



# Sensitive Data Disclosed

**LSEC & Agoria-ICT DLP Event**

*December 16<sup>th</sup>, 2008*

**Wouter Janssen**

*woujanssen@deloitte.com*



**Audit • Tax • Consulting • Financial Advisory.**

## Agenda

- What is data leakage
- Incident risk analysis
- Business considerations & challenges
- Data protection: a starting point
- An approach for data protection
- Questions & answers

## What is Data Leakage?



## Some incidents in the media

### Family details lost

Two computer discs holding personal details of all UK families with a child under 16 missing (25M people)  
*United Kingdom, November 2007*  
[http://news.bbc.co.uk/2/hi/uk\\_news/politics/7103566.stm](http://news.bbc.co.uk/2/hi/uk_news/politics/7103566.stm)

### Personal employee information on the street

Car manufacturer in Belgium loses CD with detail about 2.000 employees in public transport  
*Belgium, December 2007*  
[http://www.security.nl/article/17632/1/Toyota\\_Belgie\\_verliest\\_vertrouwelijke\\_CD\\_in\\_openbaar\\_vervoer.html](http://www.security.nl/article/17632/1/Toyota_Belgie_verliest_vertrouwelijke_CD_in_openbaar_vervoer.html)

### Confidential customer data disclosed

Insurance company leaks confidential information on 55.000 customers  
*The Netherlands, December 2007*  
[http://www.security.nl/article/17633/1/Zorgverzekeraar\\_CZ\\_lekt\\_gegevens\\_55.000\\_klanten.html](http://www.security.nl/article/17633/1/Zorgverzekeraar_CZ_lekt_gegevens_55.000_klanten.html)

2007/09 - A dutch military intelligence officer loses USB stick with secret information  
 2008/03 - UK DoD lost 11.000 military ID cards  
 2008/04 - Bank loses customers' data disc with details of 370.000 customers  
 .....

## Data leakage

- Sensitive information seems to leak away all the time and everywhere
- Incidents where confidential information falls in the wrong hands are often not reported:
  - Is the incident detected?
  - Do the responsible staff members escalate?
  - Does the organisation go public?
- Examples of sensitive information:
  - Personally identifiable data (PII)
  - Medical records
  - Patent or trade secrets
  - Corporate information
  - Customer information
  - Military secrets
  - Electronic Evidence

## Data: an asset and a liability

Data is both an asset and a liability. As organizations grow, the volume and complexity of data increase to support the business. Certain types of data within the enterprise data must be protected against theft, loss, and misuse.

Without an effective method to:

- **Discover** data, it is difficult to apply the appropriate security controls to it;
- **Classify** data, it is difficult to understand the importance and sensitivity of the data;
- **Control** data, it is difficult to restrict access to data, prevent misuse of it, and secure it at rest and in transit;
- **Audit** data and its usage, it is difficult to enforce the security controls.

As a result, it is difficult to adequately **protect** data throughout its lifecycle across the enterprise

*Some day, on the corporate balance sheet, there will be an entry which reads, "Information"; for in most cases, the information is more valuable than the hardware which processes it.*  
- Grace Murray Hopper, USN (Ret)

## Incident Analysis

### How does information leak away?

- Storage media theft or loss
- Unauthorised copying or unintended use
- Inadequate information (medium) disposal
- Uncareful use or communication
- System break-in and theft

### Some trends

1. The amount of stored information increases rapidly
2. The information value changes
3. More interconnectivity and data redundancy
4. Availability of new end-user technologies

Deloitte.

7

©2008 Deloitte. All rights reserved

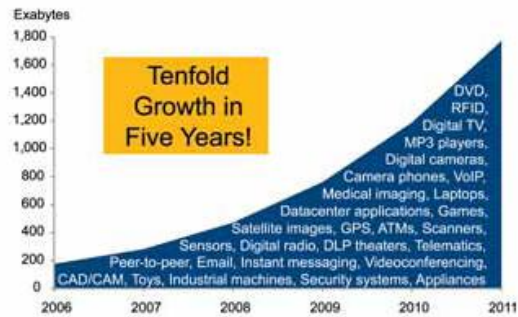
## 1. Data growth

Approximately 70% of the digital universe is created by individuals, but enterprises are responsible for the **security, privacy, reliability, and compliance** of 85%\*

The IDC research shows that the digital universe — information that is either created, captured, or replicated in digital form — was 281 exabytes in 2007.

