



Data Protection

Understanding the Effectiveness of a Data Protection Program

IIA: Almost Free Seminar

21 June 2011



Agenda



- ▶ Data protection overview
- ▶ Case studies
- ▶ Ernst & Young's point of view
- ▶ Understanding the effectiveness of a program

Why is a Data Protection a Concern?

Data loss in the news



- ▶ Large retail company — 45.6 million credit and debit card numbers were stolen over a period of more than 18 months
- ▶ Large BCBS insurer — 57 hard drives containing member-protected health information were stolen
- ▶ Department of Commerce — an employee inadvertently transmitted over the Internet an unencrypted file containing the personally identifiable information (PII) of Commerce employees to other department employees
- ▶ A medical center in Kentucky is notifying 5,418 patients of a breach resulting from the theft of an unencrypted portable hard drive stored in a locked area
- ▶ FTC Consent Decree requires monitoring and filtering of outbound computer traffic to block export of sensitive information

- ▶ More than 250 privacy laws that mandate disclosure of data breaches
- ▶ 2% of laptop inventory cannot be located
- ▶ Fortune 500 companies lose two laptops a day

Sources: Ponemon Institute, engadget, Computerworld and CNET news.

High Value Data

It's all about the data

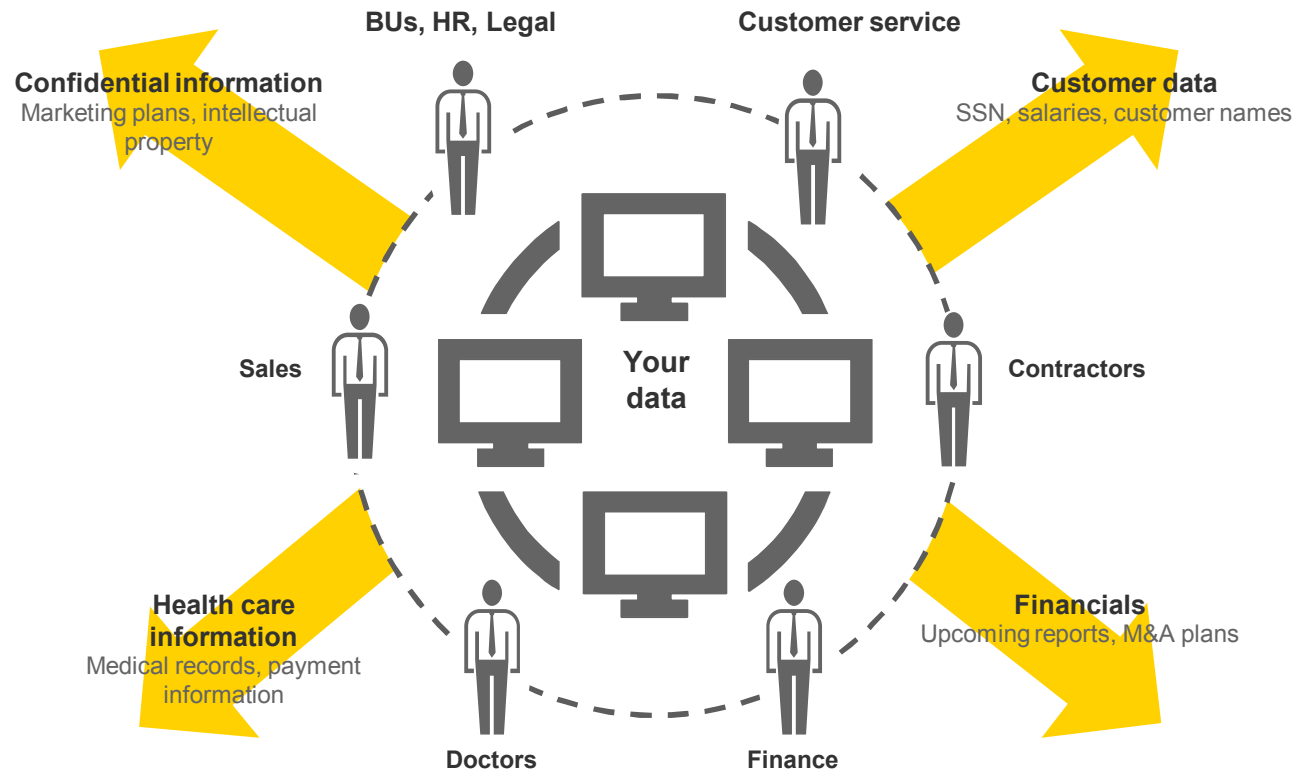
Compliance	Intellectual Property	High Business Impact (HBI) Information
<ul style="list-style-type: none">▶ SOX▶ HIPAA▶ PCI▶ Credit Card numbers▶ GLBA▶ FISMA▶ ITAR▶ SB 1386▶ Others	<ul style="list-style-type: none">▶ Customer Lists▶ Price/Cost Lists▶ Target Customer Lists▶ New Designs▶ Company Logo▶ Source Code▶ Formulas▶ Process Advantages▶ Pending Patents	<ul style="list-style-type: none">▶ Board Minutes▶ Financial Reports▶ Merger/Acquisitions▶ Product Plans▶ Hiring/Firing/RIF Plans▶ Salary Information▶ Acceptable Use

