The Other Side of Information Security

Wilco van Ginkel – Ubizen
wilco.vanginkel@ubizen.com

Purpose of this talk

Provide the audience an overview of

'The Other Side of Information Security'

in a nutshell

Nutshell because of time constraints

Agenda

- Introduction
- Business Assessment
- Risk Management
- PSPG
- Security Awareness
- Compliance
- Examples where Organisational meets Technical

Introduction

- The four fundamental security questions
- The components of a total security solution
- Trend in the market
- The Security Triangle
- The Domains

The Four Security Questions

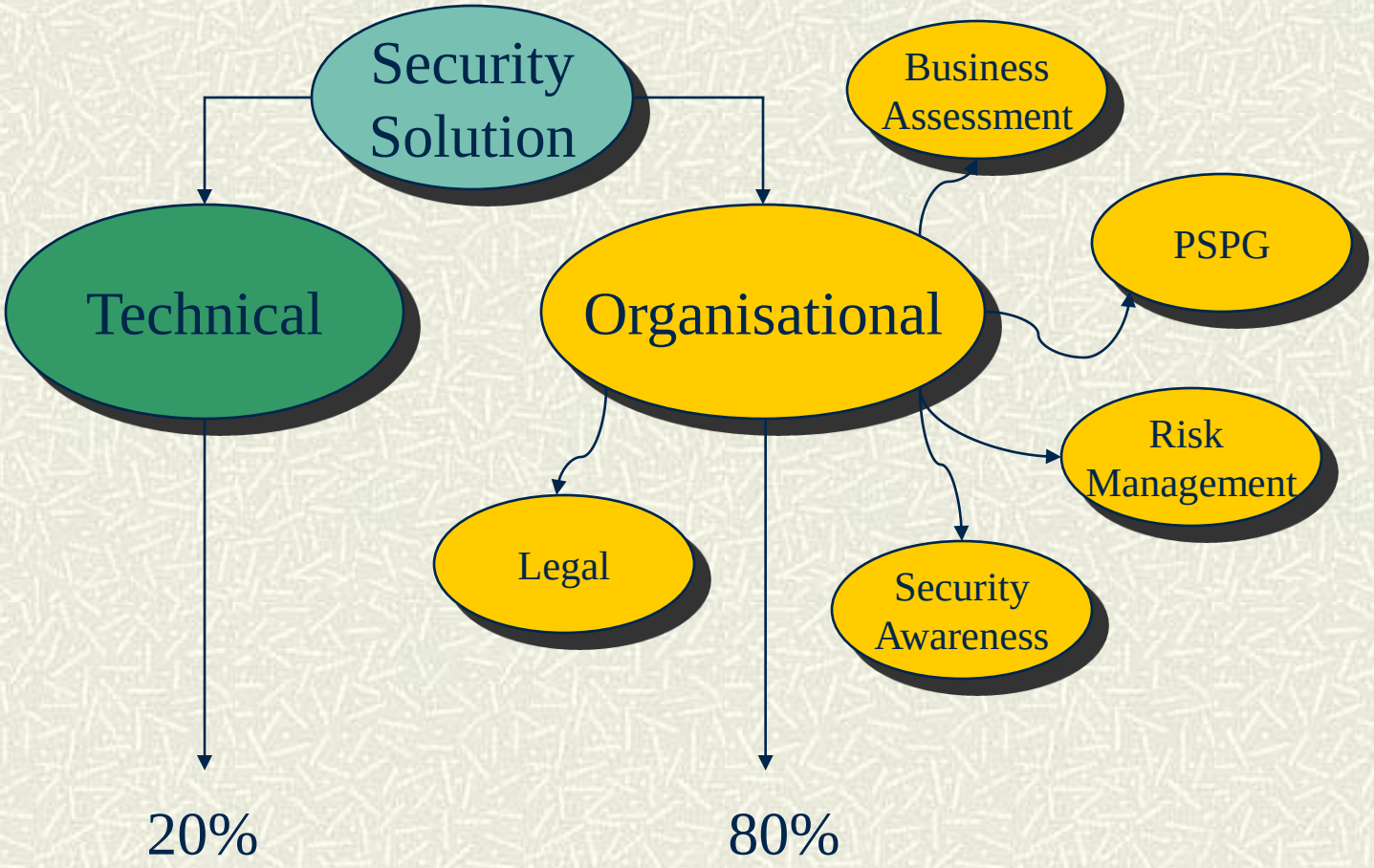
- Most organisations ask the question:

