DOCAUTHORITY

What has DocAuthority done for you?

Barnaby Davies

January 2019

DocAuthority Confidential

DOCAUTHORITY

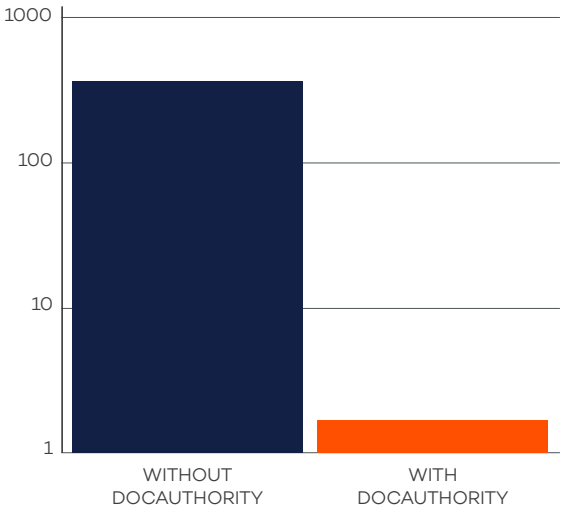
Overall comparison

Based on 50 TB of data and an average file size of 512KB, it will take one person 1798 years to complete the manual categorisation of all files in your organisation. To complete the work in 3 years it would take 600 people at an estimated cost of £89915392.

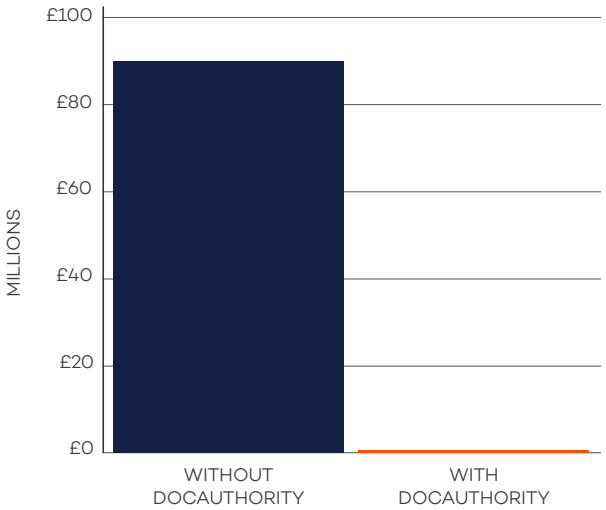
Carrying out the same activity using DocAuthority will use approximately 2 FTEs. The total cost of resource using DocAuthority is £255605.

Volume of work with and without using DocAuthority

Headcount Comparison



Resource cost comparison (£Ms)



DOCAUTHORITY

PCI-DSS: Assessment Findings

Volume of work with and without using DocAuthority

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers.

What did the assessment do?

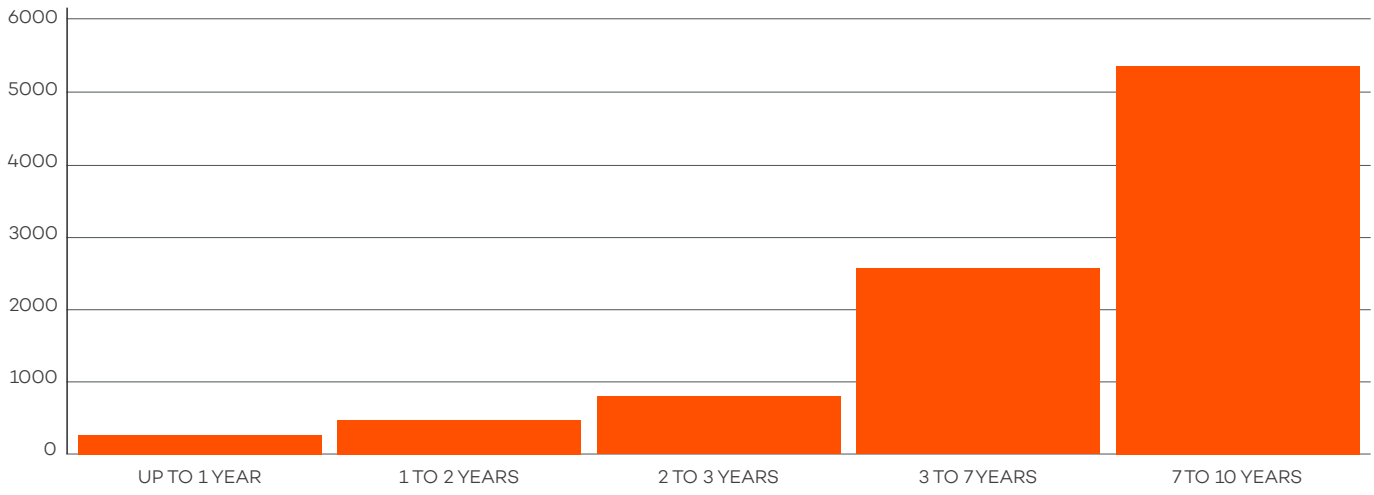
The assessment scanned a limited number of file shares, OneDrive and SharePoint repositories. The volume of data scanned was approximately 0.65% of Megacorp's data.