What you did not know needed protection

- ▶ Review of Key Employee actions before they announced departure
- ▶ Unreported but Important Memos/Reports
- ▶ Code names of projects not reported to Security department

Complexity of Data Protection

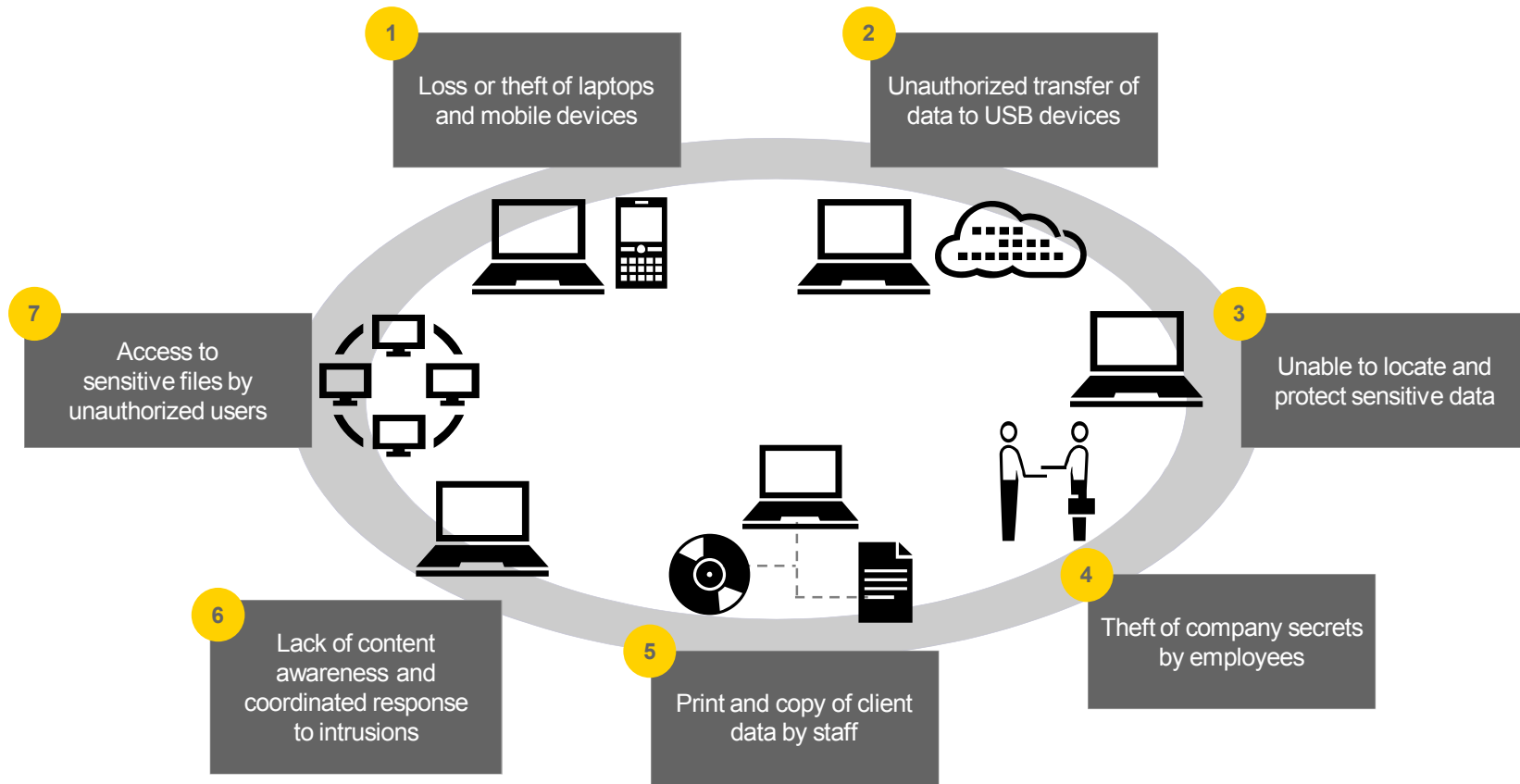
Today's challenges with protecting data



Data breach incidents cost US companies \$204 per compromised record, with an average total per-incident cost of \$6.75m – Ponemon Institute

Data Loss Incidents

How does it happen?



Example 1: Technology Company

Client Concerns

- ▶ Organization is concerned about software code being pirated
- ▶ During recent quarter ending, client was concerned about employees communicating confidential information to analysts prior to analyst call
- ▶ Client wanted to understand their data loss exposure

Things to Consider

- ▶ Do the employees know what they can or can not communicate to outsiders?
- ▶ Does the organization have adequate controls around this sensitive information?
- ▶ Should the people leaking information even have access to this information?
- ▶ Can the company detect or prevent this from happening?
