FFI Forsvarets forskningsinstitutt

Effectiveness of Organisational Information security measures

Evaluation methods and main findings
FRISC Winter School 25th April 2013

Janne Hagen, PhD

Why is this topic relevant for researchers focusing on technical security mechanisms?

- Objectives of this presentation
  - Extending the perspective: Understanding the human factor and the link to security technology
  - An introduction to organizational security and security management – get security research into a broader context
  - An introduction on how to evaluate the effectiveness of organizational security measures

Content

- Threats and trends – towards an increasing gap between security and threats
- How to mitigate the human security challenge?
- How to evaluate the effectiveness of organizational security measures?

Threats and trends

- We are every single day exposed to intelligence and industrial espionage and the attacks against humans are increasing
- Modern countries have huge security challenges, vulnerabilities are often detected in software and commercial of the shelves technologies and the gap between threats and security is increasing:
  - We are publishing our lives and thoughts on social media – sharing is everything
  - “Kids are on social media while they are still in the womb, and they are born with a PDA on their lap”
  - New apps and services are developed, but few developers think much about the flip side of the coin (security) or unintended use by adversaries
  - Public sector goes digital
  - Stuff moves into the cloud

What have we lost, and where did the risk assessment go?

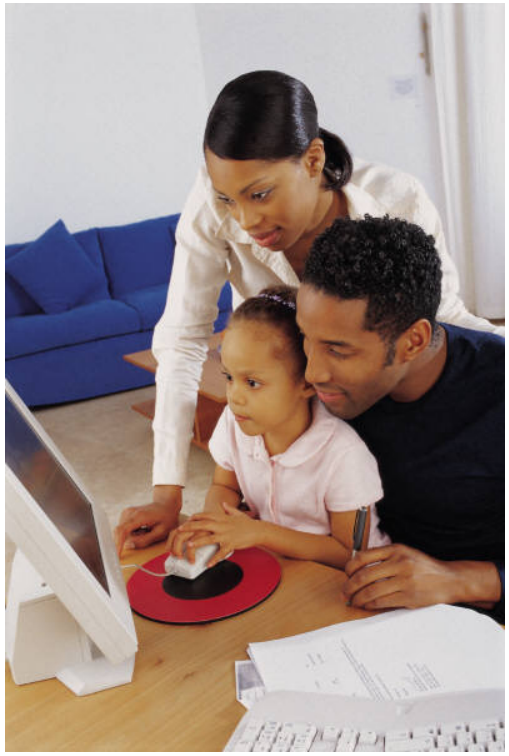
- We are using two senses, only: Vision and hearing, the ability to taste and smell, and even feel a touch is not used, except tapping the keyboard: What does this do to us?

- From real money to virtual money
- From real friendship to virtual friendship, where the number counts more than the quality of the relation?