What did the assessment find?

- The assessment found 'x' files containing PCI data
- These files were found on 'y' servers, in 'z' countries and 'v' folders
- 'W' people in your estate can access some portion of these files
- Based on the assessment volumes, 'nnn' files are expected to found in your estate

---

Age of files



DOCAUTHORITY

PCI-DSS: Assessment Findings

Consequences?

1. Fines of between $5,000 & $100,000 per month
2. Infringement consequences
3. Compensation costs for PCI non-compliance
4. Legal action
5. Damaged reputation for PCI non-compliance
6. Revenue loss
7. Additional audit costs

Next steps?

- Map file locations to business units, provide reports to business owners
- Files moved to offline location where they can be reviewed / deleted
- Feed into training and communications to deter storage of PCI data

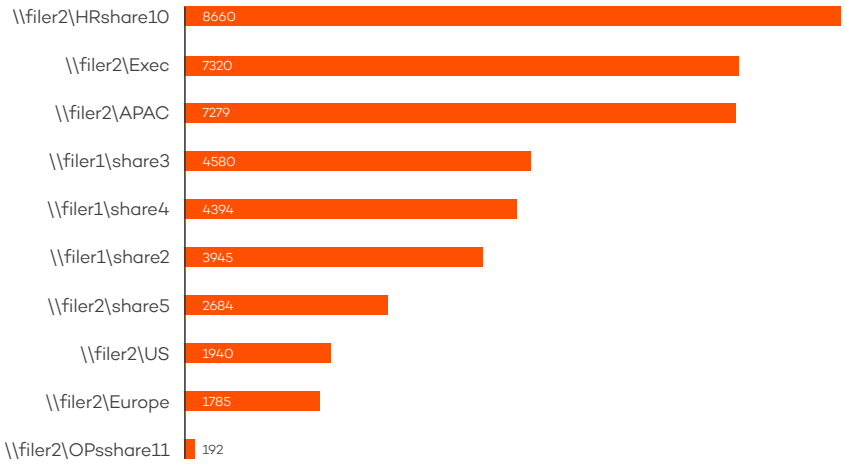
---

Benefits

1. Reduction in risk
2. Increased compliance
3. Reduced overhead and cost
4. Better understanding of business processes which can lead to PCI-DSS breaches
5. Opportunity for business units to remediate their own file shares

---

Top 10 Locations



DOCAUTHORITY

Retention: Assessment Findings

What is retention?

Under Data Protection law, Megacorp may not hold personal data longer than is necessary for the purposes for which the data was obtained. In addition, Megacorp is required to retain certain records to demonstrate compliance with statutory or regulatory requirements.

What did the assessment do?

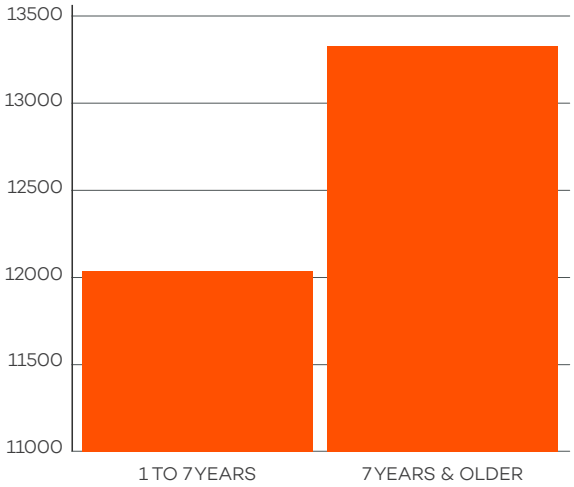
The assessment scanned a limited number of file shares, OneDrive and SharePoint repositories. The volume of data scanned was approximately 0.65% of Megacorp's data. 3 items on Megacorp's retention schedule were reviewed.