- ▶ How would the company deal with this situation?



Example 2: Oil & Gas Company

Client Concerns

- ▶ Organization suspected hack by the Chinese
- ▶ System administrators accidentally discovered compromised systems when they were logged off
- ▶ Client did not know how long suspected systems were compromised and what had been stolen
- ▶ Organization notified FBI and DHS of data breach

Things to Consider

- ▶ How long has the company been hacked?
- ▶ Has the company lost any valuable information?
- ▶ Does the company have to report this breach to anyone?
- ▶ What is the root cause of the breach, and can it happen again?
- ▶ Was there an insider or was this completely accomplished from the outside?



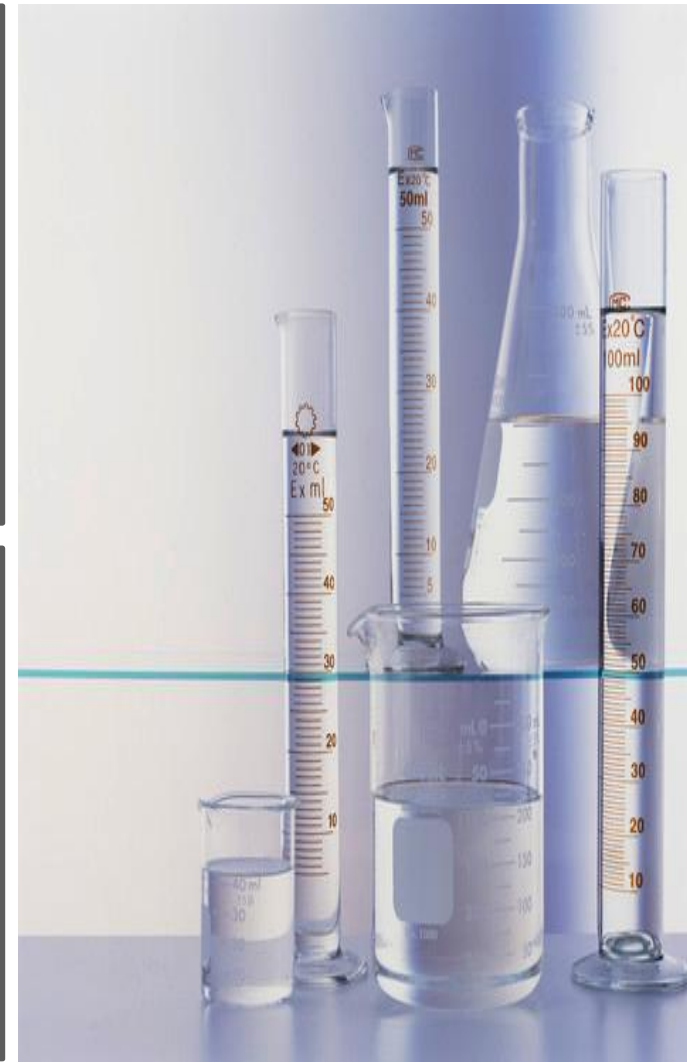
Example 3: Chemical Research Company

Client Concerns

- ▶ Foreign national working as a chemist in the R&D department resigns
- ▶ Before the employee leaves, she downloads a large amount of intellectual property from highly restricted file shares
- ▶ Client discovers this after the employee has left and now has concerns on the extent of the damage and tries to prevent this from happening in the future