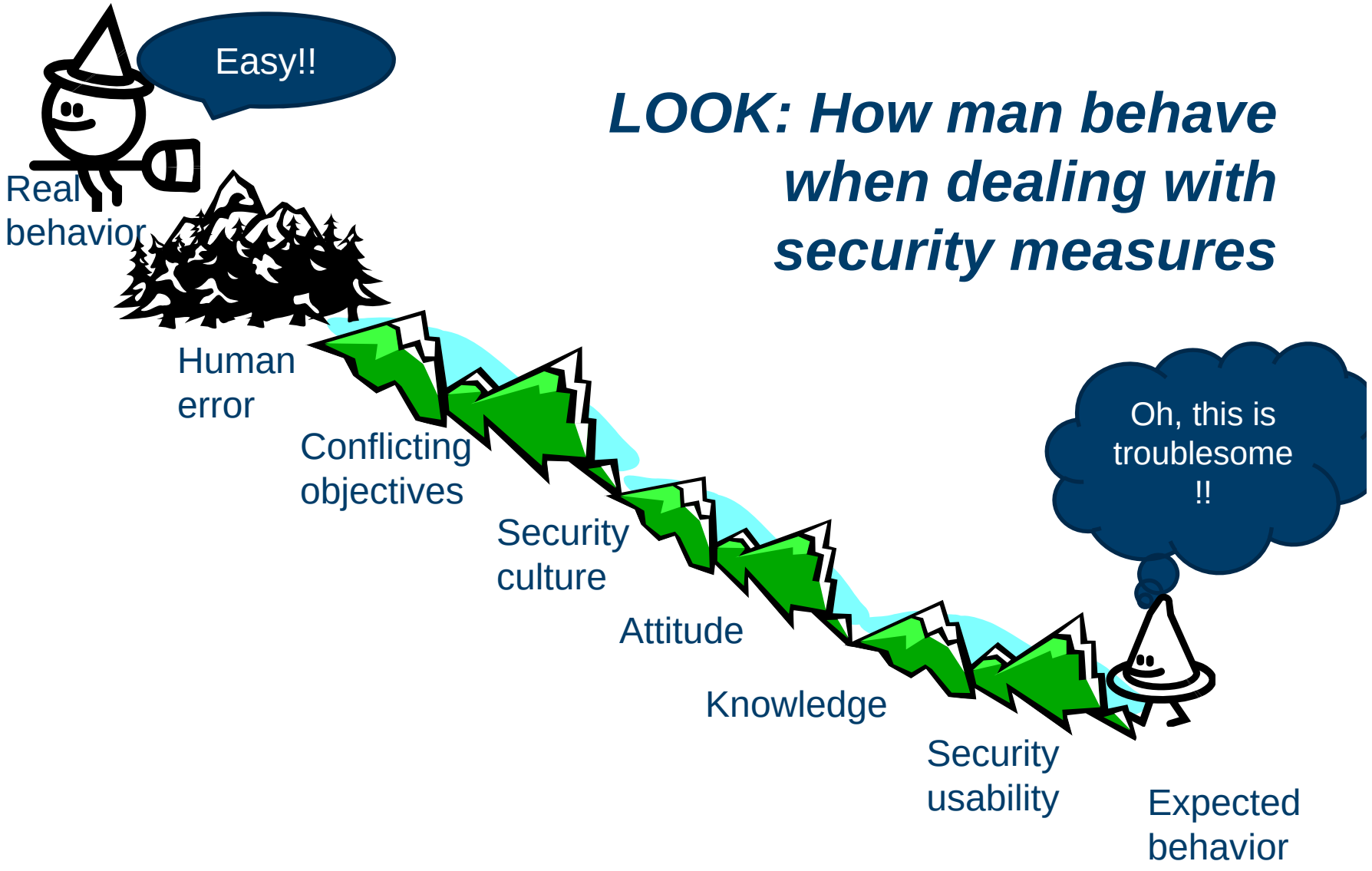
- What does this mean to information security and in particular trust?

A few questions:

- Easier to become a victim for targeted attacks?
- Is it simpler to cheat us, since we’re using fewer senses?
- At work, digitalization enables huge control and measurements regimes and time is always a problem, is it easier to make failures under such circumstances?



The answer: Humans - The weakest link



LOOK: How man behave when dealing with security measures

How do employees ommit security measures?

- Intended ommittance - >security simplification:
  - Do not read security guidelines
  - Use simple password policies, when possible, or the same password on several services
  - De-classify work in progress
  - Prioritize visibility in press to security - ex management (power supply)
  - Follow mainstream – everybody does
  - Disgruntled employee

- Unintended ommittance:
  - Phising
  - Social engineering
  - Human errors due to lack of knowledge or awareness

How to mitigate the human security challenge?

- Theoretical approaches
- Introduction to organizational security
- Security management principles
- The contributions of employees to security and insecurity
- The big challenge: Early training!

Theoretical approaches

- “The beauty and the beast” – Socio Technical Theory and the General Deterrence Theory

- You probably know the tale….but in the cyber domain the beast is not always a prince….it it is a real beast and the princess is also not always the princess she claims to be…but a witch

Theoretical approaches: Human roles in information security

Roles	Measures needed to improve/deal with each role and its theoretical connection	
	Socio-technical Theory	**General Deterrence Theory**
Resource person and contributor		
Causing unintentional failures	Awareness and training Improved working conditions	
Dealing with conflicting goals	Management follow-up	
Victim of social engineering	Awareness and training	
Disgruntled employee and/or opportunistic attacker	Management and follow up work	Sanctions and punishment
Spy or planted criminal	Screening and background checks	Sanctions and punishment

How should we best deal with security problems and unwanted behavior?