In 2011, the amount of digital information produced in the year should equal nearly 1,800 exabytes, or 10 times that produced in 2006

IDC forecasts tenfold data growth over five year planning horizon



Source: IDC 2008

\* IDC Forecast of Worldwide Information Growth Through 2011

Deloitte.

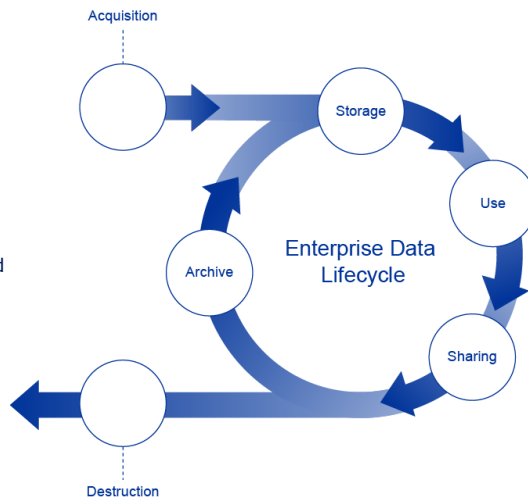
©2008 Deloitte. All rights reserved

## 2. Changing value throughout data lifecycle

The intrinsic and contextual value of data and associated ownership risk vary throughout the data lifecycle

The business value of information assets – gains on process and function performance, revenue and margin contribution – is function of:

- Inherent Value
- Contextual Value
- Enterprise Context
- Associated Risk
- Cost of ownership



Deloitte.

- 9 -

©2008 Deloitte. All rights reserved

## 3. More interconnectivity & data redundancy

- The internet is the highway for business communication
- Critical information is stored on various locations
- More connectivity between suppliers, companies, customers and employees
- Backups are made and kept on multiple levels and places
- Traditionally companies control data access upfront, not lifecycle-based

Internet-enablement and multi-site storage makes data storage more vulnerable to emerging internet threats:

- *More hacking for profit (information theft, extortion, organised crime)*
- *Vulnerability defense*
- *An ever-growing internet community*

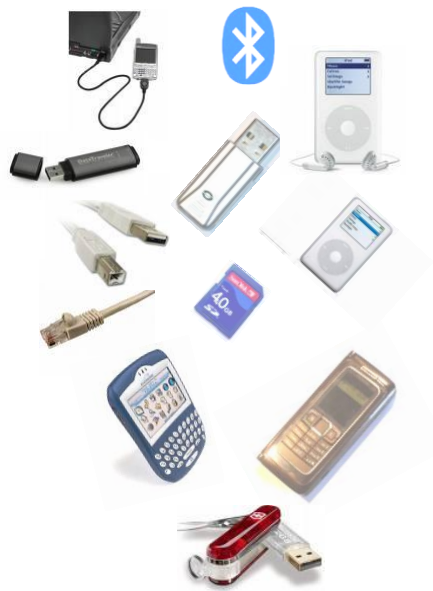
Deloitte.

10

©2008 Deloitte. All rights reserved

## 4. New end-user technologies

- Fast innovation of storage & communication technologies
- Fast end-user adoption
- More employee-enablement
- Loss of private-work boundary for IT equipment, information and location
- "Dual-Use" devices present and used in most companies



Deloitte.

