Information Risk and Governance – What You Need to Know to Make Your Organization Successful at Reducing Information Risk

Houston ARMA

Joe Shepley

February 27, 2019

DOCULABS

ARMA HOUSTON

What You'll Learn

- The enterprise risks posed by poor information governance
- Doculabs' perspective on how the information management landscape is shifting
- How other firms are using Privacy to drive better information governance and reduce enterprise risk
- Ways that you all can reduce enterprise risk at your organizations through better information governance
- Next steps

Introductions

Joe Shepley

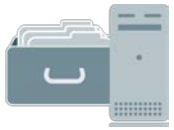
Vice President
and Practice Leader

The Information Risk of Poor Information Management

Poor information management affects:

Privacy and Information Security – larger risk footprint due to unmanaged sensitive content

E-discovery – higher cost, risk, and effort due to high volume of unmanaged content



Records Management – low/no compliance with corporate records management policy

IT – difficult/impossible to take a proactive approach to storage and network management due to high volumes of unmanaged content

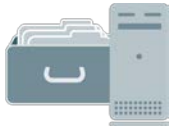
"The Business" – difficult to work at the "speed of business" when you can't deliver the right content to the right person at the right time

Benefits of Reducing Information Risk

Good information management can improve all of these domains:

Privacy and Information Security – less sensitive content to be compromised when a breach happens equals smaller risk footprint

E-discovery – less discoverable content equals lower per matter e-discovery costs



Records Management – more visibility into content equals better ability to comply with corporate records policy

IT – better understanding of what content lives where, owned by whom equals more effective storage and network management

“The Business” – less junk and stale content combined with better awareness of high value content equals less time spent searching for, creating, managing, and sharing content, more time doing their “real jobs”

But what's driving information risk?

MORE

- Data
- Types of data
- Ways to create, consume, and collaborate on data
- Data subject to more and stricter regulation
- Threats to data from inside and outside the organization

Protect

Lessen impact

Increase value

Knowledge

What data is on what systems, who owns it?

Access

Who can get to what?

Lifecycle

Keep only as long as obligated, then purge

Marketplace Perspective

- Three years ago, Privacy and Information Management were at best loosely coupled
- Responsibility for managing information lived in IT, RM, or Legal – Privacy just a stakeholder
- Within last 24 months, shift has begun for Privacy to own IM outright, or at least be a majority stakeholder
- Insurance (P&C and Health Payers) and Utilities (generation and transmission) leading the charge

Ask Yourself

Do I know what data lives in what systems, who owns it, who has access to it, and who is accessing it?

Do I have agreement from key stakeholders on how to manage sensitive data, junk data, and stale data to reduce risk and increase value?

Do I have the policy and compliance infrastructure in place to allow me to manage data to reduce risk and increase value?

Do I have the technology in place to allow me to manage data to reduce risk and increase value in an efficient and sustainable way?

