Presentation Outline

Overview of Data Integrity and Information Protection

KPMG Data Loss Barometer 2012

Information Protection Challenges

Some causes of Poor Data Integrity

Some common Information Protection Principles

Management of Data Integrity and Information Protection
Overview Of Data Integrity and Information Protection
Overview Of Data Integrity and Information Protection

Current Issues around the world

Michelle Obama's ID details hacked from data brokers

Hackers stole millions of social security numbers by cracking open the networks of large US data brokers, reveals an investigation.

The ID details of US First Lady Michelle Obama and many other famous people were exposed by the hack attack.

Journalist Brian Krebs tracked the information back to hackers who ran an online market for confidential data.

He found they got their data by compromising computers sitting on the data brokers' corporate networks.

The social security numbers of Michelle Obama and many others were stolen from data brokers.
Information protection (IP) focuses on the protection of information from inappropriate access or use, using a variety of means as required, including, but not limited to, policy and standards; physical and electronic security measures; and compliance monitoring and reporting. IP represents the point at which the management of information converges with security policy and measures.

Information Protection is safeguarding all information regardless of its form.
Definition of Data Integrity

Data integrity refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle, and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data.

Data integrity can mean ensuring data is "whole" or complete, the condition in which data is identically maintained during any operation (such as transfer, storage or retrieval), the preservation of data for their intended use.

Put simply, data integrity is the assurance that data is consistent and correct.
Surveys regularly conducted by KPMG globally, addressing Data Loss published incidents, reveals the following findings in the January 2012 report:

- **External data losses** rose 40% vs. 2011, affecting 160 million people.
- **Hacking remains the most significant threat**, causing 67% of total data loss incidents.
- **Personally identifiable information remains the #1 data loss type**.
- **Government, Education, & Technology** were the worst affected sectors for data loss.
- **Over 96% of data loss incidents in media** were attributed to hacking in the first half of 2012.

“As organizations are involved in redundancies and downward pressure on costs forces drastic changes, there is a significant risk that disgruntled employees can cause serious damage to an organization through data breaches.”

*Edge Zarrella*

*Head of IT Advisory, KPMG Global*
Data Integrity and Information Protection

Challenges

Company A

- Hackers
- Competitors
- Partners
- Employees
- Financial Markets
- Service Providers
- Customers
- Contractors
- Investors
- General Public/Media
Data Integrity and Information Protection

Protecting information in a constantly challenging environment

Virtual

Physical

Information

External work environments

Outsourced Activities

Professional Networks

E-Mail Communication

Media

WWW

Mobile Devices

Removable Devices

Compliance/Legislation

Disposal/Archival Of physical media

Blogs

Leavers

P2P applications

Websites (corporate, Industry & Private)

Wireless Networks

Geographical/Political changes

Social Networks

End Point Security

Physical Security

IT infrastructure & maintenance

Privacy

Corporate communication
Some causes of Poor Data Integrity

- Entry Errors
- Incomplete Data
- Collection Errors
- System Design
- Others
Some common Information Protection Principles

Collection

1. Lawful
   - When an entity collects your personal information, the information must be collected for a lawful purpose. It must also be directly related to the entity’s activities and necessary for that purpose.

2. Direct
   - Your information must be collected directly from you, unless you have given your consent otherwise. Parents and guardians can give consent for minors.

3. Open
   - You must be informed about the purpose of the information being collected, how it will be stored and used. The entity should also disclose information on subsequent access and updates.
Some common Information Protection Principles

Collection

4. Relevant

• The entity must ensure that the information is relevant, accurate, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

5. Storage

• Secure - your information must be stored securely, not kept any longer than necessary, and disposed of appropriately. It should be protected from unauthorised access, use or disclosure.
Some common Information Protection Principles

Access

6. Transparent

• The entity must provide you with enough details about what personal information they are storing, why they are storing it and what rights you have to access it.

7. Accessible

• The entity must allow you to access your personal information without unreasonable delay and expense.

8. Correct

• The entity must allow you to update, correct or amend your personal information where necessary.
Some common Information Protection Principles

Usage

9. Accurate

- The entity must make sure that your information is accurate before using it.

10. Limited

- Entities can only use your information for the purpose for which it was collected, for a directly related purpose, or for a purpose to which you have given your consent. It can also be used without your consent in order to deal with a serious and imminent threat to any person's health or safety.

Disclosure

11. Restricted

- The entity can only disclose your information with your consent or if you were told at the time they collected it from you that they would do so. Otherwise the entity can disclose your information if it is for a related purpose and they don't think that you would object. Your information can also be used without your consent in order to deal with a serious and imminent threat to any person's health or safety.
Some common Information Protection Principles

12. Safeguarded

- The entity cannot disclose your sensitive personal information without your consent, for example information about your ethnic or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership. Otherwise it can only disclose sensitive information without your consent in order to deal with a serious and imminent threat to any person's health or safety. However there are other limited circumstances in which this information may be disclosed.
Management of Data Integrity and Information Protection
Management of Data Integrity and Information Protection

An overview of Data Leakage Prevention Program
### Data Protection

**What should an organization have in place?**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Mapping:</td>
<td>• Know what and Where you assets are.</td>
</tr>
<tr>
<td>Information Classification:</td>
<td>• Identify the value of your information assets, prioritize your effort.</td>
</tr>
<tr>
<td>Risk –Information Matrix:</td>
<td>• Identify risks and impact of information</td>
</tr>
<tr>
<td>Policies and procedures:</td>
<td>• Create clear guidelines for employees and for monitoring.</td>
</tr>
<tr>
<td>Access management:</td>
<td>• Correlate access rights to the risk-information matrix.</td>
</tr>
<tr>
<td>IT related (Preventive) measures:</td>
<td>• Implement technical tools and controls</td>
</tr>
<tr>
<td></td>
<td>• Be cost effective- prioritize your investments, use plateaus.</td>
</tr>
<tr>
<td></td>
<td>• Correlate measures implementation with classification level and identified</td>
</tr>
<tr>
<td></td>
<td>risks.</td>
</tr>
<tr>
<td>Physical Measures:</td>
<td>• Address loss of assets (physical), relevant aspects of perimeter security</td>
</tr>
<tr>
<td>Awareness Plan:</td>
<td>• Make your employees aware of risks and possible implications</td>
</tr>
<tr>
<td>Monitoring and Reporting:</td>
<td>• Remain in control over breaches in policies and changes in risks and needs</td>
</tr>
</tbody>
</table>

© 2014 KPMG, a partnership established under Ghanaian law and a member firm of the KPMG network of independent member firms affiliated with KPMG International cooperative (“KPMG International”) a Swiss entity. All rights reserved. Printed in Ghana. KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss entity.
“The world is a dangerous place to live; Not because of people who are evil, but because of the people who don’t do anything about it”

- Albert Einstein
QUESTIONS
Thank you