Protecting Information Assets
- Week 3 -

Data Classification Processes and Models

MIS5206 Week 3

- Readings
- In the News
- Data Classification Processes and Models
- Test Taking Tip
- Quiz

Reading

- Vacca Chapter 14
- “In the News” article
- Continue Analysis: Case 1
- ISO 27001 – Assignment 1

In the News

Recommended Presentations from Cyber Defense Summit 2014

Content from the SANS Cyber Defense Summit (full agenda – pdf) last month

https://www.novainfosec.com/2014/09/04/recommended-presentations-from-cyber-defense-summit-2014/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+novainfosecportalblog+%28NovaInfosec.com+Blog%29&utm_content=FeedBurner

Data Classification Processes and Models

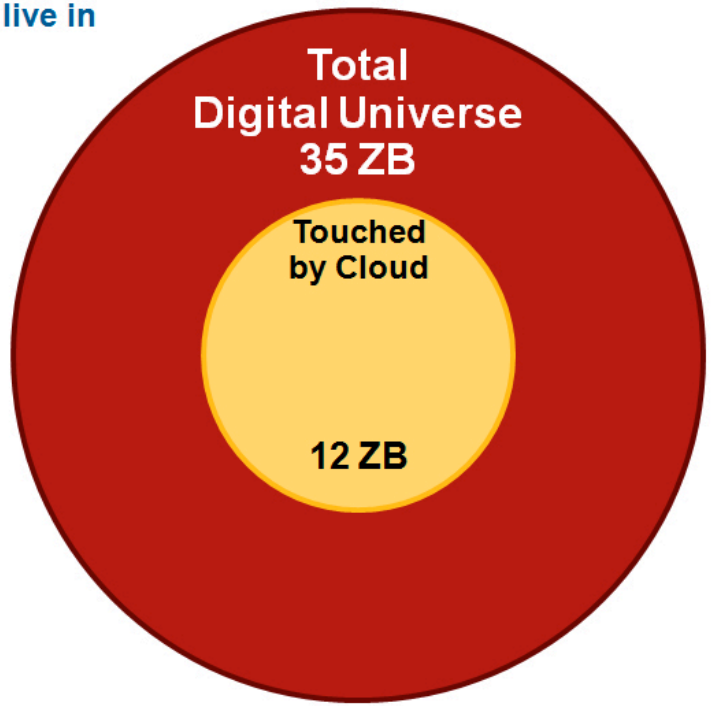
Data classification is essential to ensuring that data is appropriately protected and done so in the most cost-effective manner. The goal is to classify data according to its risk associated with its loss or disclosure and to identify the level of confidentiality, integrity and availability required.

Projected Growth of Data

The Digital Universe in the Clouds, 2020

EMC² where information lives®

By 2020, more than a third of the Digital Universe will either live in or pass through the cloud