- Which is the best strategy - the socio-technical approach or the general deterrence?

- Do the the broken window theory apply to cyberspace; if yes, what can we do about it?

The “key” to solve the problem: Information Security Management System

Information management system

- Introduction to ISO/IEC and the ISMS standards ISO/IEC 27001 and 27002
- Why should organizations apply the standard?
- To what extent do organizations use the standards
- The flip side of the coin
- The way to successful implementation
- Summary

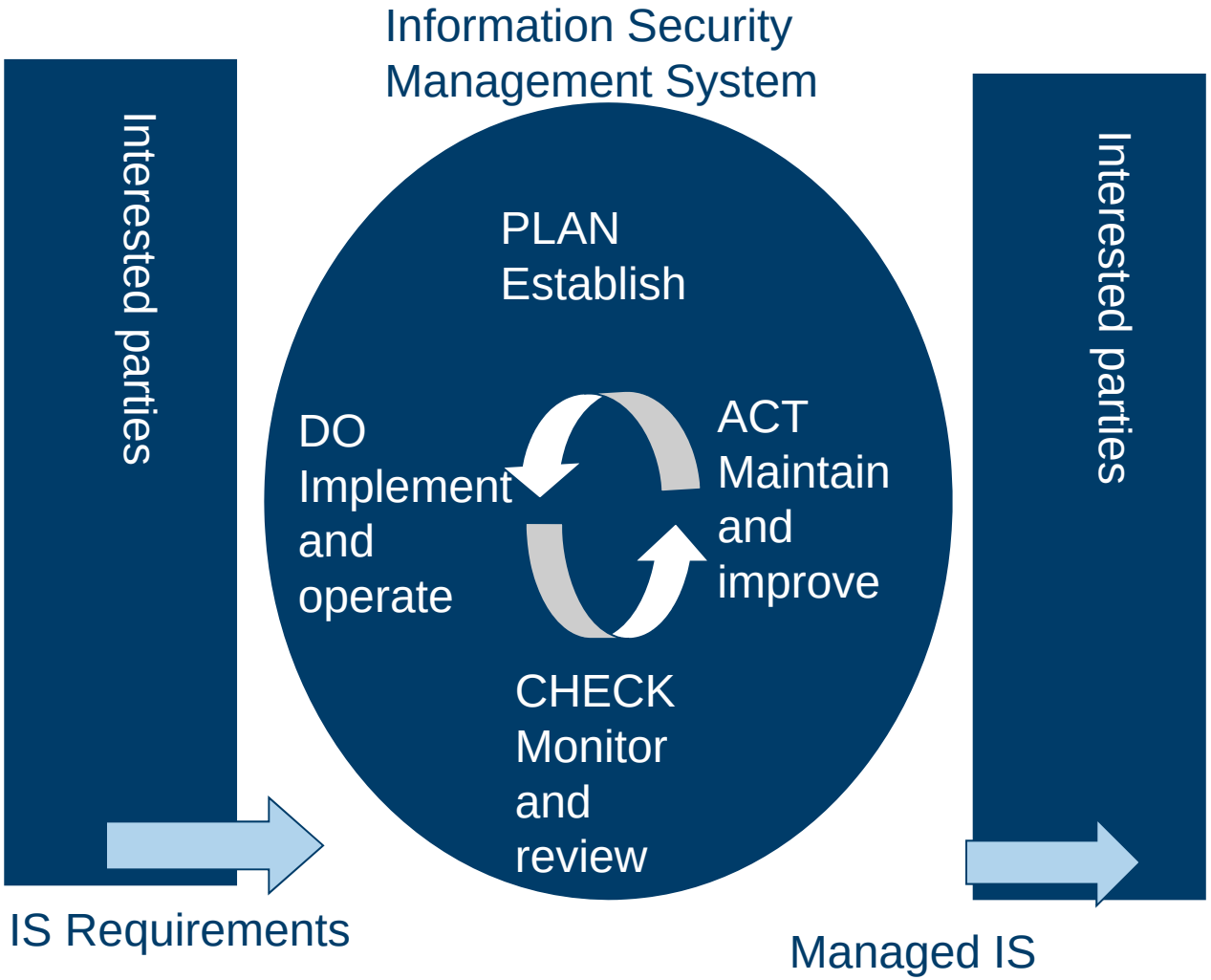
Introduction to ISO/IEC and the ISMS standards ISO/IEC 27001 and 27002