11

©2008 Deloitte. All rights reserved

## Information leakage considerations

- **Focus Area** *Information may leak organisation-wide and at various levels, therefore difficult to set a focus*
- **No real "loss"** *The information is often still available after leakage*
- **Detection** *Usually storage media loss is detected, not information loss*
- **No way back** *Once information has leaked, there is no "undo" action*
- **Value vs. Cost** *Difficult to estimate the value of information and the cost of disclosure*
- **Communication** *Nobody wants to bring the bad news (or bear the consequences)*
- **Privacy vs. Control** *How to balance between control and personal privacy*

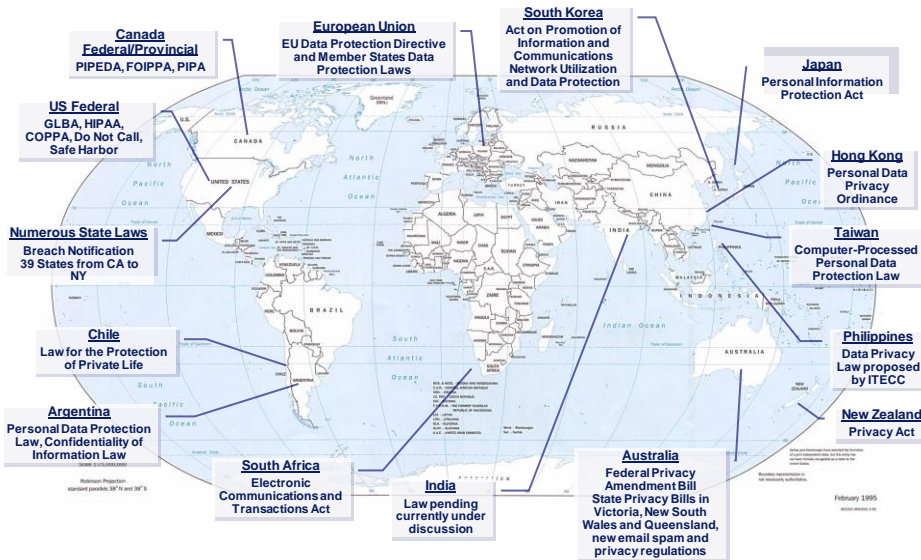


12 Deloitte.

12

©2008 Deloitte. All rights reserved

## Proliferation of Privacy and Data Protection Laws, Regulations & Standards



13

©2008 Deloitte. All rights reserved

## Business challenges

The Current Landscape		Impact on Business
<b>Geo-Political</b>	<ul style="list-style-type: none"> <li>Recent and predicted global events (e.g. terrorism, pandemics, etc.) are resulting in increased interdependent risks</li> <li>A continued focus on protecting the critical infrastructure will remain prevalent, requiring the public and private sectors working together</li> </ul>	<ul style="list-style-type: none"> <li>Reputational and brand damage</li> <li>Remediation cost                             <ul style="list-style-type: none"> <li>Reduced customer, partners confidence</li> <li>Fines and penalties</li> </ul> </li> <li>Low employee morale</li> <li>Productivity loss</li> <li>Unavailability of business-critical systems</li> </ul>
<b>Economic</b>	<ul style="list-style-type: none"> <li>The internet is being utilised as a cost-effective channel</li> <li>Reduced confidence in low-cost channels has a direct impact on operational efficiencies</li> <li>Reacting to a breach proves more expensive than proactive measures</li> </ul>	
<b>Legal and Compliance</b>	<ul style="list-style-type: none"> <li>Regulations and reporting requirements place new demands on FIs</li> <li>Legislation and regulation are not necessarily leading to sustainable and effective solutions</li> <li>More security and privacy regulations are expected</li> </ul>	
<b>Socio-Cultural</b>	<ul style="list-style-type: none"> <li>The 'techno-generation' possesses different behaviors and ethics</li> <li>Desire for work / life balance drives remote access and mobile device usage, exposing organisations to new threats</li> <li>Lack of security awareness within the educational system</li> <li>Cultural differences in appreciating threat and risk</li> </ul>	
<b>Technical</b>	<ul style="list-style-type: none"> <li>Device convergence obscures the distinction between corporate and personally-owned technology</li> <li>Personal storage devices ease the theft/leakage of sensitive data</li> <li>Software engineering not as rigorous as civil engineering</li> </ul>	

Deloitte.

Sources: Information Security Forum, Deloitte Research

©2008 Deloitte. All rights reserved

## Data leakage prevention (DLP) business drivers



Deloitte.

