

accenture
High performance. Delivered.

Information Security Management
 - Overview -

M. van den Heuvel
 Accenture Technology Consulting
 27 November 2007

Agenda

- What is information security management about?
- Why security / risk management?
- Risk management cycle
- Essential definitions
- Who should worry?
- Do they really have to worry?
- Cost vs. Security
- Key success factors
- Regulations and standards

Copyright © Accenture 2007. All Rights Reserved

What is information security management about?

Risk Management Information Security
 Information Risk Management
 IT security IT Security Management IT risk management

At the end of the day, it's all about securing information.
 What aspects of information are key?
 C (Confidentiality)
 I (Integrity)
 A (Availability)

Copyright © Accenture 2007. All Rights Reserved

What is information security management about? (cont.)

- **IT Security** is the process of implementing **measures and systems** designed to **securely protect and safeguard information** (business and personal data, voice conversations, still images, motion pictures, multimedia presentations, including those not yet conceived) utilizing various forms of technology developed to create, store, use and exchange such information **against any unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure**, thereby preserving the value, confidentiality, integrity, availability, intended use and its ability to perform their permitted critical functions".

By SANS institute

Copyright © Accenture 2007. All Rights Reserved

What is information security management about? (cont.)

- **Information Security** refers to the **processes and methodologies** which are designed and implemented to **protect** print, electronic, or any other form of **confidential, private and sensitive information or data** from **unauthorized access, use, misuse, disclosure, destruction, modification, or disruption**.

By SANS institute

Copyright © Accenture 2007. All Rights Reserved

Why Security / Risk Management?

- Common Gaps in Enterprise Security
 - Security investments not always focused on greatest return
 - Combination of mile and millimeter depth of protection
 - Inability to articulate the case for security to upper management and to obtain requisite budget
 - Security policies in place but little compliance checking
- Risk changes over time
- Risk is different for every business