What did the assessment find?

- In all 3 instances documents were found which were beyond their retention schedule
- In the case of P11ds below, most were beyond their published retention date
- The P11ds were found in 'n' different folders making it very difficult for the business to find and apply retention protocols

---

P11ds by age



DOCAUTHORITY

Retention: Assessment Findings

Consequences?

1. Regulatory investigation and possible fines
2. Additional overhead an cost
3. Enforcement proceedings
4. Fines
5. An increase in the exercise of individual rights
6. Compensation claims

Next steps?

- Identify locations of all file types on retention schedule
- Analysis of age of files relative to retention schedule
- Consider what guidance is needed for for PII not included in retention schedule
- Move files beyond retention to offline storage for review / deletion

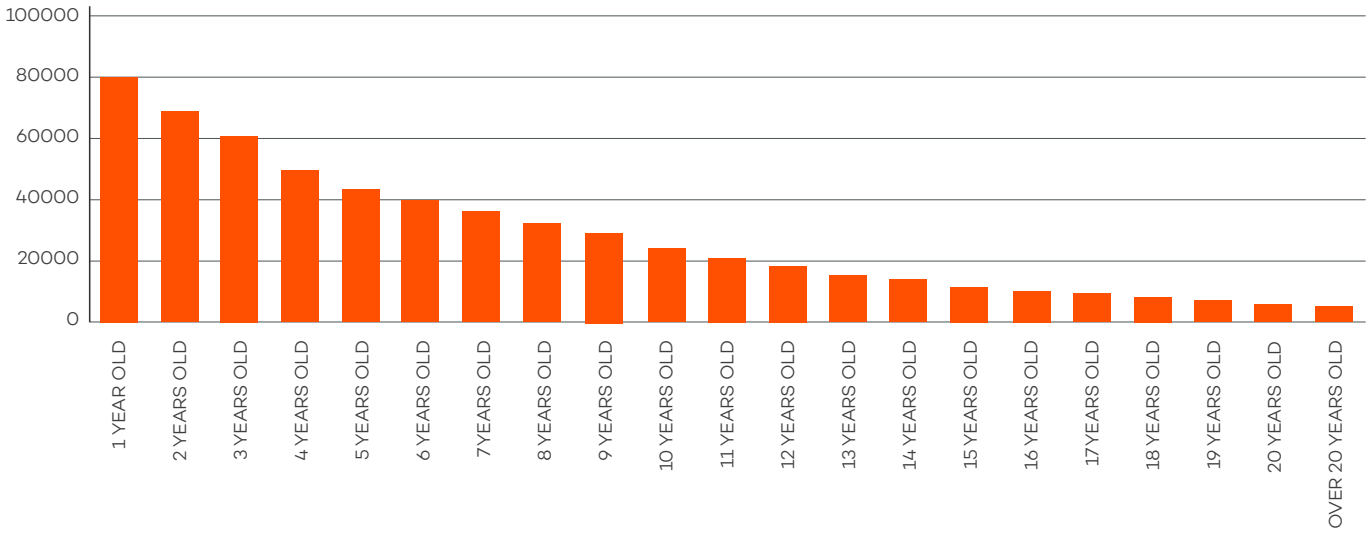
---

Benefits

1. 100% conformance to published retention schedules achievable
2. Ability to review which departments are performing records retention and which aren't
3. Fully auditable and opportunity to evidence retention activities to third parties

---

File volumes by age



DOCAUTHORITY

ACL Management: Assessment Findings

What is ACL Management?

Access control lists control who in your organisation has access to what data. You must ensure that you have appropriate security measures in place to protect the personal data you hold. This is the 'integrity and confidentiality' principle of the GDPR – also known as the security principle.

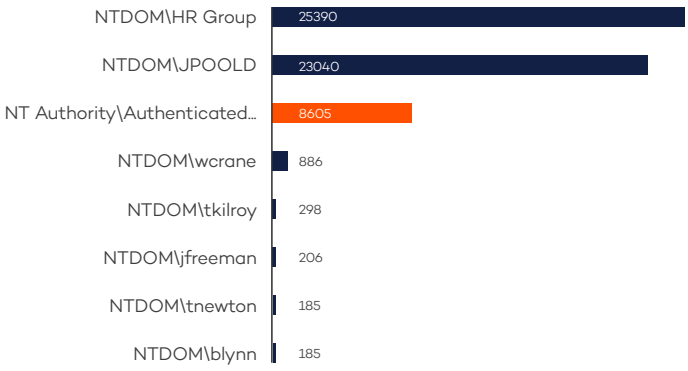
What did the assessment do?