15

©2008 Deloitte. All rights reserved

## We know the problem, how to deal with it?

1. Establish a **centralised governance** model on data protection
2. Update existing information security **policies**
3. Create employee **awareness**
4. Ensure compliance of business **processes and standards** with policies
5. **Implement controls** to ensure compliance and detect deviations and violations

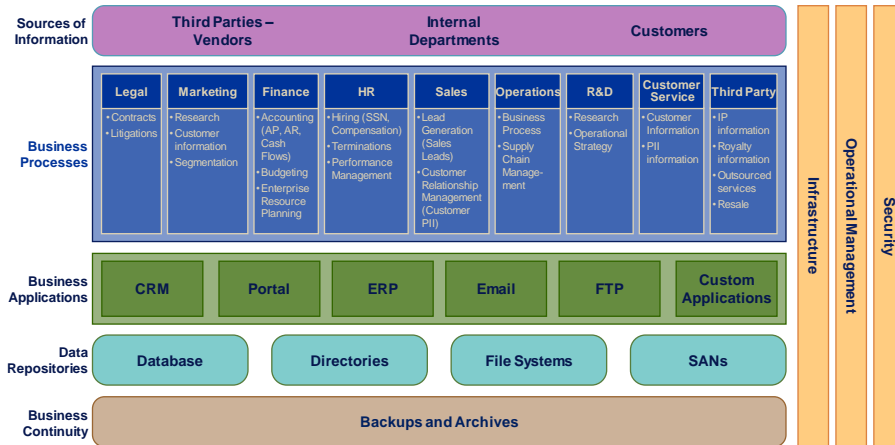


Deloitte.

16

©2008 Deloitte. All rights reserved

## Data protection conceptual architecture

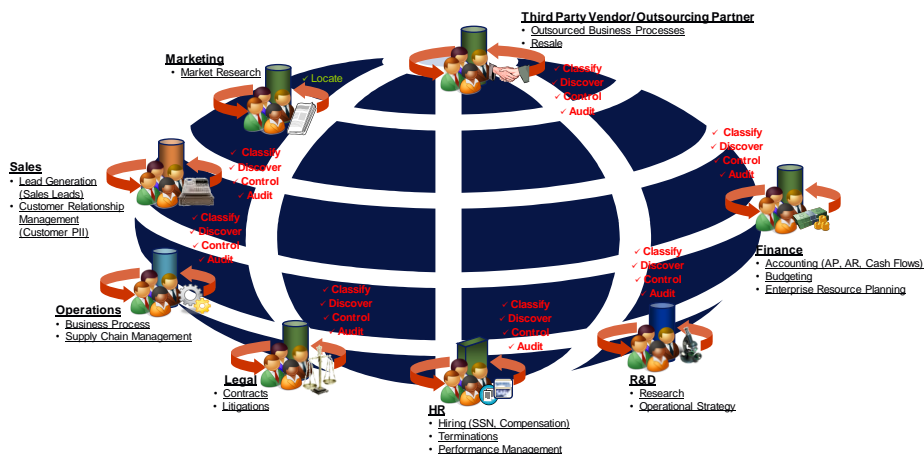


Deloitte.

©2008 Deloitte. All rights reserved

### 1. A central governance model

- ✓ is used to define the overall data protection strategy and provide oversight to ensure the strategy is effectively and efficiently implemented throughout the organization
- ✓ provides oversight of data protection policies, procedures, and technologies throughout the organization. Controls may still be enforced by the individual data owner or department, but they are defined centrally.