  '*How* should I protect'

More important is to ask <u>first</u>:

1. *Why* should I need protection?
2. How *difficult* will it be to protect?
3. *What* and against *who* should I protect?
4. Then

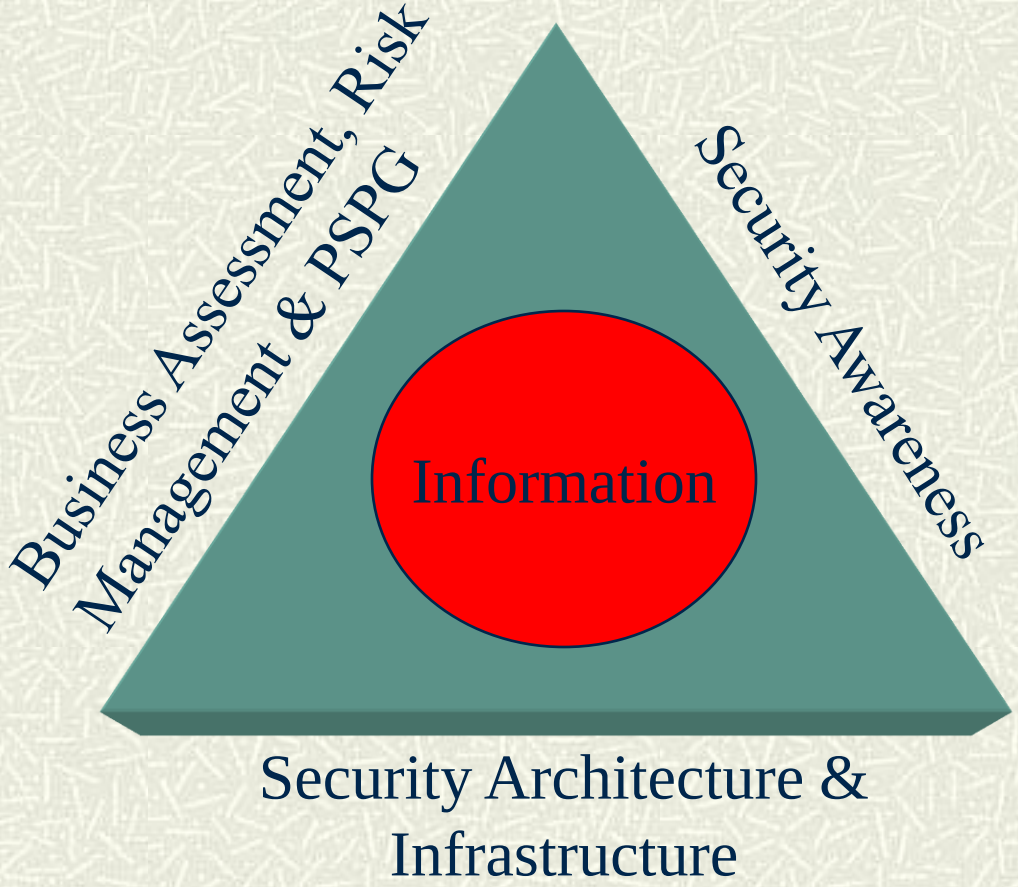
Components


Security Solution
Technical
Organisational
Business Assessment
PSPG
Risk Management
Legal
Security Awareness
20%
80%

Trend

- Security is considered more and more as part of the normal business process
- We are not talking ‘Rocket Science’
- Does this mean that technology is dead or something?
- Most organisations just don’t know how to do it…