- The International Standardization Organization:
  - Founded 1947, headquarter in Geneva, Switzerland
  - 162 members (full membership, correspondent membership and subscriber membership)
  - Standards are copyrighted, drafts are free

- The International Electro-technical Commission (IEC)
  - Founded 1906, headquarter in Geneva
  - 86 members (full members and associated members)
  - Standards are available for purchase, some are free

ISO/IEC 27001: 2005 Process Approach

- Risk management
- Continual improvement
- Change management
- Management commitment

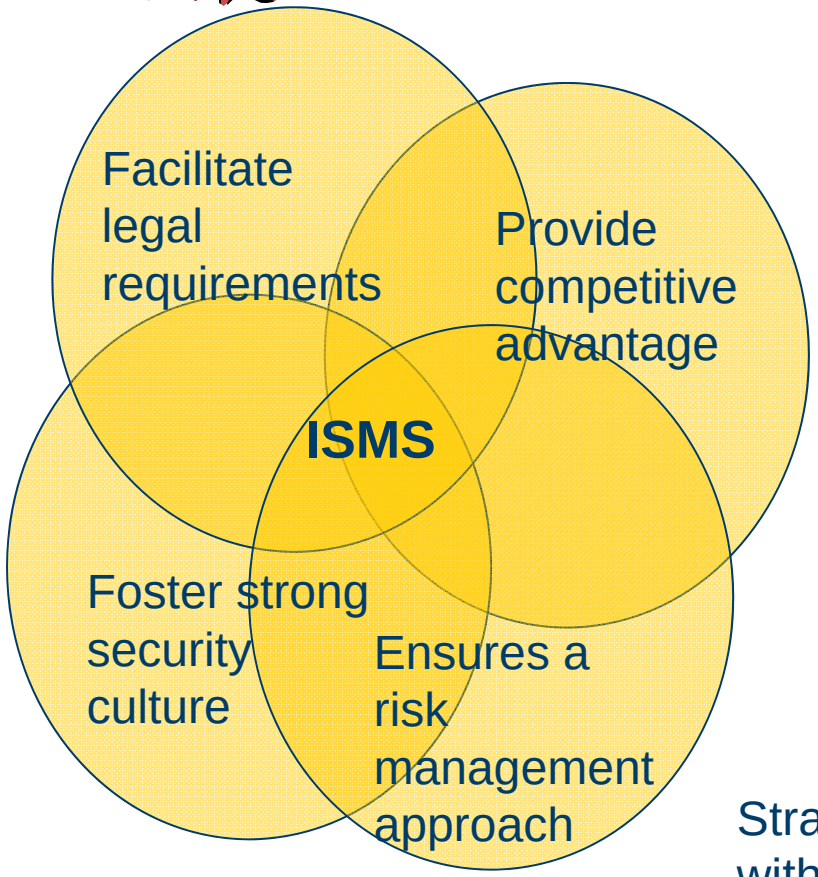


ISO/IEC 27002:2005: 11 controls

1. Security policy
2. Organization of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communication and operations management
7. Access control
8. Information system acquisition, development and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance

Why should organizations apply the standards?

Compliance with national and international laws and regulations



Customer trust, quality and positive return on investments

Commit management to IS and training employees

Strategies for dealing with risk

To what extent do organizations use the standards?

- 5693 businesses worldwide are certified against the standard ISO/IEC 27001 (January 2009)
  - Norway:10
  - Netherlands: 12
  - Sweden: 9
  - USA: 94
  - Japan: 3191!