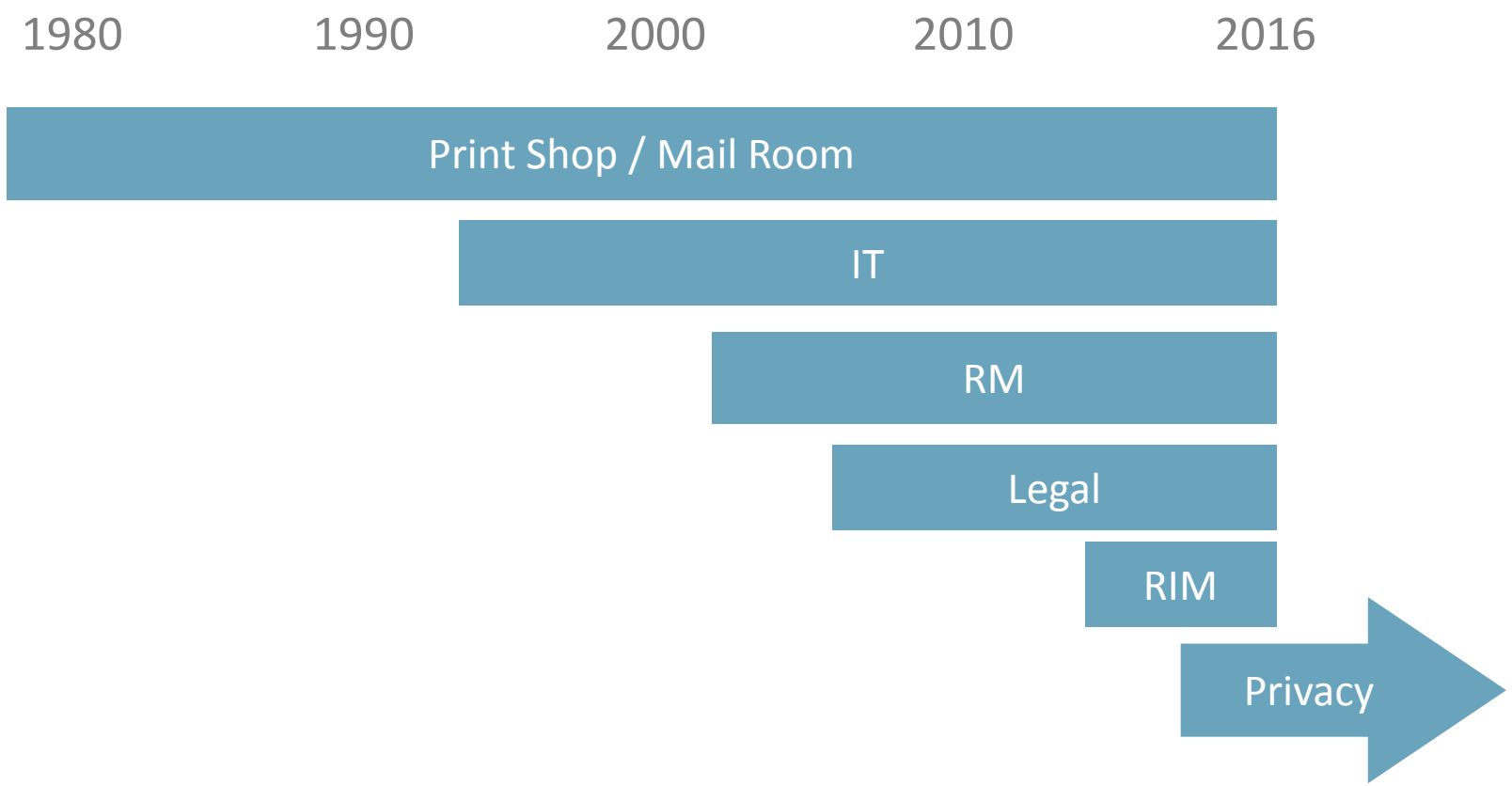
Why is it so hard to address information management?

The Problem with Information Management

- What is it?
- Corporate orphan
- Underwhelming technology
- Requires massive organizational change
- Weak business case

Help is on the way

Ownership is Shifting



Why Privacy Should Address Information Risk

- The question of a breach isn't ***if***, it's ***when***.
- When they get in, what will they find?
- When they find 5, 10, 15+ years of sensitive data that's past its legal and operational life, Privacy is on the hook - not records or IT.

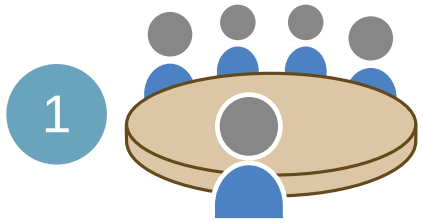
- Privacy needs to address information management to reduce the risk surface and do their job effectively.

How Information Management Can Help

- While Privacy typically has budget and organizational support, it (often) lacks information management expertise.

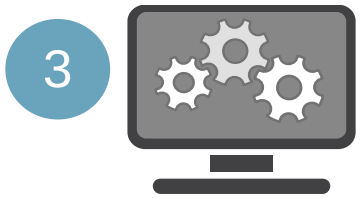
- Records and information management can help Privacy close this knowledge gap and be successful.

Scenario 1: Orphaned Data Cleanup and Disposition Approach (per Department)



Conduct initial department content scan. Use results to meet with department content owners to provide overview of scan results and agree on cleanup and disposition approach for orphaned data.

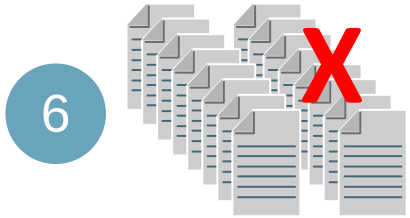
Assign data ownership for information to be moved based on the clean up rules in initial department scan.



Scan repositories based on established rules. Move orphaned data to destination or temporary repository.

Identify records in orphaned data set and flag with retention codes. Migrate to records management system if appropriate.

Identify legal holds on orphaned data set. Ensure they are flagged or migrated to legal hold repository.



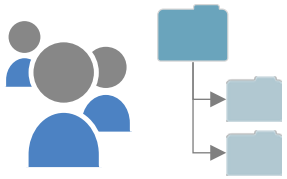
Move remaining identified orphaned data into temporary archive or dispose per rules.

Scenario 2: Shared Drive to SharePoint in 0365 Migration Approach (per department)

1

Conduct clean up of current repository by identifying records, legal hold, ROT, etc.