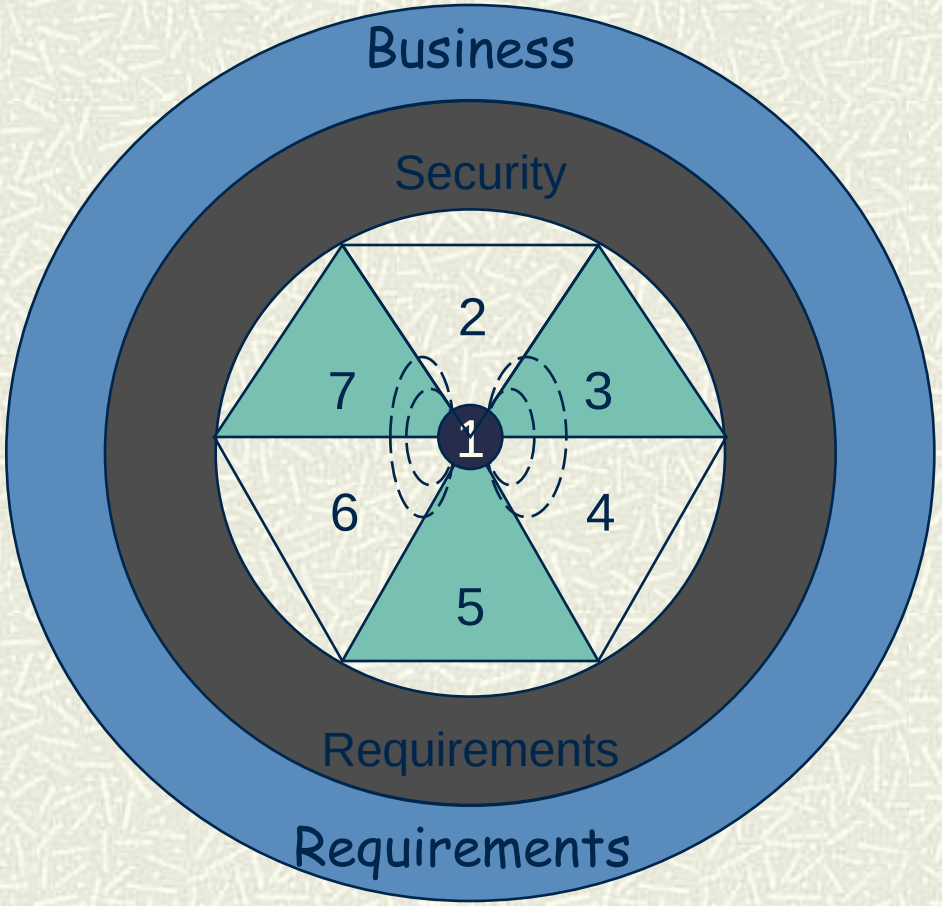
Security Triangle



The Domains

Domains:

1. I.T.
2. Physical
3. Environmental
4. Human
5. Organizational
6. Administrative
7. Legal



The first step

- ‘Meet the parents’
- Because:
  - They are the end responsibles for security
  - They decide about the budget
  - They should support security
  - They have authority
- How:
  - Business Assessment & Risk Management

Business Assessment - 1

- *Why* should I need protection:
  - Discuss the stakes
  - Discuss the different types of information
  - Discuss the Security Requirements (CIAR)
  - Discuss strategic questions, like:
    - Replacement value of IT
    - Targets
    - Is IT just support or strategic for the organisation
    - …

Examples of Stakes

- Company Image
- Loss of customers
- Loss of service
- Legal pursuits
- Financial recovery costs
- …

Examples of Information

- Public
- Confidential
- Privacy
- Company critical
- …

Security Requirements

- CIAR
- Can be more fine-grained:
  - Internal vs external
  - Function vs data
- Example → External Data Confidentiality
- Example → Accountability (Non-repudiation):
  - Broken anonymity
  - Unavailability of proof
  - Unavailability of accountability function

Business Assessment - 2

- How *difficult* will it be to protect?
  - Evaluate the constraints, like
    - Financial
    - Internal knowledge
    - Dependency on partners
    - Calendar
    - …

Risk Management - 1

- Risk Management consists of two parts:
  - Risk Assessment
  - Risk Treatment (mitigation)
- Risk Assessment:
  - Risk Analysis (identification + evaluation)
  - Risk Valuation
- Against *what* and *who* should I protect → *Risk Assessment*
- How to protect → *Risk Treatment*
- Dependency between security requirements & risk management…