Source: IDC Digital Universe Study, sponsored by EMC, May 2010

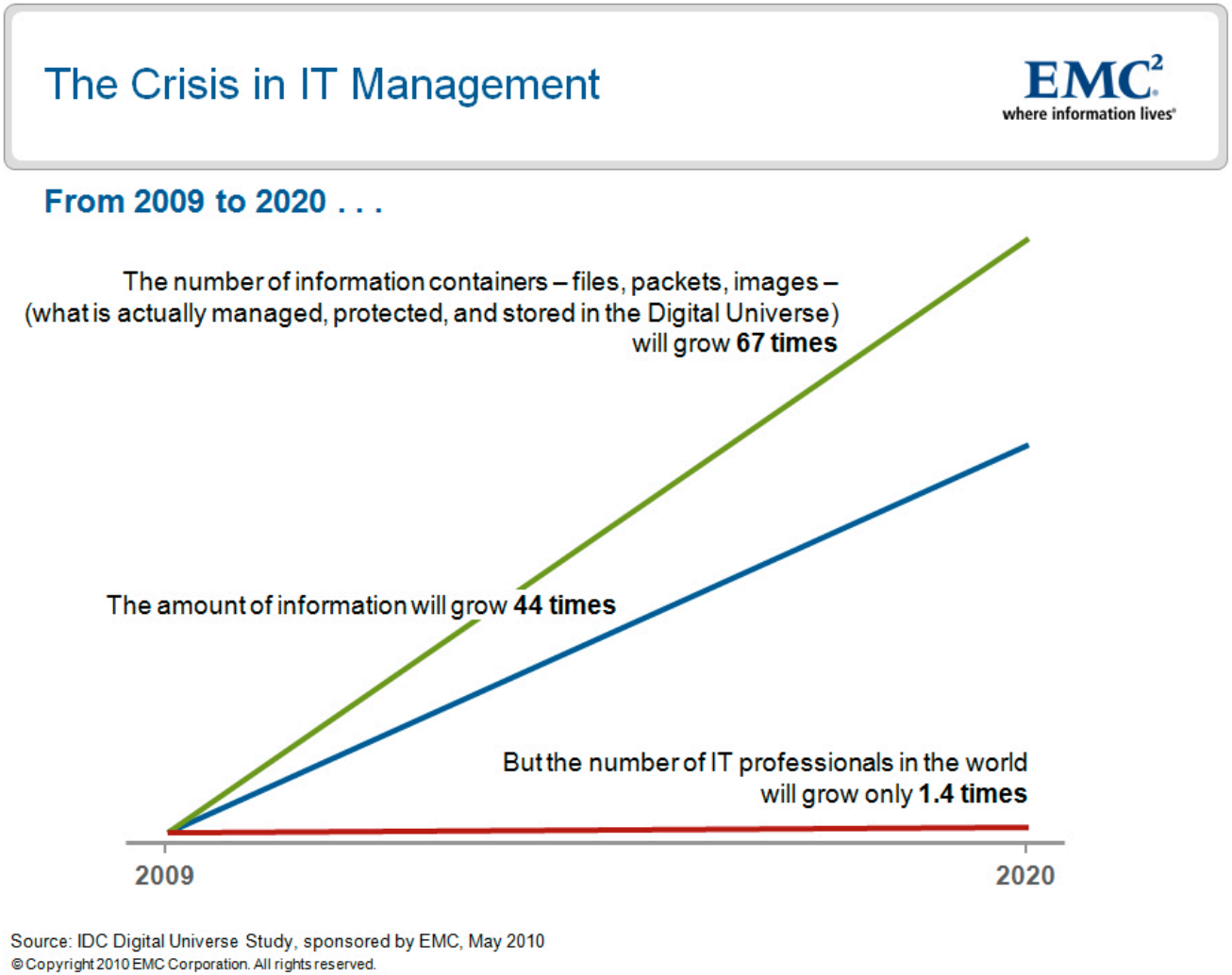
Projected Growth of Data

What is a Zetta Byte?

Kilobyte
Megabyte
Gigabyte
Terabyte
Petabyte
Exabyte
Zettabyte

A zettabyte is a quantity of information or information storage capacity equal to 1021 bytes. Research from the University of California, San Diego reports that in 2008, Americans consumed 3.6 zettabytes of information.

Projected Growth of Data

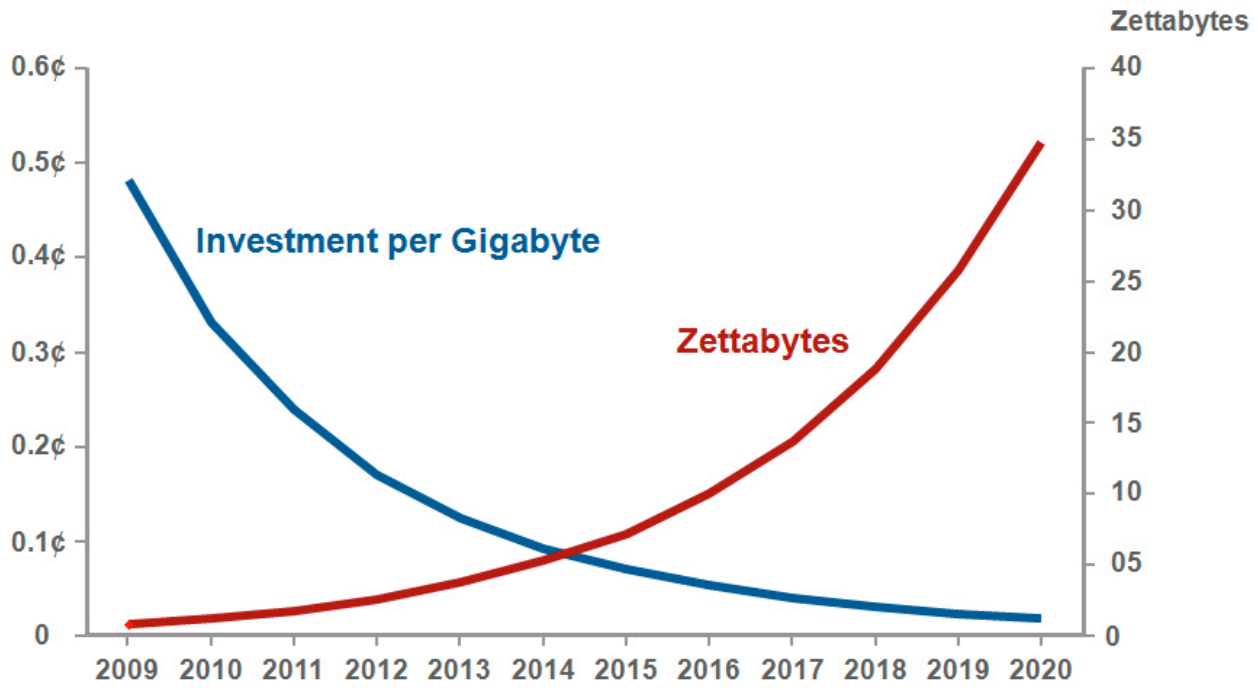


Projected Growth of Data

The Decreasing Cost of Managing Information will be an Incentive to Create More Information

