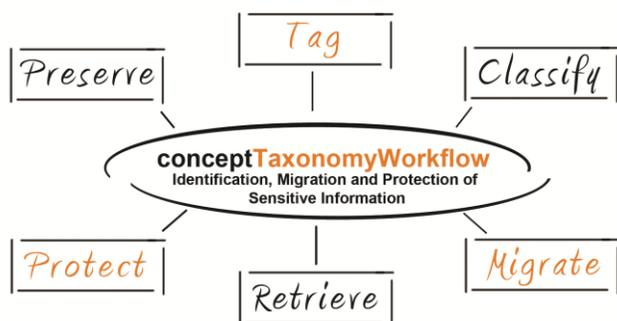# conceptSearching

conceptTaxonomyWorkflow Solution Overview

Preventing Data Exposure

Metadata driven Identification, Migration and Protection of Sensitive Information

Are you at Risk of Sensitive Data Exposure?

Managing private data effectively is a critical initiative in many organizations where a data breach can lead to severe legal and financial repercussions. With new government oversight and regulations such as Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley Act (SOX), the Privacy Act, the Occupational Safety and Health Act (OSH Act), International traffic in Arms Regulations (ITAR) and the Payment Card Security Standards (PCI Security Standards), organizations are under increasing pressure to ensure compliance and protection of data - whether it is confidential customer information, restricted employee information or sensitive business information.

As private and public institutions embrace more electronic processes in order to reduce costs and improve services to customers or citizens, it has become essential to counter the increased risks of data exposure. But the amount of data created every day by business is staggering and is increasing at a compound annual growth rate of 60%. With over 253 million data breaches in both the public and private sector since 2005, all organizations must proactively address privacy data protection issues to reduce risks and potential liabilities.

Protecting and Preserving the Confidentiality of each Document

Years ago, we had specific applications to hold specific content, but that demarcation has been broken down by the introduction of platforms such as SharePoint. Data kept SharePoint tends to be loosely organized, relying on users to classify and manage the lifecycle of their content.

However, manual tagging is at best subjective and at worst dangerous: IDC confirms that *less that 50% of content is correctly indexed, meta tagged or efficiently searchable* (and that *85% of relevant documents are never retrieved in searches*.

A breach doesn't have to include PII (Personally Identifiable Information) or PHI (Protected Health Information), the effects of losing or accidentally publishing any confidential or sensitive documents can be catastrophic to an organization.

So what is to be done? In essence, a company can reduce their exposure by identifying, tagging, and then moving documents of record to the appropriate repository, governed by the appropriate security rules.

The **conceptTaxonomyWorkflow** module delivers workflow capabilities that enable intelligent automatic detection of sensitive or protected information in a document for it then to be routed to a secure location. This process interrogates the text content of all documents for any sensitive terminology that will be automatically identified and used to lock down these sensitive documents.
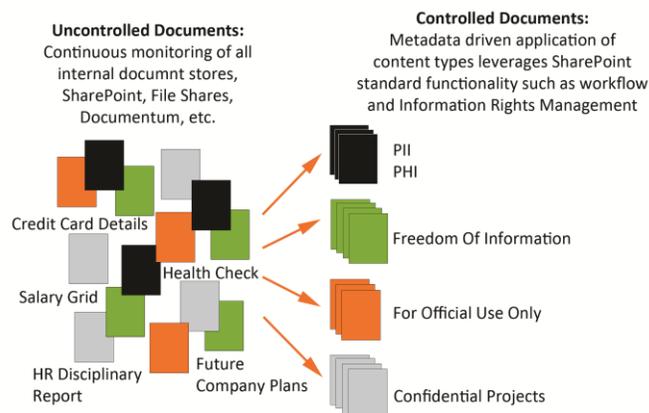
The conceptTaxonomyWorkflow module can be configured to identify and classify any type of organizationally-defined confidential or sensitive information

conceptSearching

The challenges facing all organizations include:

- Lack of tools to identify all possible privacy data exposures at the time of content creation, modification and migration

- Lack of end user compliance to segregate content from the network and ensure that uploaded privacy data is not available for general access

- Lack of governance to enforce the meta-tagging of documents based on content by end users

- Stovepipe applications which prohibit the ability to identify privacy data from within content

- Inability to automatically identify PII and exposure risks in real time

- Inability to ensure protected data assets are subject to portability and security controls

- Only 35% of all breaches involved the loss or theft of a computer or device (*Ponemon Institute*)

- Overall 70% of all breaches were due to a mistake or malicious intent by an organization's own staff (*Ponemon Institute*)

The effect on the bottom line:

- Average cost of a data breach was $6.3 million and ranges from $225K to $35 million (*Ponemon Institute*)

- The average cost per exposed record is $197 and ranges from $90 - $305 per record (*Ponemon Institute*)

Affected documents can then be controlled by performing an appropriate workflow action:

- Moving the document

- Changing its Content Type

- Automatic application of Information Rights Management

- Notifying an administrator by email

It's not about Search, but the Proactive Management of the Lifecycle of the content.

Taxonomy Workflow for Detecting and Routing

With the **conceptClassifier for SharePoint** and the **conceptTaxonomyWorkflow** module organizations can now use semantic metadata to automate the tagging of unstructured documents to deliver many automated processes:

- Build business specific confidential document detection taxonomies

- Align content to business goals

- Consistently apply document policies

- Leverage native SharePoint controls and functionality

- Ensure consistent tagging across the organization

- Perform automatic routing based on the text content of each document

For The Record

The effect on Management

- 86% say their job would be at risk if a security incident were to occur (Websense)

- 72% of IT Managers said protecting company data is more stressful than getting a divorce (Websense)

The effect on organization's brand and reputation

- In the event of a data breach, the value of brand and reputation could decline by as much as 17-30% of annual gross revenues (Ponemon Institute)

- Restoring a company's reputation after a data breach can take on average one year (Ponemon Institute)

- 65% of citizens expressed little confidence that government can be trusted to maintain and protect records about them appropriately (add source)

Microsoft Partner

Gold Independent Software Vendor (ISV)
Silver Content Management
Silver Search
Silver Portals and Collaboration