The assessment scanned a limited number of file shares, OneDrive and SharePoint repositories. The volume of data scanned was approximately 0.65% of Megacorp's data. Efforts were made to find accounts with excessive privileges and sensitive data with weak access controls.

What did the assessment find?

- Sensitive information was found across numerous locations.
- While some folders had adequate controls, others clearly did not
- Sensitive information was easily accessible by unauthorised users
- A number of accounts with excessive privileges were found

Top 10 Locations



DOCAUTHORITY

ACL Management: Assessment Findings

Consequences?

1. ICO investigation, additional overhead and cost
2. Fines
3. Loss / breach of sensitive company information
4. Lost / breach of personal data and possible litigation

Next steps

- Engage Information Security SMEs to address accounts with excessive privileges
- Engage business stakeholders to understand their preferences to address unsecured sensitive data
- Assign data owners to align access to sensitive files with authorized usage
- Consider consolidating sensitive files to fewer locations so that access is easier to manage

---

Benefits

- Reduced likelihood of a breach (either malicious or via accident)
- Reduced risk and cost
- Business stakeholders can review and take corrective action

---

Name	Read access to number of files
NTDOM\ybryan	16021300
NTDOM\dascan	16021100
ExpiredUser	3731800
NTDOM\jpoole	3060700
NTDOM\wcrane	2172500
NTDOM\tkilroy	1495700
NTDOM\jfreeman	1353900
NTDOM\tnewton	876200
NTDOM\blynn	781600
NTDOM\Medical	738500
NTDOM\omichelle	457600
NTDOM\bdavies	360000
NTDOM\apennington	340100
NTDOM\jsmith	289100

DOCAUTHORITY

Obsolescence: Assessment Findings

What is obsolescence?

As much as 32% of an organisation's data is ROT. This is data identified as Redundant, duplicate, obsolete (no longer having business value), and trivial data with little or no business value. Businesses need to actively minimise ROT data by justifiably deleting it on a regular basis.

What did the assessment do?

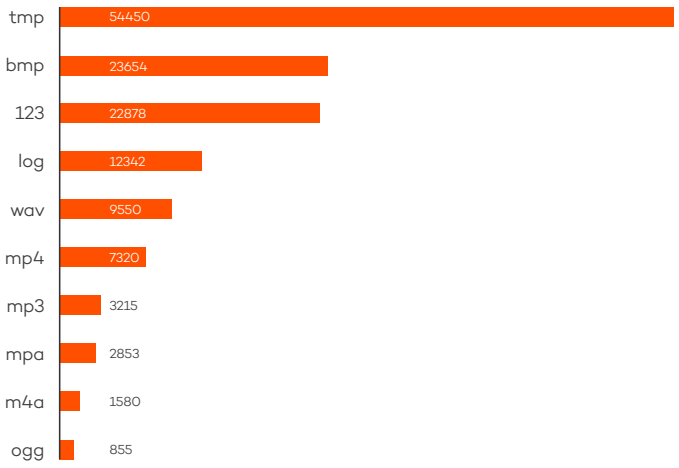
The assessment scanned a limited number of file shares, OneDrive and SharePoint repositories. The volume of data scanned was approximately 0.65% of Megacorp's data. Specific efforts were made to identify very old flies or file types felt to have limited value.

What did the assessment find?

- The assessment found a number of potential candidates for obsolescence
- There is a considerable number of multimedia files in legacy formats
- There are also a number of Lotus123 files for which there is no current means to open within Megacorp

---

File types by volume



DOCAUTHORITY

Obsolescence: Assessment Findings

Consequences?

1. Spiralling costs
2. Threat of possible disclosure
3. Risk of a breach of regulated data

Next steps?