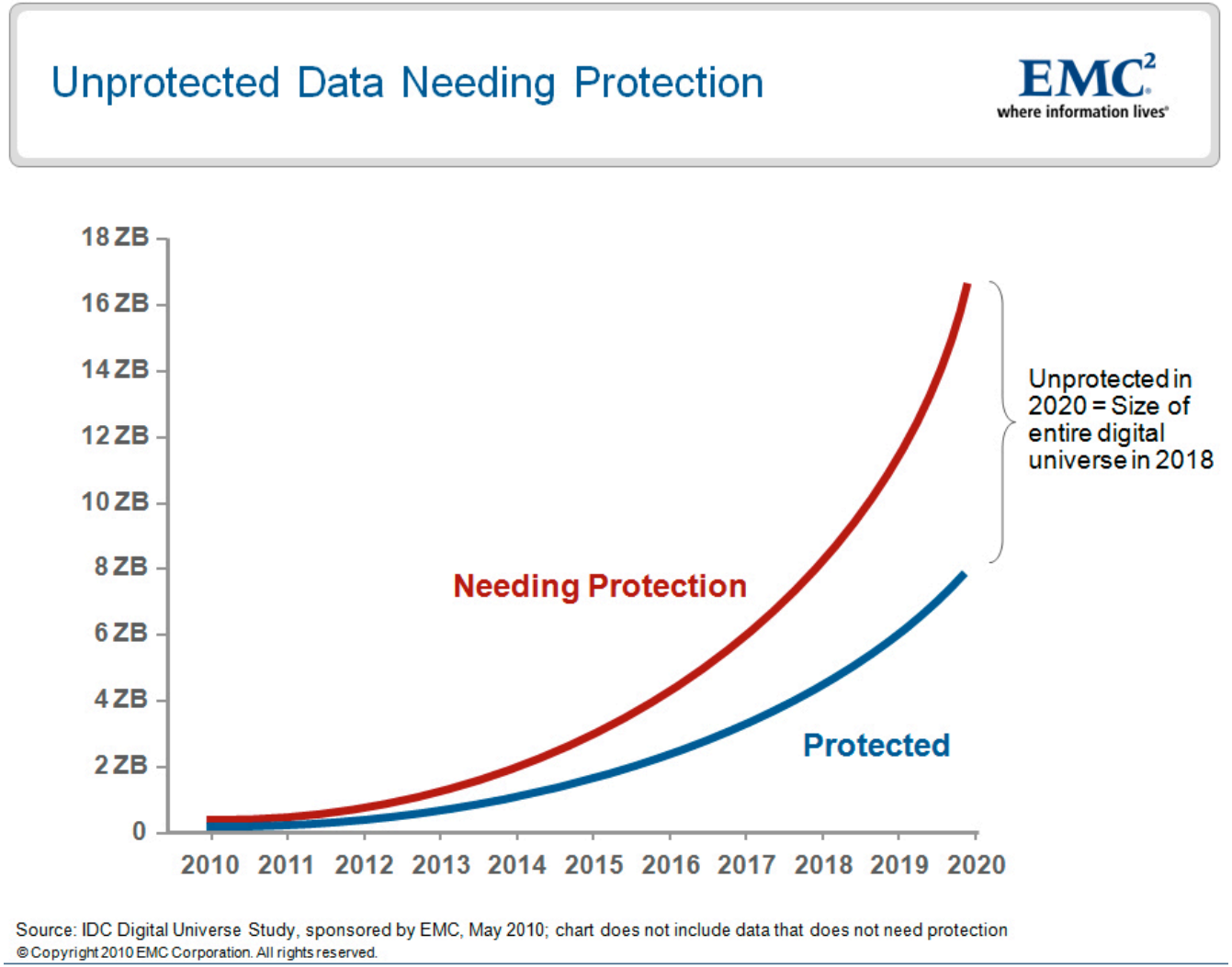
EMC² where information lives®

Total Investment in the Digital Universe: $4 Trillion in 2009



Source: IDC Digital Universe Study, sponsored by EMC, May 2010

Projected Growth of Data



Key Concepts

Classification	Grouping of data according to pre-determined types
Cost-Effectiveness	Appropriateness of the level of risk mitigation expenditure
Confidentiality	Restriction who may know about and/or have access to information
Integrity	Confidence that information is complete and unaltered
Availability	Access to information

Data Retention

Why have a formal data retention policy?