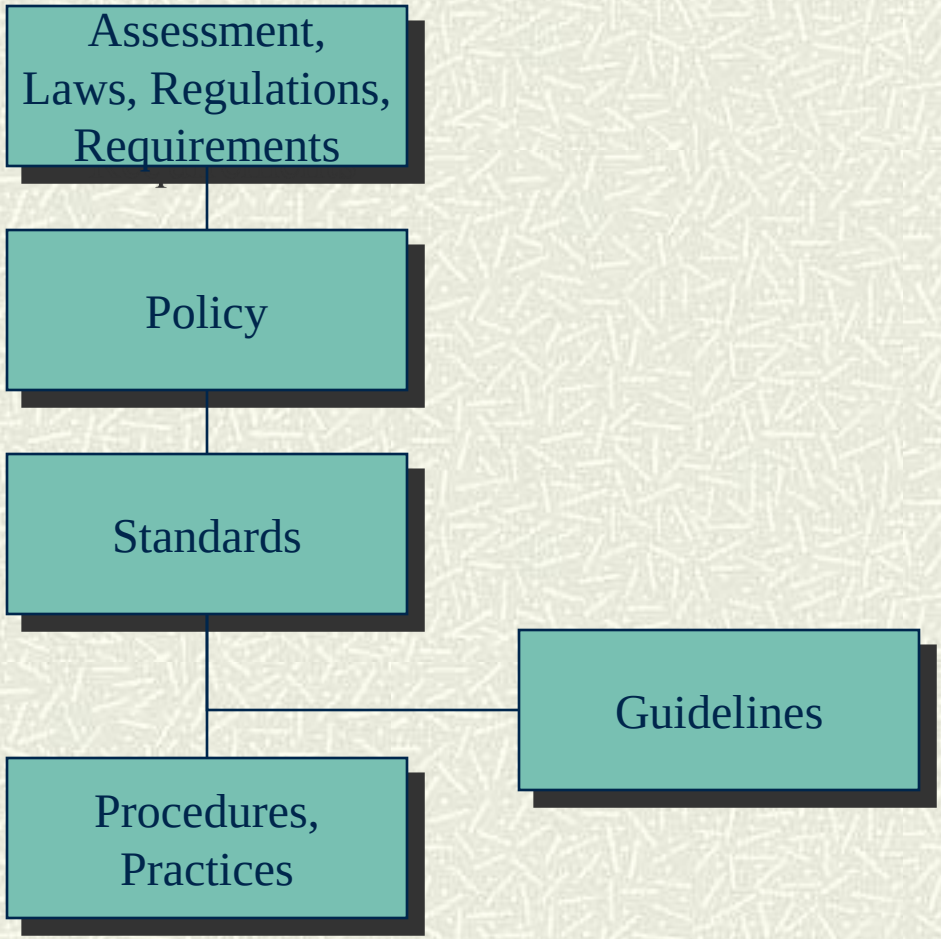
Risk Management - 2

- Some attention points:
  - Different Risk Assessment/Analysis methodologies:
    - Generic
    - Detailed
    - Business oriented
  - Sometimes difficult to determine the ‘value’
  - Make sure that you’ve the right people, meaning:
    - Who know the business processes
    - Who have authority to decide
  - Be careful when using risk management tools…

PSPG - 1

- Policies → high-level statements of a companies belief, goals and objectives
- Standards → mandatory rules & regulations
- Procedures → how to implement the policies, standards and guidelines
- Guidelines → recommendations