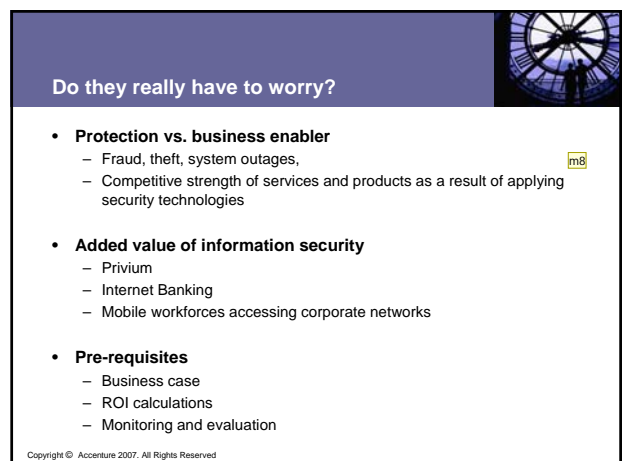
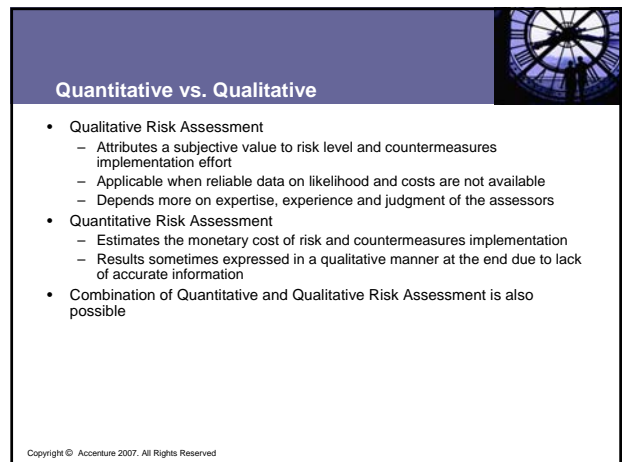
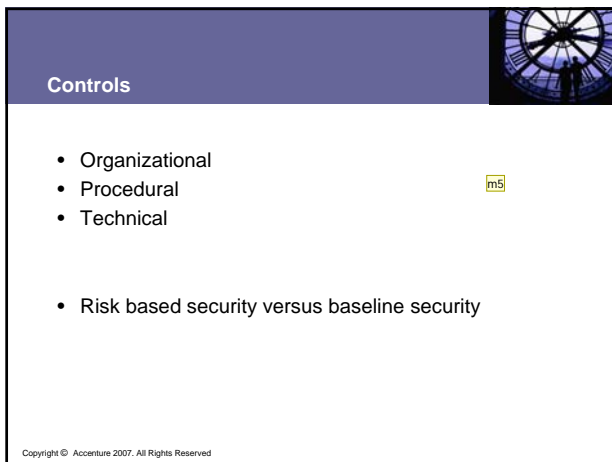
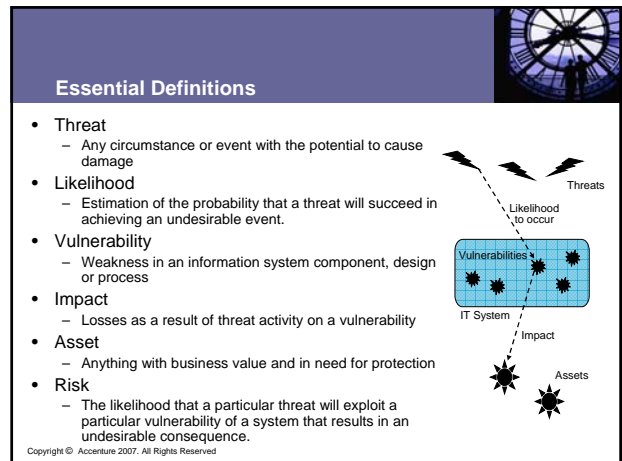
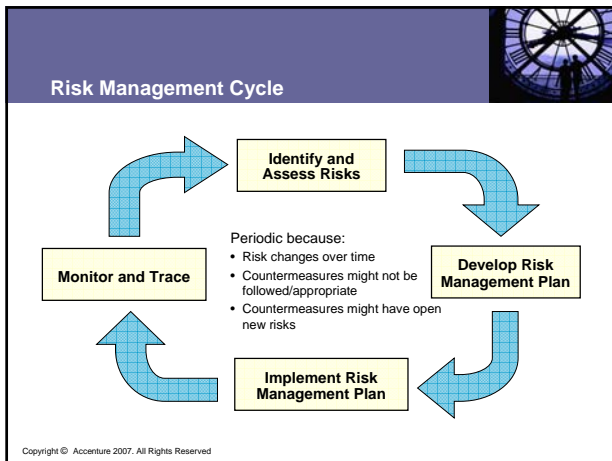
Copyright © Accenture 2007. All Rights Reserved

Dia 4

- m1 Als je bepaalde woorden wilt highlighten kun je er een box om heen tekenen waardoor ze beter uitkomen (of een ander effect verzinnen). Nu is het een beetje een woordenbrij...
floris.van.den.dool; 22-11-2007

Dia 5

- m2 wat is het verschil met de vorige definitie (IT versus Information?). Ik mis de people, process, technology dimensies...
floris.van.den.dool; 22-11-2007



