at risk from a file-related data breach, is a 5% likelihood for the total business impact to exceed $200M / year an acceptable level of risk?

2. For a **$100B enterprise**, the likelihood of a data breach is significantly higher – and assuming $10B in revenue at risk from a file-related data breach, there's a 5% likelihood that the total business impact will exceed $6.3B / year. Is this an acceptable level of risk?

3. For **smaller business** with $100M in revenue, the likelihood of a data breach is much lower – and even assuming that all $100M is at risk from a file-related data breach, the 5% likely to exceed business impact in this scenario is about $8M per year. Is this an acceptable level of risk?

In fact, there's no one right answer. Business decisions regarding what do to about these risks (e.g., avoid? accept? transfer? take steps to manage to an acceptable level?) will vary from one organization to another, based on the context and the appetite for risk amongst their respective senior leadership teams. But this is the kind of analysis and quantification that helps to make a clear business case, and a better-informed business decision.

Reducing the Risk of Document-Related Ransomware: Two Strategies

With this in mind, let's look at the risk of **ransomware**, which is currently top of mind for organizations of all sizes. Although ransomware has been a weapon in the cybercriminal's arsenal since as early as 1989, it became a top of mind threat in the wake of publicity that followed massive, worldwide ransomware attacks such as Petya (2016), WannaCry (2017), and NotPetya (2017) – and most recently includes Ryuk, Cerber, and SamSam (2021).

Today, technically sophisticated and financially motivated attackers are constantly evolving and adapting their targeting and deployment of ransomware – to evade the protection mechanisms put in place by the defenders, and to maximize their own return on investment.

Ransomware refers to malicious code designed to gain unauthorized access to data, and encrypt the data to block access by legitimate users. Attackers then demand that victims pay a ransom, in exchange for the key to decrypt and recover their own data.

% difference, All Respondents, n = 1,357, Source: Aberdeen, July 2021

Key factors for the *likelihood* side of the risk of document-related ransomware include:

The annualized likelihood of experiencing at least one ransomware attack, and of those the likelihood of being attacked more than once.

The likelihood of a ransomware attack successfully infecting at least one endpoint, and of those the likelihood of subsequently expanding to infect multiple endpoints.

The existence of a cyber insurance policy that covers the payment of ransoms.

The ability to restore data quickly and effectively from backups.

Similarly, the business impact side of the risk of document-related ransomware has several potential factors, including:

Lost productivity of users and responders – i.e., the extent to which users are unable to do their jobs during the time the data they need is encrypted and unavailable.

Loss of current revenue – i.e., the extent to which data being encrypted and unavailable disrupts the organization's ability to generate revenue during the time of disruption.

Loss or exposure of sensitive data – i.e., the extent to which ransomware results in a data breach, with its associated costs, fines, and / or penalties. Recently, some have also been exfiltrating the encrypted data and threatening to disclose it unless payment is made, adding extortion to ransom as ways for the attackers to get paid.

Loss of future profitability – i.e., the extent to which the organization's handling of the ransomware attack results in lower revenue (e.g., customers take their business elsewhere) or higher costs (e.g., higher marketing expenditures required to attract and retain new customers).

The **total number of users** affected, **total volume of data to be recovered**, and **total time-to-recover** using current capabilities.

As another example, consider Aberdeen's quantitative analysis involving ransomware that affects traditional enterprise endpoints for 1,000 employees and a total of 10 TB of digital documents that potentially need to be recovered.

For simplicity, the analysis focuses on the lost productivity of users as the primary business impact – this analysis therefore reflects a conservative, understated estimate of the total business impact of ransomware in this scenario.

Based on these characteristics and research-based ranges for performance at data backup and recovery, Aberdeen's analysis estimates the annualized risk of document-related ransomware in this scenario as follows:

- Median (50% likely to exceed) about $500K
- "Long tail" (5% likely to exceed) $2.5M

As discussed previously, the question for the senior leadership team then becomes much more sharply focused: Is a 5% likelihood to exceed $2.5M / year an acceptable level of risk, for file-related ransomware?

If not, the quantitative analysis also helps to demonstrate the value of various technical strategies to reduce the risk of ransomware to a more acceptable level. For example, to reduce the risk of document-related ransomware here are two effective strategies to consider:

Containment – i.e., deploying technologies that are designed to monitor and detect the presence and initiation of document-based ransomware activities (e.g., file encryption) and quickly isolate and shut them down. This can significantly reduce the "blast radius" in terms of the number of users, endpoints, and files affected. This approach can significantly reduce the likelihood side of the risk of document-related ransomware.

Rapid Recovery – i.e., deploying technologies or services that are designed to improve the speed and scale of the data recovery process, whether on a device-by-device basis, or on an enterprise-wide scale. Increasingly, organizations are turning to cloud-based data backup and recovery solutions (e.g., DR as a Service) for these capabilities, as opposed to traditional in-house solutions. By reducing the total time-to-recover, this approach can significantly reduce the business impact side of the risk of document-related ransomware.

Summary and Key Takeaways

Documents – whether paper-based, or fully digital (i.e., files) – are an integral part of the core business processes and workflows for virtually every organization. These companies want not only to **enable the opportunities** for leveraging documents in the Digital Workplace, but also to **manage the risks**.

Your digital documents represent valuable data! A significant percentage of your organization's **intellectual property** is captured in its digital data, in the form of files. And your valuable data is at risk – e.g., from **data breaches**, and **ransomware** – which can and should be quantified in terms of how likely and how much business impact, to help senior business leaders make better-informed business decisions regarding what to do about it.

To reduce the risk of document-related ransomware, which is currently top mind for organizations of all sizes, here are two effective strategies to consider:

- **Containment** – i.e., monitoring, detecting, isolating, and shutting down ransomware attacks, significantly reducing the "blast radius" of document-related ransomware in terms of the number of users, endpoints, files affected.
- **Rapid Recovery** – i.e., improving the speed and scale of the data backup and recovery process, from individual devices to an enterprise-wide scale, significantly reducing the total time-to-recover from document-related ransomware.

Learn about Ricoh USA's Solutions