PSPG - 2



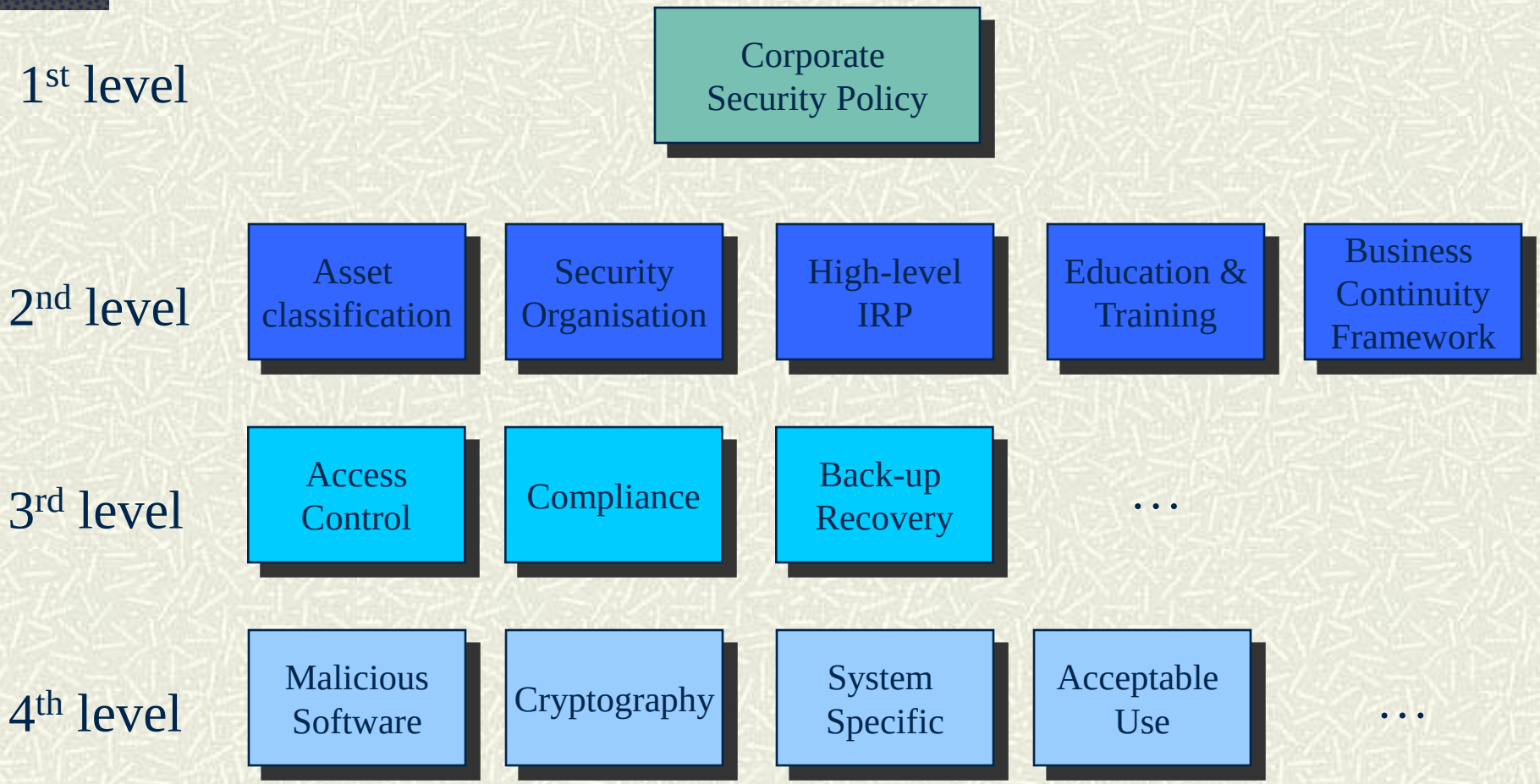
From 'Information Security, Policies, Procedures, and Standards'

PSPG - 3

- Example:
  - *Policy* → Access to company information systems is restricted to authorised users only
  - *Standard* → Users are required to have a unique User-id & confidential password
  - *Procedure* → User-id & password requests must contain a signature of the authorised system owner. Approval of the signature must be verified against the company list of authorised signatures
  - *Guideline* → Passwords should have 5 to 8 alphanumeric characters

From 'Information Security, Policies, Procedures, and Standards'

PSPG Building Blocks



PSPG - 4

- Make sure that:
  - The PSPG documents are supported by the System Owner
  - The PSPG documents are developed by a representative group within the organisation
  - The PSPG documents are clearly communicated
  - The PSPG documents are useful and pragmatic
  - You pay attention to the organisational culture!
  - You pay attention to the international culture!

Security Standards - 1

- Are you on our own?
- No, there are standards out there
- A set of best practices
- Can be a good starting point and prevents to re-invent the wheel
- However, be careful not to implement a security standard blindly…