Dia 9

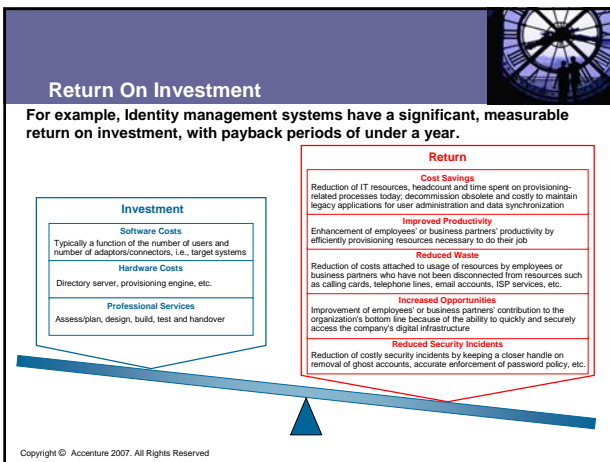
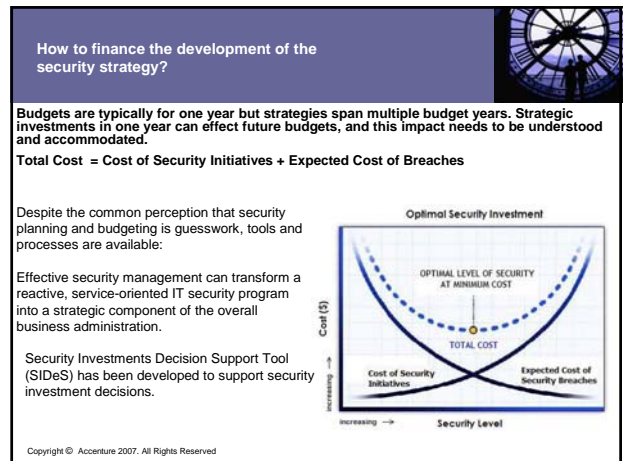
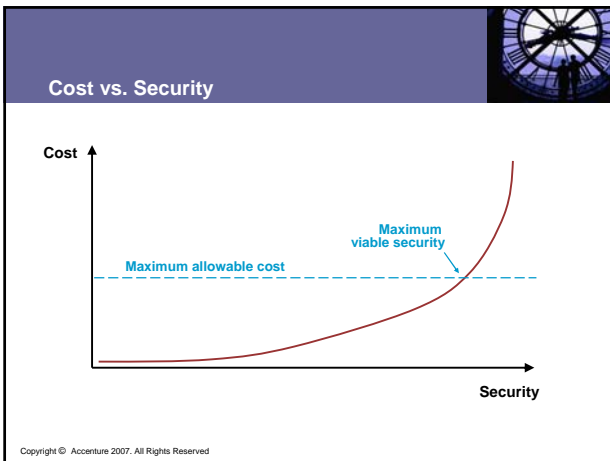
- m5 ik zou hier een plaatje (cartoon of anderszins) bij zoeken. Enerzijds om te illustreren, anderzijds om het wat minder droog te maken. Ik stuur je wel een voorbeeld
floris.van.den.dool; 22-11-2007

Dia 11

- m7 gooi hier een statistiek bij vanuit het Symantec threat rapport. Een grafiek met trends en voorspellingen.
floris.van.den.dool; 22-11-2007

Dia 12

- m8 noem ook I&AM als een manier om je processen te optimaliseren
floris.van.den.dool; 22-11-2007



- ### Key success factors
- Security Awareness
 - Social Engineering
 - Clean desk policy
 - Law and regulations
 - Operations management
 - Patch management, configuration management
 - Perimeter security
 - Splitting up networks into smaller domains with specific risk profiles and specific security controls

- ### Law and external regulations
- SOx (Sarbanes-Oxley)
 - Base I
 - PCI- DSS (Payment Card Industry Data Security Standard)
 - WBP (Wet Bescherming Persoonsgegevens)
 - US GAAP (Generally Accepted Accounting Principles in the United States)
 - US Export regulations for encryption technologies

- ### Industry standards / best practices
- BS7799 / ISO 17001 (British Standard for Information Security)
 - Common Criteria / ISO 15408 (framework in which computer system users can specify their security requirements)
 - ITIL Security Management
 - The COSO Enterprise Risk Management -- Integrated Framework and Application Techniques (the Committee of Sponsoring Organizations)
 - COBIT (The Control Objectives for Information and related Technology)

Dia 16

- m9 hier kun je terug komen op de people, process, technologie dimensies
floris.van.den.dool; 22-11-2007
- m10 dit komt een beetje uit de lucht vallen en is een slide op zich waard...
floris.van.den.dool; 22-11-2007

Dia 17

- m11 waarom komt die slide pas hier? Ik zou die eerder in het verhaal verwachten.
floris.van.den.dool; 22-11-2007

Any questions?