Things to Consider

- ▶ How does the company monitor employees with access to sensitive information?
- ▶ Is there still an insider threat?
- ▶ Does the company have any legal protection related to employee theft?
- ▶ Does the company have to report the loss?
- ▶ How can the company prevent this from happening in the future?



Ernst & Young Point of View

13th Annual Global Information Security Survey

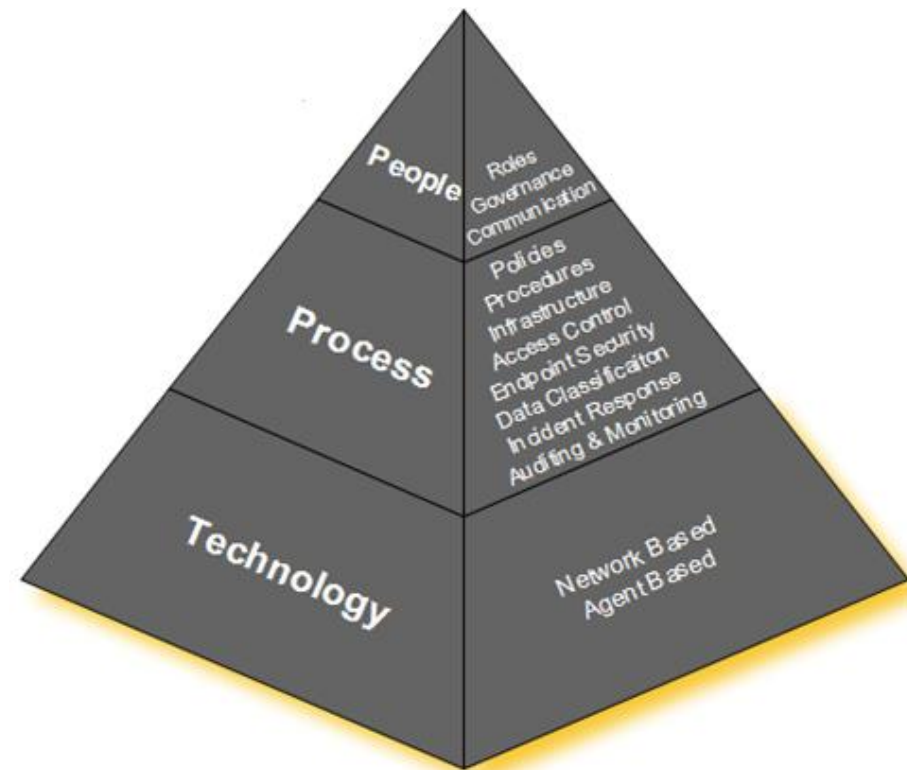


- ▶ More than half say protecting reputation and brand is their biggest information security challenge
- ▶ 64% see the disclosure of sensitive data as one of their top five IT risks
- ▶ 55% indicate they are increasing the level of investment related to their top five areas of information security risk
- ▶ 52% see the use of personal devices as the main cause of an increasing risk of data leakage
- ▶ 50% plan to spend more in the next year on data loss prevention efforts

Program Success Factors

People, process and technology considerations

- ▶ A **top-down approach** must be applied to holistically address the problem of data loss
- ▶ Governance must be established and roles and responsibilities defined to effectively manage and maintain the program
- ▶ Supporting IT processes must be enhanced based upon gaps uncovered by data loss risk assessment
- ▶ Technology solutions must be adopted to cover data at rest, data in motion and data in use, to effectively monitor, prevent and respond to data protection requirements

