


Classification Policies

CSH5 Chapter 67
 “Developing Classification Policies for Data”
 Karthik Raman & Kevin Beets



Copyright © 2014 M. E. Kabay. All rights reserved.

TOPICS




- Introduction
- Purpose / Benefits
- Role in IA
- Legal Requirements
- Design & Implementation
- DC Solutions



Copyright © 2014 M. E. Kabay. All rights reserved.

Introduction

TOP SECRET



- Popular literature / media refer to “TOP SECRET”
 - ❑ No clear understanding of issues
 - ❑ Misrepresentation as negative: hiding information from stakeholders
- Data classification
 - ❑ Labels info to support compliance with data-protection policies
 - ❑ Historically used by government, military, government contractors
 - ❑ Now increasingly used to comply with legal requirements on commercial organizations
 - ✓ Financial / operational records
 - ✓ Privacy protection


Copyright © 2014 M. E. Kabay. All rights reserved.

Purpose / Benefits

- Information life cycle management (ILM)
 - ❑ Control of data
 - ❑ Throughout life cycle
 - ✓ Creation
 - ✓ Access
 - ✓ Modification
 - ✓ Destruction
- Legal requirements increasing pressure in private sector; e.g.,
 - ❑ HIPAA
 - ❑ European Privacy Directive


Benefits

- Compliance with data standards, legal requirements
- Streamlined/secure data sharing
- Efficient data storage / retrieval
- Tracking data through ILM



Copyright © 2014 M. E. Kabay. All rights reserved.


Role in IA




- Federal Financial Institutions Examinations Council (FFIEC) guidelines
 - ❑ Ensure consistent protection of data
 - ❑ Focus controls / efforts efficiently
 - ❑ Systems must be classified at highest level of information stored / transmitted
- Supports risk analysis
- Clarifies basis for access restrictions
- Supports business continuity planning & disaster recovery planning
- May be *mandatory*
- *Necessary for data-loss prevention (DLP)*

Copyright © 2014 M. E. Kabay. All rights reserved.

Legal Requirements in US




- Privacy Act of 1974
 - ❑ Including Computer Matching & Privacy Protection Act of 1988
- Family Educational Rights & Privacy Act (FERPA)
- Health Insurance Portability & Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- Federal rules of Civil Procedure (FRCP)



Copyright © 2014 M. E. Kabay. All rights reserved.

Compliance Standards (1)

- US Federal Government Executive Order 12958
 - ❑ Further Amendment to Executive Order 12958... Classified National Security Information
- ISO/IEC 27001:2005
 - ❑ Guidelines & principles for information security management
 - ❑ 5 levels
 - ✓ Public documents
 - ✓ Internal use only
 - ✓ Proprietary
 - ✓ Highly confidential
 - ✓ Top secret



7

Compliance Standards (2)

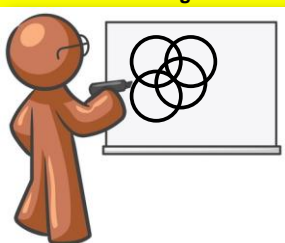
- Defense contracting (DoD)
- Finances (Federal Financial Institutions Examination Council – FFIEC)
- Life sciences (FDA)
- Media, telecom (FCC)



8

Design


- Obtain management approval
- Study BCP, IT assets, storage-management
- Present benefits DC to business unit (BU) heads
- Survey users in BUs re data utilization / management & preferences for organization & labeling
- List revenue-generation & mission-critical usage of data for each BU;
- Study information sharing



9

Implementation

- Obtain management approval
- Map data-labeling to available hardware, networks, systems, storage
- Apply automation / DC tools as appropriate
- Guide users through adoption & solicit feedback
- Develop service-level agreements (SLAs) for data usage
- Plan for DLP
- Develop cost model
- Report results to management



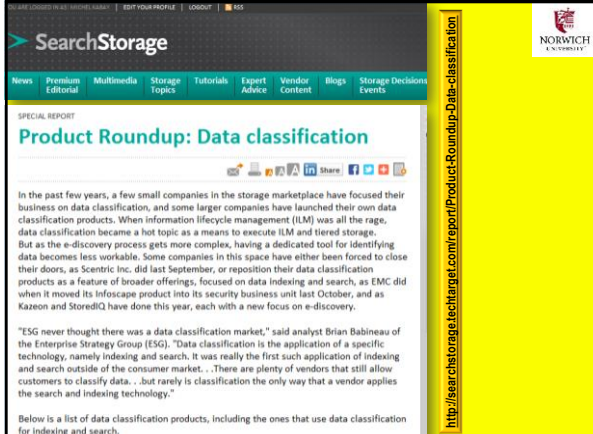
10

DC Solutions

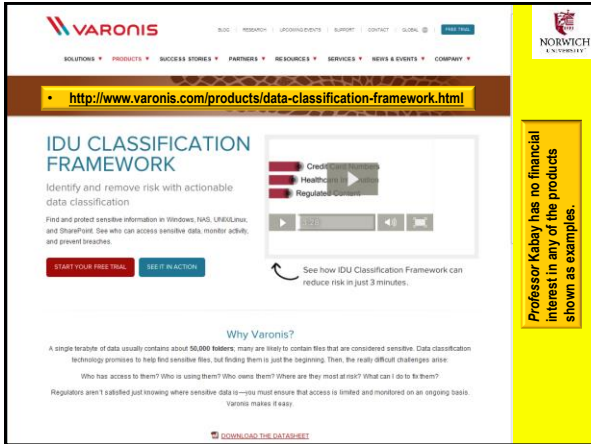
- Primarily related to data storage
 - ❑ Virtualization
 - ❑ Deduplication
 - ❑ Cheaper media
- Features of DC software
 - ❑ Policy-based data-type discovery
 - ❑ File metadata classification
 - ❑ Multiple file system management
 - ❑ Compliance & legal consideration
 - ❑ Report style



11



12



VARONIS

<http://www.varonis.com/products/data-classification-framework.html>

IDU CLASSIFICATION FRAMEWORK

Identify and remove risk with actionable data classification

Find and protect sensitive information in Windows, NAS, UNIX/Linux, and SharePoint. See who can access sensitive data, monitor activity, and prevent breaches.