- Relations to Quality Management (ISO 9001)
  - (Norwegian) ISO/IEC 27001 – 50% ISO 9001

- The standard as ISMS guideline/framework:
  - The Norwegian Oil and Gas Industry, 104 - Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems

The flip side of the coin

- Resource intensive (knowledge, money)
- No guaranty for quality in implemented measures or protection
  - Firewalls versus filter settings
  - Education versus quality and quantity
- No solution to the challenge of asymmetry between protection and attack
- Human management challenges remain (conflicting objectives)

PLAN
Establish

DO
Implement
and
operate

ACT
Maintain
and
improve

CHECK
Monitor
and
review

The way to successful implementation

- Clear understanding of the purpose and goals
- Actively involved senior management
- ISMS embedded in regular business operational processes
- Identify all legal, regulatory, contractual and business requirements
- Select suitable risk assessment tools and train staff to use the tools
- Decide how to deal with risks - both risk acceptance level and strategies
- Improve the system when facing security incidents and non-compliance
- Do not forget repeated training of staff, partners and contractors
- Establish a regular review programme

Summary

- ISO/IEC 27001 and ISO/IEC 27002 used mostly as guideline
- Gives a good framework for establishing and operating an ISMS through the PDCA cycle
- When applied, ensures documentation and routines, and management involvement
- When properly used, ensures continual improvement and corrective and preventive actions
- However, no guaranty for the quality of controls

References

1. ISO/IEC 27001: 2005 Information Technology – Security techniques – Information Security Management Systems – Requirements
2. ISO/IEC 27002: 2005 Information Technology – Security techniques – Information Security Management Systems – Requirements
3. Baker, W. H. and L Wallace, “Is Information Security Under Control? Investigating Quality in Information Security Management”, IEEE Security and Privacy, January-February, 2007: 36-44
4. Brenner, J, “ISO 27001 Risk Management and Compliance”, Risk Management Magazine, January, 2007: 25-29
5. Humphreys, T, “How to implement an ISO/IEC 27001 information security management system, ISO Management Systems, May-June 2006: 40-44
6. International Register of ISMS Certificates, http://www.iso27001certificates.com/ Downloaded 18th August 2009
7. Norwegian certification register: http://www.kvalex.no
8. Tang, J, “The Implementation of Deming’s System Model to Improve Security Management: A Case Study”, International Journal of Management, 254 (1) 2008:54-68

ISO/IEC 27002:2005: 11 controls

1. Security policy
2. Organization of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communication and operations management
7. Access control
8. Information system acquisition, development and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance

The contributions of employees to security

- Four case studies:
  - Two public and two private organizations
  - Examining formal security system, requirements, systems, routines and procedures, security awareness training
  - Interview guide with statements and personal interviews, N= 74, examining attitudes, knowledge and behaviour

- Results:
  - A good formal system does not guaranty employee compliance with policy
  - Resilient behavior among employees results in deviations in reporting and on “the spot” corrections
  - Training employees is important: Train them to observe and react!

The “key” to solve the problem: Information Security Management System + awareness raising and education

Knowledge of Security Instruction and Organization

Statement	Percentages that totally agree				
	Private A	Private B	Public A	Public B	Sig.
Knowledge:					
I know who the security manager is.	96	95	88	73	0.07
I know who the data security manager is.	70	30	44	65	0.03
I know where to find the instructions.	100	100	68	46	0.00
Attitudes:					
It is important to read the security instructions in order to have up-to-date knowledge.	78	80	48	58	0.06
Behaviour:					
It is less than 3 months since I last time looked up the security instructions.	65	90	32	5	0.00
It is less than 3 months since I last time contacted security personnel.	52	45	32	31	0.36
N (Number of employees asked)	23	20	25	26	

Reported Security Breaches

Statement	Percentages that totally agree				
	Private A	Private B	Public A	Public B	Sig.
Attitude:					
I will report security incidents.	83	65	76	42	0.02
I will confer with a college who breaks the rules.	83	55	80	42	0.01
I will report IT vulnerabilities.	65	75	76	35	0.01
Behavior:					
I have witnessed a security breach in the last 12 months.	26	25	44	12	0.07
I have reported a security breach in the last 12 months.	13	20	28	4	0.12
(N)	23	20	25	26	

Ranking the cases according to their formal security organization and the informal organization, or security culture