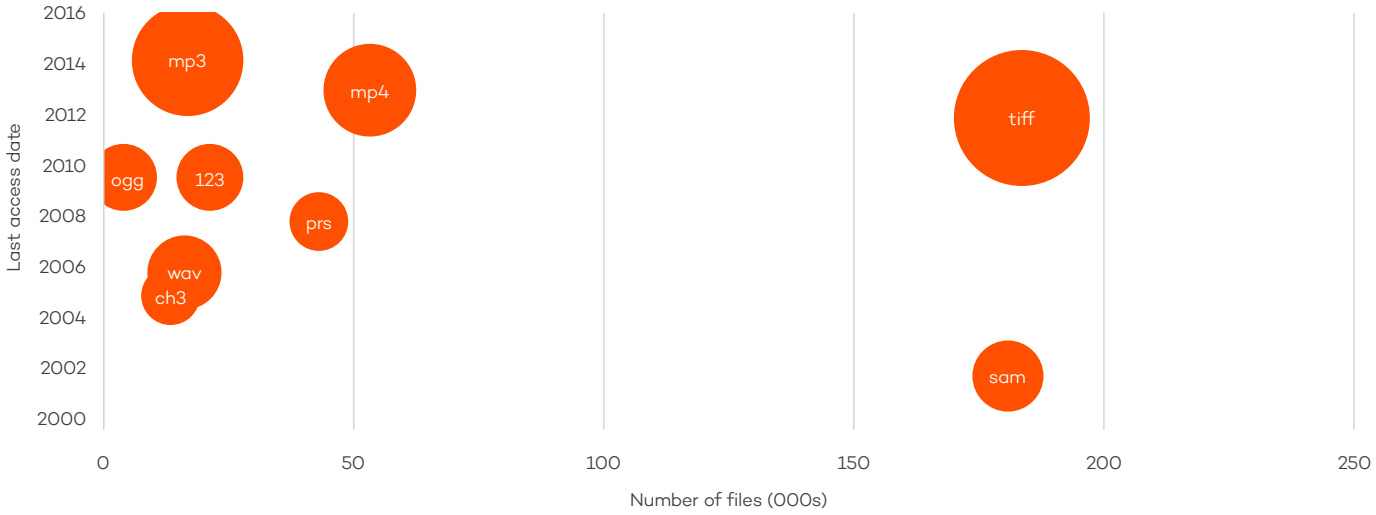
- Generate a criteria for what might comprise ROT in your organisation
- Analysis and reporting to identify quick / low risk wins
- Set policy on what ROT is, what should be done with it and who is responsible

---

Benefits

- Cost control / cost reduction
- Reduced risk
- Improved access and controls for high value business data
- Efficient tools to take corrective action

Legacy file types by number, volume and last access date



DOCAUTHORITY

PII: Assessment Findings

What is PII?

Personally Identifiable Information (PII) is information that relates to an identified or identifiable individual. Data protection laws require that you have a lawful basis to hold personal information, that it is accurate, that you do not store it for longer than is required, that you maintain it's accuracy and secure it appropriately.

What did the assessment do?

The assessment scanned a limited number of file shares, OneDrive and SharePoint repositories. The volume of data scanned was approximately 0.65% of Megacorp's data. Specific efforts were made to identify PII which was covered by Megacorp's retention schedule or was clearly obsolete.

What did the assessment find?

- The assessment found a number of significant file groups containing PII which were not included on any retention schedule
- PII in these file groups was not clearly safeguarded in terms of who had access to it
- Some of this data was sufficiently sensitive to present a risk to Megacorp
- Some of the files could be immediately deleted with no impact on Megacorp

---

Name	# files
P60s	16742
P11ds	7722
Job Description	5808
Eligibility form	5786
Progress Note	3828
Invoice	3520
Therapy services termination letter	3344
Medical leave request	3190
Employee Work Hours	3146
Offer letters	3080

DOCAUTHORITY

PII: Assessment Findings

Consequences?