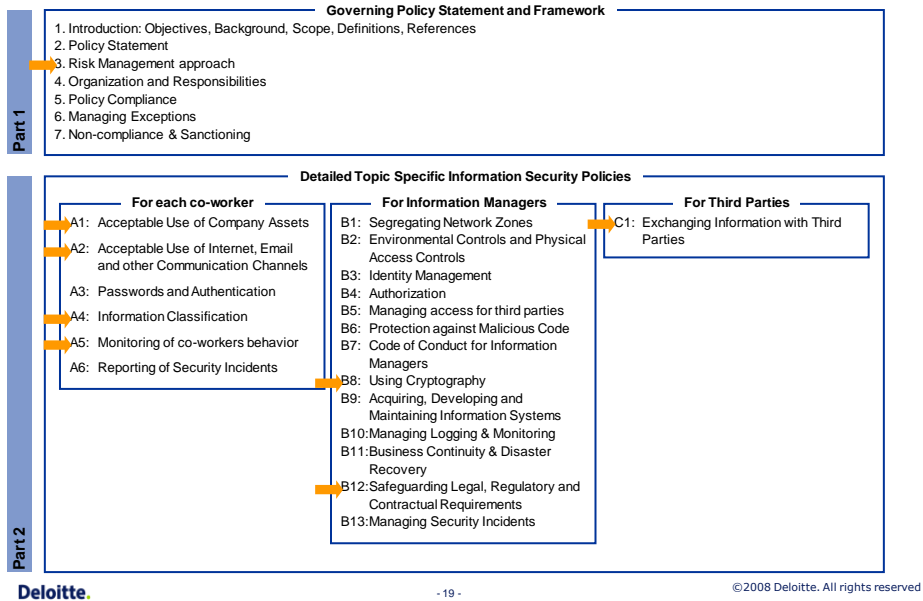


Deloitte.

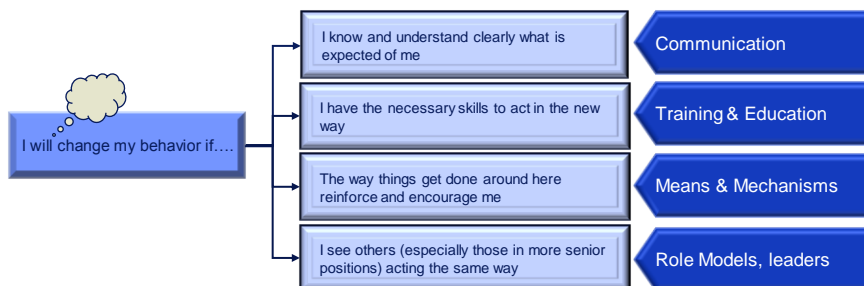
- 18 -

©2008 Deloitte. All rights reserved

## 2. Updating the existing information security policies



## 3. User awareness

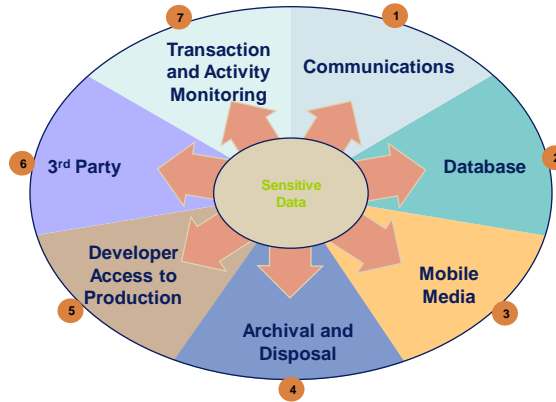


### Lessons learned

- Identify and describe the necessary behavioural change
- Involve internal communications in awareness programs
- Manage problem at all levels
- Communicate incidents
- Measure and publish results

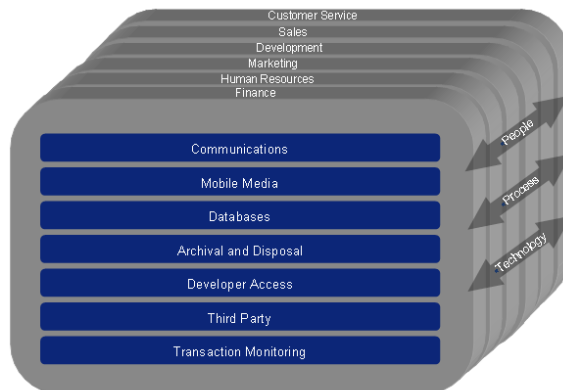
#### 4. Processes & standards: our 7 environments