Ranking measurements: 4 = low-quality; 1 = highest-quality

Main characteristics:	Private A: High-quality formal system	Private B: Trust and culture	Public A: Competence and Involvement	Public B: Self-regulation
Formal				
Security policy	1	2	4	3
Reporting	1	4	3	2
Computer security	1	4	3	2
Visitor security	1	2	1	1
Credits (rank)	4 (1)	12 (4)	11 (3)	8 (2)
Informal organization, or security culture				
Security policy	4	2	1	3
Reporting	3	2	1	4
Computer security	1	2	3	4
Vistor security	1	3	1	2
Credits (rank):	9 (2)	9 (2)	6 (1)	13 (3)

Organizational security

- We know from the Norwegian Computer Crime Survey that:
  - Mature security technologies is well distributed among Norwegian enterprises
  - There is less security in depth, despite that insiders (own employees, consultants and contractors) are behind about half of the incidents
  - Crime and incidents are seldom reported to the police, just the largest incidents are
  - Enterprises implement new technologies, much of it without thinking on potential risks

The big challenge: Early training!

- Computer security and programming into the public school
  (National Strategy for Information Security)
  Or even into the kindergarten!

- Is training enough, why or why not?
- What should be included in such training?

Back to the research questions

1. How to mitigate the human security challenge?
   - Education and training, awareness raising for all members of the society
   - Reporting incidents to the police and following this harmonizing statutes on computer crime world wide because crime is world wide
   - Risk management system (risk based approach, change management, continual improvement and management commitment)
2. How do we evaluate the effectiveness of organizational security measures?

Presumption

"The human factor is often neglected in the information security work within organizations, although its impact on security may be measured by the use of simple indicators and influenced significantly by security measures."

Theoretical approaches of security measurement

- Four perspectives for measuring effectiveness of information security measures:
  - The risk management perspective
  - The economic perspective – return of security investments
  - The legal perspective – compliance to law
  - The cultural perspective – examining attitudes, knowledge, and behaviour aspects according to organizational policy requirements

- Evaluation and measurement methods:
  - indicators, metrics, penetration testing, compliance with standards, risk assessments etc....

Research methods

- Research strategies:
  - Surveys
  - Case studies
  - Experiments
- Mix of qualitative and quantitative methods contribute to:
  - Complementary
  - Facilitation
  - Triangulation

A case: How to measure compliance with organizational security policy?

- Get an overview of the formal security system
  - Organizational security policy
  - Guidelines and requirements
  - Education and training
  - Incident handling and reactions
- Formulate statements:
  - Attitudes: I will report security incidents
  - Knowledge: I know that I am obliged to report security incidents
  - Behavior:
    - I have witnessed security incidents reported security incidents
    - I have reported security incidents
- Interview of employees:
  - Present mixed statements and ask follow up questions to check out facts
- Analyze the data
  - Where is the problem: Any differences between attitudes, knowledge or behavior?
  - Benchmarking among sections and departments – where is the biggest problem?

To sum up:

- Difference between awareness and good behavior, there is not necessarily a correlation between the two
- A good formal security system/organization does not correlate with a good security culture