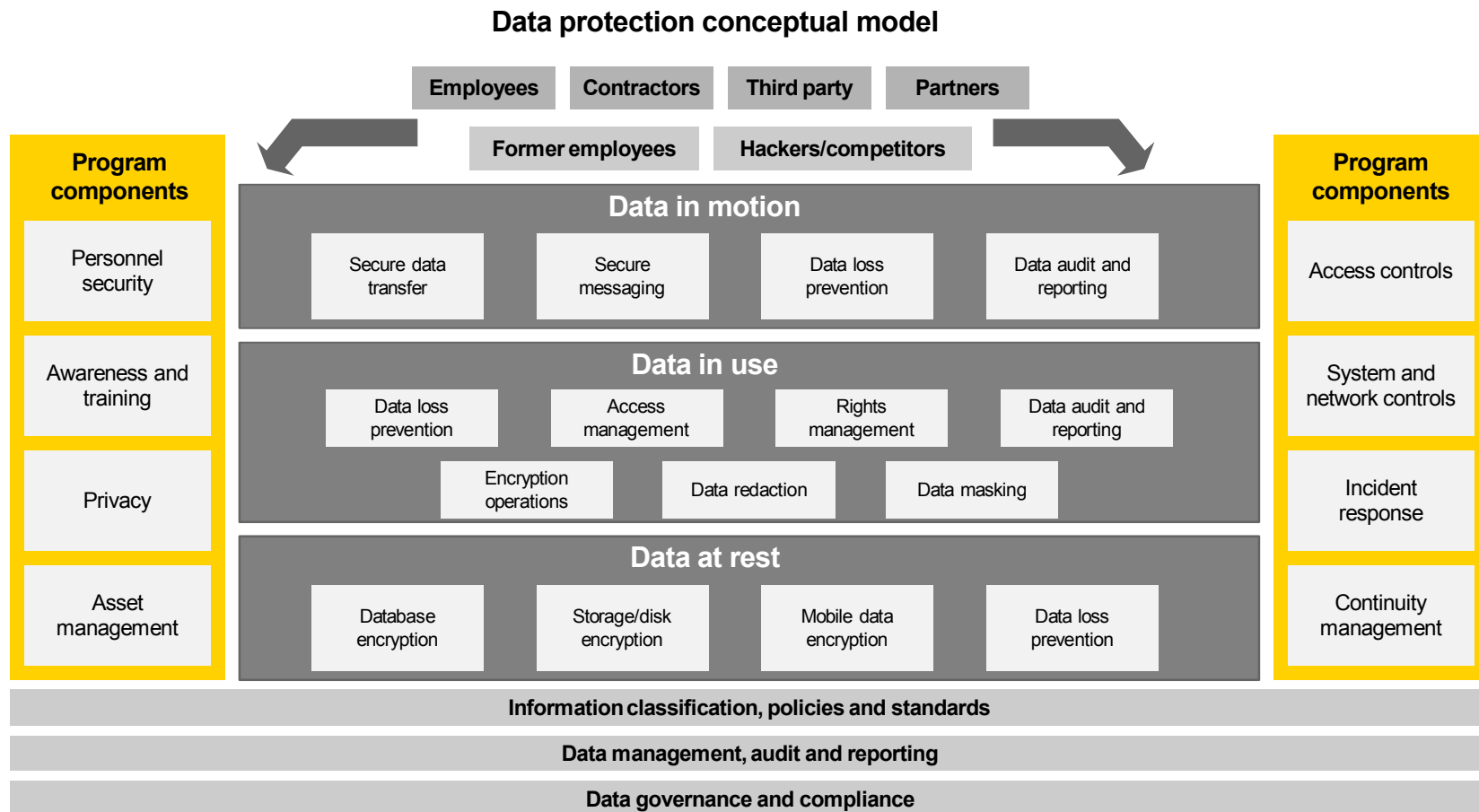


A data protection program must include all domains of people, process and technology