Identify per business process the data flows through the relevant environments



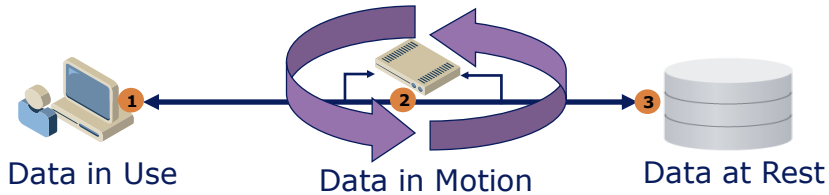
Design and implement environment-specific controls in order to reduce the **risk** of data transfer to an **unintended** state

#### 4. Processes & standards with relevant environments



- **Review** processes for data use, sensitivity and risk of leakage
- **Consider** the seven technical environments when defining risk
- **Define** control objectives and design adequate controls
- **Implement** mitigating controls where appropriate
- **Monitor and periodically audit** the effectiveness of the implemented controls

## 5. Implement data protection controls



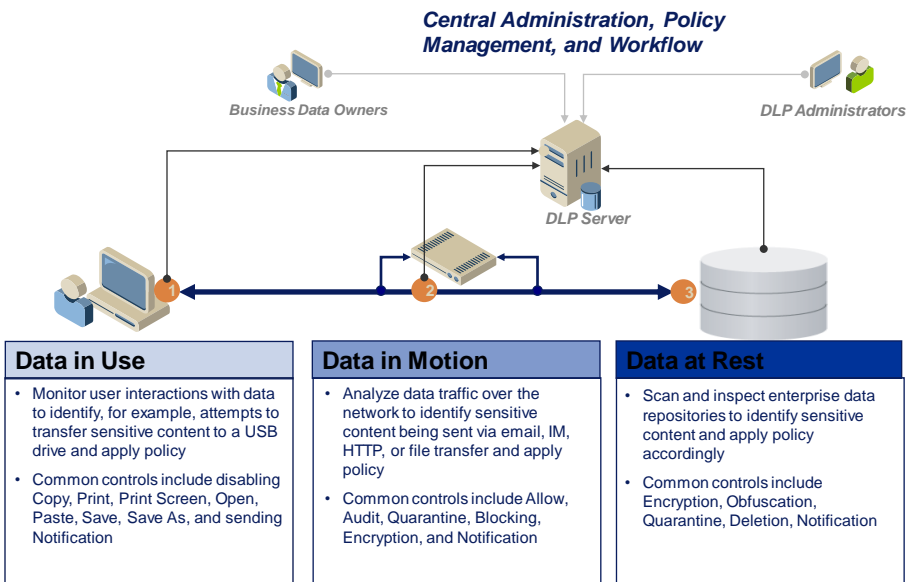
Data in Use	Data in Motion	Data at Rest
<ul style="list-style-type: none"> <li>Monitor user interactions with data to identify, for example, attempts to transfer sensitive content to a USB drive and apply policy</li> <li>Common controls include disabling Copy, Print, Print Screen, Open, Paste, Save, Save As, and sending Notification</li> </ul>	<ul style="list-style-type: none"> <li>Analyze data traffic over the network to identify sensitive content being sent via email, IM, HTTP, or file transfer and apply policy</li> <li>Common controls include Allow, Audit, Quarantine, Blocking, Encryption, and Notification</li> </ul>	<ul style="list-style-type: none"> <li>Scan and inspect enterprise data repositories to identify sensitive content and apply policy accordingly</li> <li>Common controls include Encryption, Obfuscation, Quarantine, Deletion, Notification</li> </ul>

Deloitte.

23

©2008 Deloitte. All rights reserved

## Embedding DLP technology: a conceptual model



Deloitte.

- 24 -

©2008 Deloitte. All rights reserved

# QUESTIONS & ANSWERS

25

25

©2008 Deloitte. All rights reserved

Thank You

**Deloitte.**

**Wouter Janssen**  
CISA CISSP CISM CFE

Senior Manager  
Deloitte Enterprise Risk Services

Berkenlaan 8b  
1831 Diegem  
Belgium

Phone: +32 2 800 25 16  
E-mail: [woujanssen@deloitte.com](mailto:woujanssen@deloitte.com)



**Deloitte.**

26

©2008 Deloitte. All rights reserved