How to evaluate the effectiveness of security e-learning

- Enterprise case:
  - Wilh Wilh. Group – an international logistics provider

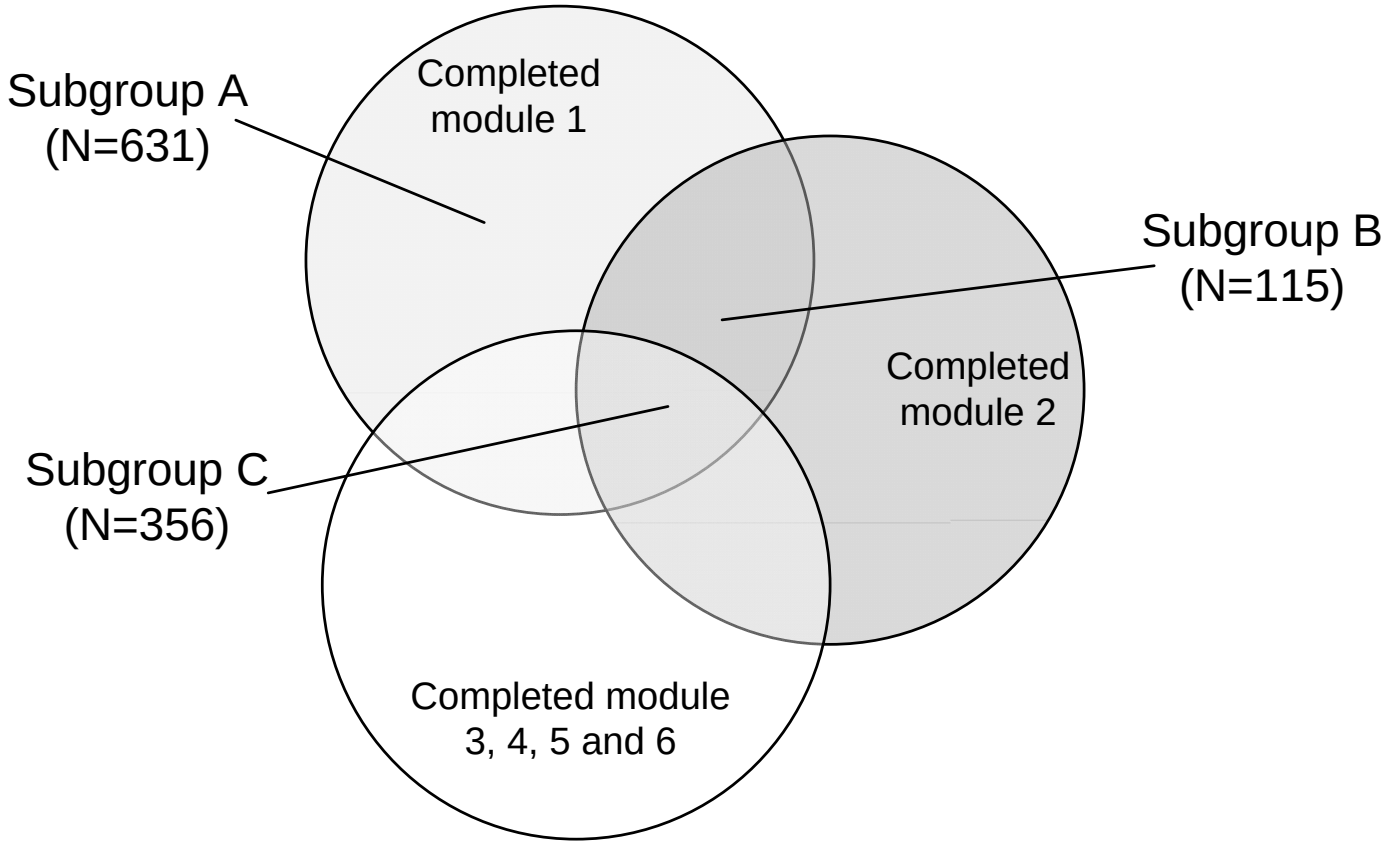
- E-learning program with six modules:
  - Introduction
  - Information security
  - Travel security
  - Personal security
  - Security of facilities
  - Internal/external communication

- Does it work as intended?
- Do employees increase their knowledge, and improve their attitudes and behavior?