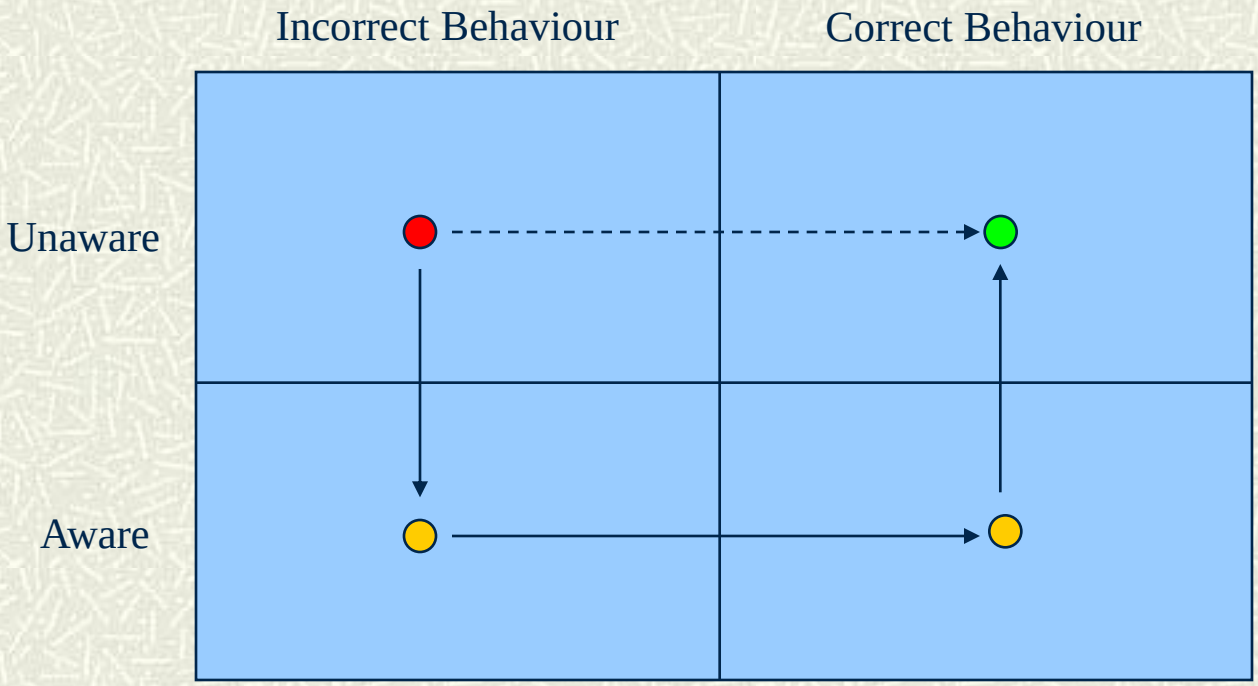
Security Standards - 2

- Some well-known examples are:
  - ISO/17799 (BS/7799 part 1 + 2)
  - Cobit-3
  - ITIL
  - ISO-13335
  - Common Criteria (ISO-15408)
  - NIST
  - IETF
  - …
- Certification…

Security Awareness - 1

- The most critical success factor of Information Security
- Awareness should be at any level in the organisation
- It is all about psychology…

Security Awareness - 2



Compliance

- Do we still comply with our PSPG's?
- Auditing:
  - Quick Scan
  - Review
  - Full Audit
- Monitoring
- Internal vs external
- Technical vs organisational

Organisational meets technical - 1

- Example:
  - CSP → Accountability principle
  - Access Control Policy → strong authentication
  - Standard → Tokens

Organisational meets technical - 2

- Example:
  - CSP → Information across untrusted networks should be protected
  - Cryptography Policy → Symmetric Encryption at least 128 bits, preferred choice 3-DES
  - Guideline → Hardware Encryptors

Organisational meets technical - 3

- Example:
  - Within the business process ‘Electronic Transactions’, there is a high security requirement for *Integrity* and *Non-repudiation*
  - Defined risks are:
    - Unauthorised change of the transaction
    - Denial of sending the transaction
  - Standard → Digital signatures
  - Cryptography Policy → Use RSA, minimum key length of at least 1024 bits

Useful links

- www.isaca.org
- www.bsi-global.com
- www.nist.gov
- www.ietf.org
- www.iso.org
- www.cenorm.be/isss
- www.sse-cmm.org

Useful books

- ‘Writing Information Security Policies’, Scott Barman
- ‘Building an Information Security Awareness Program’, Mark B. Desman
- ‘Information Security Risk Analysis’, Thomas Peltier
- ‘Information Security Policies, Procedures, and Standards’, Thomas Peltier
- ‘Information Security Policies made easy, version 8’, Crisson Wood
- ‘Incident Response’ (O-Reilly), Richard Forno
- ‘Computer Forensics’, Warren Kruse II & Jay G. Heiser
- ‘Know your enemy’ → honeypot project
- ‘Information Warfare’, Dorothy Dennings
- …

Reading stuff to fill long winter nights…

- ISO TR13335 General Management of IT Security
- ISO 15408 Common Criteria for evaluation and certification of IT security
- Baseline Protection Manual (BSI.DE)
- BS7799: Code of practice for Information Security Management (two parts)
- CobiT: Governance, Control and Audit for Information and Related Technology (ISACA)
- SSE-CMM: System Security Engineering - Capability Maturity Model

Questions

Discussions