1. Fines and litigation
2. Risk to reputation
3. Impact to revenue
4. Costs to mop up breach

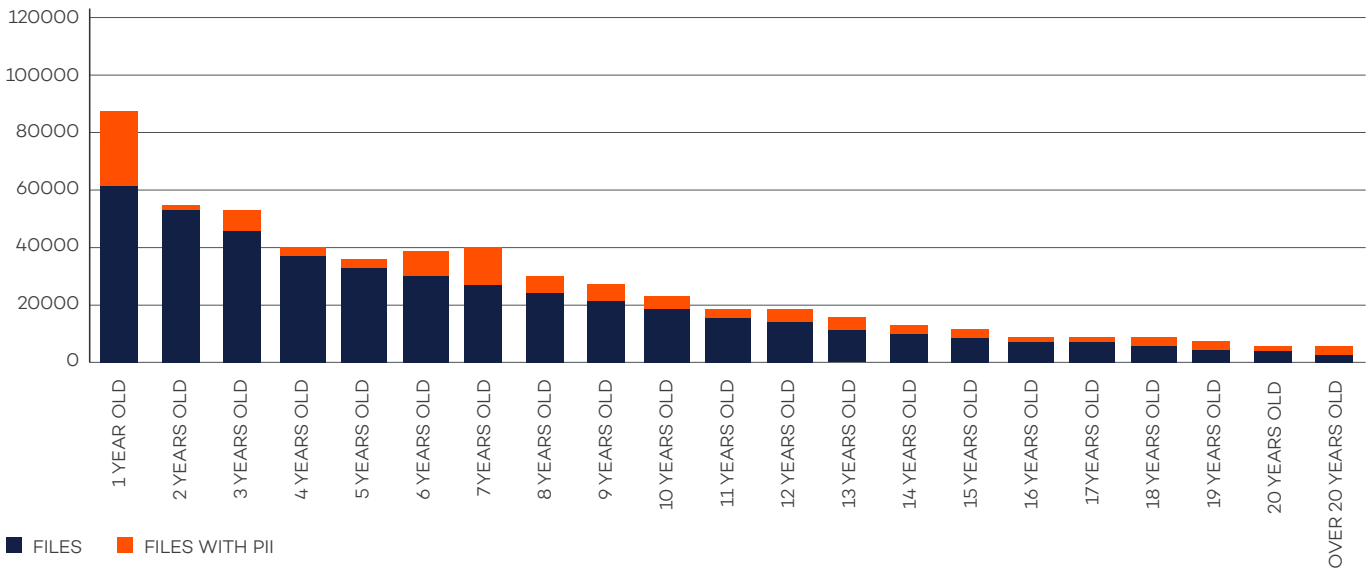
Next steps?

- Review your privacy notice to better understand what PII your organisation can lawfully hold
- Conduct and exercise to define the PII you seek to identify
- Mobilise an activity to catalogue PII held by Megacorp and implement appropriate safeguards
- Delete files which you have no lawful basis to process

Benefits

1. Reduced risks associated to data breaches
2. Ability to manage ACLs, security controls and confidentiality in a more selective and cost efficient manger
3. Reduced audit costs / overhead

Identified PII in files over time



DOCAUTHORITY

Enterprise search: Assessment Findings

What is Enterprise Search?

Enterprise search provides the means to quickly search using key words and business context. Information catalogued by DocAuthority can be searched and matching documents will be returned instantly. Search tools are particularly beneficial for 'knowledge workers' who develop products and services by applying knowledge they have acquired.

What did the assessment do?

By establishing a number of metrics the assessment was able to model and provide some forecasts for the savings available to Megacorp. This modelling was conducted using calculations taken from an IDC whitepaper "The High Cost of Not Finding Information"

What did the assessment find?

- 1200 staff in Megacorp are knowledge workers.
- The typical salary of a knowledge worker is £80K
- 53 subject access requests are received by Megacorp each year
- The volume of data not centrally indexed within Megacorp is 60%

Scenario 1: Time wasted searching

Not all information within an enterprise is searchable.

$$\left(\frac{\text{2.5 hours per week}}{\text{37.5 working hours}} \times 100 \right) = \textbf{8\% of time wasted}$$

1200 knowledge workers × 8% × £80K salary = **£7.68M**

£7.68M × 60% of data which is not indexed = **£4.6M per year**

DOCAUTHORITY

Enterprise search: Assessment Findings

Consequences?

1. Potential for bad decisions based on faulty information
2. Duplicated time and effort due to re-work
3. Lost productivity
4. Unrealised savings

Next steps?

- Consider implementing an enterprise search tool
- Let all knowledge workers use Enterprise Search
- Improve data accessibility using taxonomy and data inventory
- Publish a link to an enterprise search tool on your intranet
- Leverage an enterprise search tool to reduce DSAR costs or help with document retention activities

---

Scenario 2 : Cost of rework

This calculation captures the costs and inefficiencies that result primarily from intellectual rework, substandard performance, and inability to find knowledge. The resulting costs of this are estimated to £5850K per year per knowledge worker.

1200 knowledge workers × £5K salary = **£7.02M**

Scenario 3 : Opportunity cost

Based on 1200 knowledge workers and £45 /hr:

1200 × 45 × 2.5* × 50% failed searches = **£6.7K per week**

This equates to £351K per year

*2.5 (hours) is the amount of time each knowledge worker spends looking for information in a week