START YOUR FREE TRIAL | SEE IT IN ACTION

See how IDU Classification Framework can reduce risk in just 3 minutes.

Why Varonis?

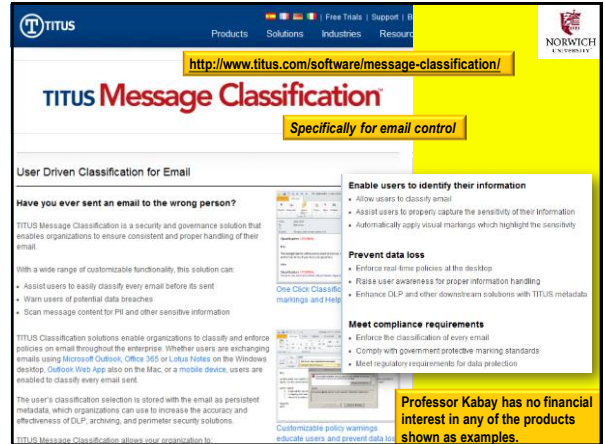
A single terabyte of data usually contains about 50,000 folders, many are likely to contain files that are considered sensitive. Data classification technology promises to help find sensitive files, but finding them is just the beginning. There are really difficult challenges ahead:

- Who has access to them? Who is using them? Who owns them? Where are they? Most of all? What can I do for them?

Regulators aren't satisfied just knowing where sensitive data is - you must ensure that access is limited and monitored on an ongoing basis. Varonis makes it easy.

DOWNLOAD THE DATASHEET

Professor Kabay has no financial interest in any of the products shown as examples.



TITUS

<http://www.titus.com/software/message-classification/>

TITUS Message Classification

Specifically for email control

User Driven Classification for Email

Have you ever sent an email to the wrong person?

TITUS Message Classification is a security and governance solution that enables organizations to ensure consistent and proper handling of their email.

With a wide range of customizable functionality, this solution can:

- Assist users to easily classify every email before its sent
- Warn users of potential data breaches
- Scan message content for PII and other sensitive information

TITUS Classification solutions enable organizations to classify and enforce policies on email throughout the enterprise. Whether users are exchanging emails using Microsoft Outlook, Office 365 or Lotus Notes on the Windows desktop, Outlook Web App also on the Mac, or a mobile device, users are enabled to classify every email sent.

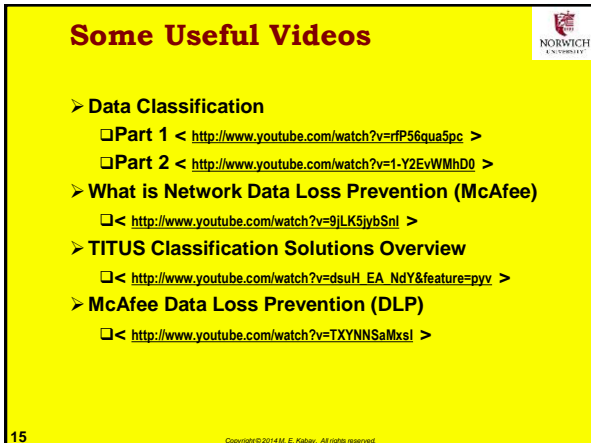
The user's classification selection is stored with the email as persistent metadata, which organizations can use to increase the accuracy and effectiveness of DLP, archiving, and perimeter security solutions.

TITUS Message Classification allows your organization to:

- Enable users to identify their information
 - Allow users to classify email
 - Assist users to properly capture the sensitivity of their information
 - Automatically apply visual markings which highlight the sensitivity
- Prevent data loss
 - Enforce real-time policies at the desktop
 - Raise user awareness for proper information handling
 - Enhance DLP and other downstream solutions with TITUS metadata
- Meet compliance requirements
 - Enforce the classification of every email
 - Comply with government protective marking standards
 - Meet regulatory requirements for data protection

Customizable policy warnings educate users and prevent data loss

Professor Kabay has no financial interest in any of the products shown as examples.



Some Useful Videos

- Data Classification
 - ❑ Part 1 < <http://www.youtube.com/watch?v=rfP56qua5pc> >
 - ❑ Part 2 < <http://www.youtube.com/watch?v=1-Y2EwWmhD0> >
- What is Network Data Loss Prevention (McAfee)
 - ❑ < <http://www.youtube.com/watch?v=9jLK5jybSnI> >
- TITUS Classification Solutions Overview
 - ❑ < http://www.youtube.com/watch?v=dsuH_EA_NdY&feature=pyv >
- McAfee Data Loss Prevention (DLP)
 - ❑ < <http://www.youtube.com/watch?v=TXYNNSaMxsl> >

15

Copyright © 2014 M. E. Kabay. All rights reserved.



DISCUSSION

16

Copyright © 2014 M. E. Kabay. All rights reserved.