- Applicable Laws and Regulations
- Resource Limits
- Privacy
- Access
- Security
- Plagiarism and Copyright
- Enforcement

Data Retention

Why companies need to do have a formal data retention policy now

- Practical Concerns
- Regulatory Concerns
- Privacy Concerns

Data Retention

Practical Concerns

Data Retention

Regulatory Concerns

DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 15 March 2006

on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the Opinion of the European Economic and Social Committee (1),

Acting in accordance with the procedure laid down in Article 251 of the Treaty (2),

erased or made anonymous when no longer needed for the purpose of the transmission of a communication, except for the data necessary for billing or interconnection payments. Subject to consent, certain data may also be processed for marketing purposes and the provision of value-added services.

(4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.

Data Retention

Privacy Concerns

- **Support Petition Against Data Retention**
  The EDRI and XS4ALL petition against data retention has attracted almost 42,000 signatures, of which over 16,000 are from the Netherlands (where the campaign was launched) and over 5,000 from Germany and Finland. Runners-up in the daily country count are Sweden and Bulgaria (almost 2,000 each), followed by Austria (almost 1,500) and Italy (well over 1,000). Belgium, Slovenia and France have each almost reached 1,000 signatures.

  Currently, 66 organizations and companies have signed in support of the petition. The petition is now available in 17 languages.

Data Retention

Establishing a Data Retention Policy

- Establishment of Data Classes
- Classification of Data
- Establishment of Retention Periods
- Selection of Archive Methods
  - Paper-based
  - Electronic forms
- Creation of End-of-Life Processes
- Creation of Policies for Destruction of Media
- Identification of Roles and Responsibilities
- Creation of Enforcement Mechanisms

Data Retention

Handling Customer Data

- Conduct an enterprise application compliance review
- Implement Payment Application Data Security Standard (PA-DSS)
- Pilot data tokenization solutions
- Implement end-to-end encryption
- Restrict Internal access to customer data

Data Governance Roles

Owner	Steward	Custodian
Manages the business function that generates and/or uses the data. Has business and/or regulatory responsibility for data quality and management.	Focuses on managing data content and the business logic behind all data transformations.	Oversees the safe transport and storage of data. Focuses ion the underlying infrastructure and activities required to keep the data intact.

Examples of Classifications

The need to protect information has different characteristics in different sort of organizations. The principle distinction is between Government and Business. But, the terms used overlap in scope and are often intermingled sometimes resulting in confusion

Unclassified
Sensitive but unclassified (SBU)
Public
Confidential
Client Confidential
Company Confidential
Sensitive
Proprietary
Private
Secret
Top secret

Information Security Classification

Information Category	Description	Examples
Unclassified Public	Information is not confidential and can be made public without any implications for Company. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	• Product brochures widely distributed • Information widely available in the public domain, including publicly available Company web site areas • Sample downloads of Company software that is for sale • Financial reports required by regulatory authorities • Newsletters for external transmission
Proprietary	Information is restricted to management-approved internal access and protected from external access. Unauthorized access could influence Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	• Passwords and information on corporate security procedures • Know-how used to process client information • Standard Operating Procedures used in all parts of Company's business • All Company-developed software code, whether used internally or sold to clients
Client Confidential Data	Information received from clients in any form for processing in production by Company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Client media • Electronic transmissions from clients • Product information generated for the client by Company production activities as specified by the client
Company Confidential Data	Information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Salaries and other personnel data • Accounting data and internal financial reports • Confidential customer business data and confidential contracts • Non disclosure agreements with clients\vendors • Company business plans

Test Taking Tip

- Look for "subset" questions -

Often you will encounter questions that ask you to chose the "Best" answer.

The ideas is that at least two of the answers are correct in some sense but one is "more correct" than the others.

It can be useful to view these types of questions as having some possible answers that are actually subsets of the most correct answer.

Test Taking Tip

Example:

An attack that involves an attacker creates a misleading context in order to trick a user into making an inappropriate security-relevant decision is known as:

a) Spoofing attack
b) Surveillance attack
c) Social engineering attack
d) Man-in-the-middle attack

Test Taking Tip

Example:

An attack that involves an attacker creates a misleading context in order to trick a user into making an inappropriate security-relevant decision is known as:

a) Spoofing attack
b) Surveillance attack
c) Social engineering attack
d) Man-in-the-middle attack

Test Taking Tip

Example:

An attack that involves an attacker creates a misleading context in order to trick a user into making an inappropriate security-relevant decision is known as:

a) Spoofing attack
b) Surveillance attack
c) Social engineering attack
d) Man-in-the-middle attack

Answer: C

Quiz