The Data Protection Program

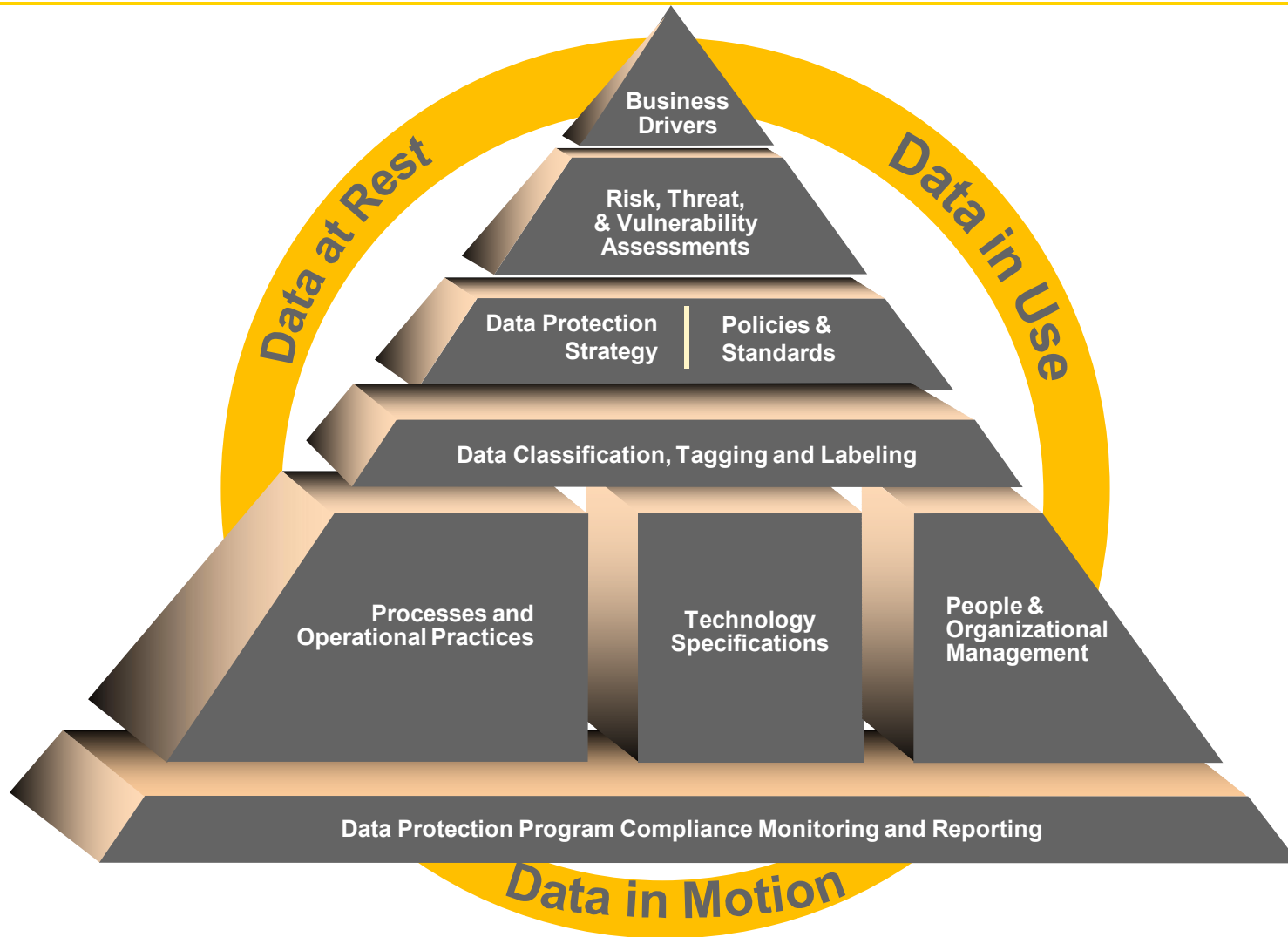
Data protection requires many people, processes, and technologies

“Data protection” is an umbrella term that describes the program, governance, policy instantiation, management controls and solution implementation of people, process and technology measures to prevent the loss of, or unauthorized access to, sensitive data



Understanding the Effectiveness

Assessing the data protection program



Contact information

Anil Markose CISA, CISSP, CIPP

Senior Manager, Ernst & Young LLP

anil.markose@ey.com

Direct: 214 969 9734

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

About Ernst & Young's Assurance Services

Strong independent assurance provides a timely and constructive challenge to management, a robust and clear perspective to audit committees and critical information for investors and other stakeholders. The quality of our audit starts with our 60,000 assurance professionals, who have the experience of auditing many of the world's leading companies. We provide a consistent worldwide audit by assembling the right multidisciplinary team to address the most complex issues, using a proven global methodology and deploying the latest, high-quality auditing tools. And we work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

© 2011 Ernst & Young LLP.
All Rights Reserved.
1010-1200121