2



Work with business, content, or record owners to develop proposed folder and metadata structure for SharePoint.

3

Work with business, content, or record owners map to files and folders from source to target repository.

4

Obtain business approval on source to target mapping, folder structure, and metadata.

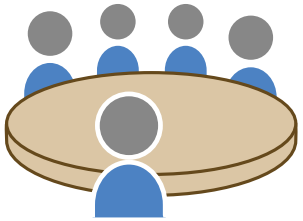
5

Using scripts or automated tools, migrate content from source to target repository (including source and target metadata).

6

Test the accuracy of content migration to target repository including source and target metadata assignment.

Scenario 3: Data Access Clean-up (per Department)



1

Conduct initial department content scan. Use results with department content owners to provide overview of initial scan results and agree on data access clean up approach.

2 Identify folders in the source repository that have global access.

3 Resolve broken inheritance and unresolved security identifiers.

4 Remove global groups (for both stale data and active data).

5 Model correct access and permissions.

6 Assign correct data owner.

Steps 2 – 6 are repeated for each of the folders that requires changes in their access and controls.

Case Study 1

Multi-state power-generation and natural gas utility

- 8,000 FTE and $6B in revenue
- Created records and information management strategy. Designed information management program structure.
- Authored records and information management policy and defined corporate information architecture.
- Used file analytics software to perform enterprise content scan and find junk, stale, and sensitive data. Defined content to move to Office365.
- Designed target SharePoint solution architecture and ran pilot implementations for key operational business units.

RESULTS

- Fully implemented information management program, staffed
- Office365 rollout in flight, meeting aggressive schedule
- Client Information Management team trained and ready to oversee remaining departments

Case Study 2

Global coal mining company

- 6,000 FTE and $4.7B in revenue
- Operated file analytics tool to perform departmental content scans to determine junk, stale, and sensitive data.
- Worked with departments to map existing records on shared drives to target state locations in records management repository.
- Performed content migrations and oversaw migration QA activities to ensure quality and effectiveness of migrations.

RESULTS

- Migrated 30+ departments from shared drives to records management repository.
- Cleaned up 30% - 40% of unneeded data – removed from migration.
- Assigned ~80% records across all departments.

Case Study 3

Global Exploration and Production oil company

- 3,300 FTE and $8.5B in revenue
- Used file analytics tool to identify stale, junk, and operational records for asset management business units.
- Defined future state SharePoint, SAP, and enterprise search solution to support more effective and compliant document management.
- Used file migration tool to migrate legacy content into future state solution.

RESULTS

- 66% of asset documentation under improved document management
- Reduction in rework and incidents due to wrong/missing documents

Case Study 4

A top blue health insurance provider serving about 3.7 million members in its state

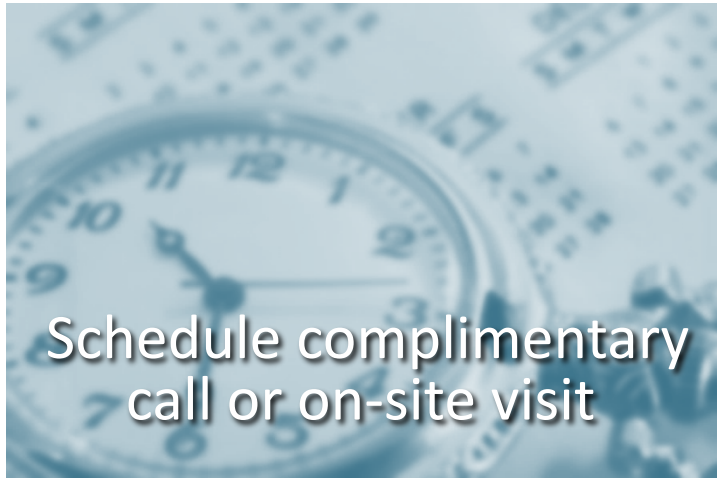
- 4,700 FTE and $6.5B in revenue
- Created unstructured data risk management strategy.
- Analyzed existing information management policies and authored remediated policies.
- Analyzed existing legal hold and e-discovery processes. Made recommendations for how to align with improved unstructured data management.
- Built sensitive data remediation approach and workplan.
- Assisted with content analysis and sensitive data identification as well as folder access remediation.

RESULTS

- 10TB+ of stale PHI and PII removed from file shares and SharePoint
- 50K+ folders with overly permissive access remediated

Questions, Comments, Feedback?

Next Steps



Joe Shepley

773.827.2945

jshepley@doculabs.com

Thank You

Joe Shepley

773-827-2945

jshepley@doculabs.com

DOCULABS