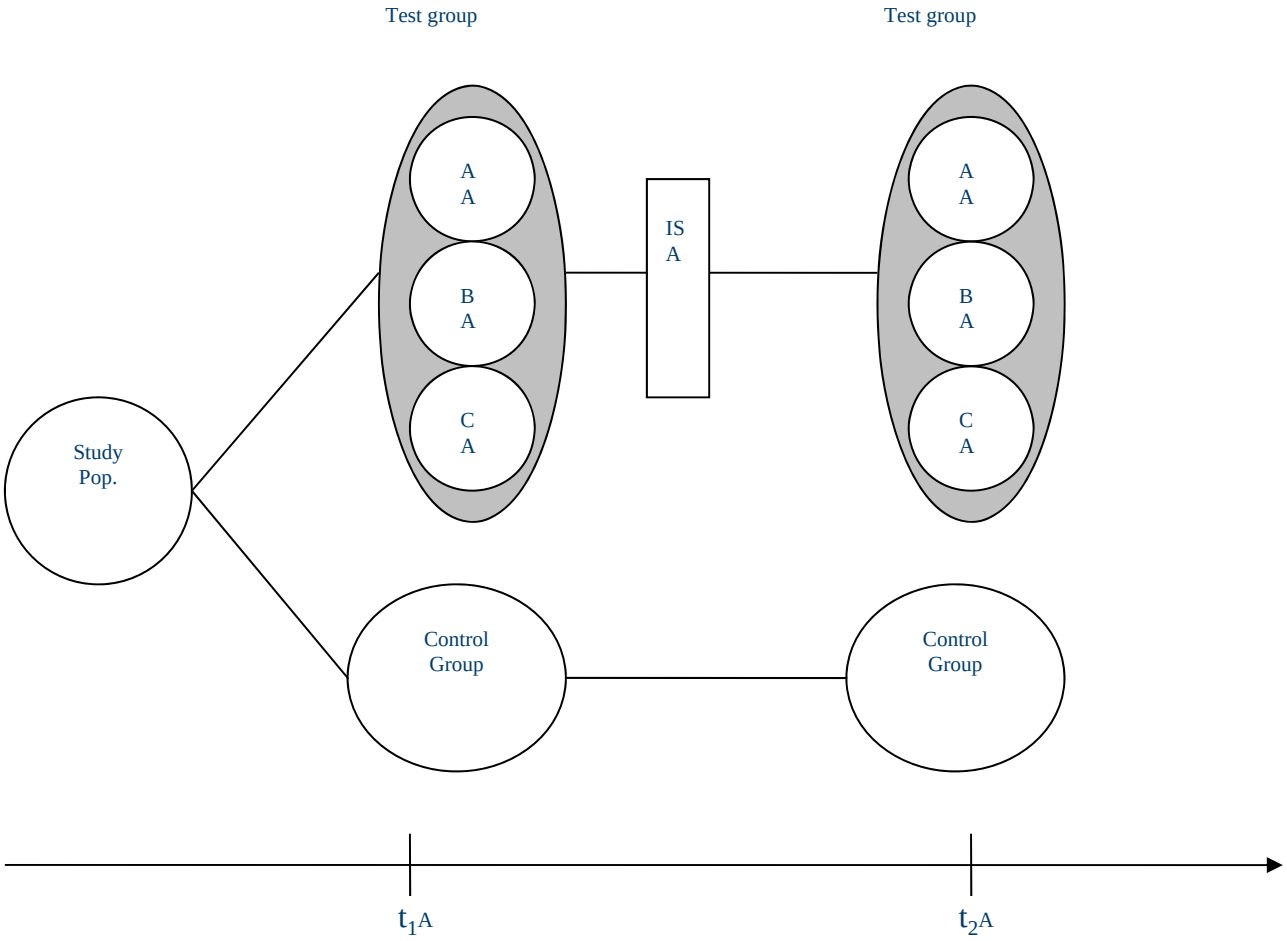
Research design

- Field experiment, use of test group and control group
- 3994 employees were divided into the two groups
- The management informed about ISA and the forthcoming evaluation of the ISA program
- The first survey was conducted 1 week before the ISA program was launched
- The second survey three weeks after the ISA program was launched.

The three sub groups and how the test group members distribute among the modules



Evaluation design



Statistical analyses

- Both surveys included questions of knowledge, awareness and behavior
  - Knowledge were measured by multiple choice questions with three possible answers,
  - Awareness were measured by the use of a five point Likert scale
  - Behaviour were measured at five point scale measuring frequences

- Used factor analysis to produce indexes that were later on included in the analysis and for the test of the hypotheses
- Used paired sample T-test procedure to test several hypotheses for differences between the test group and control group

Extract from independent sample t-tests when two ISA modules were completed versus more

Scales:
The indexes ranges from 5 (best) to 1 (poorest).
The tests for the intervention group and control group are two tailed. *p<.10, **p<.05, ***p<.01,****p<.005, ***** p<.001. SD= standard deviation, T= t-value, df=degrees of freedom.

Index	T1 Mean (SD)	T2 Mean (SD)	T (df)
Definition of integrity			
Sub Group A	1.86 (1.64)	2.04 (1.76)	1.98 (542)*
Sub Group B	1.90 (1.68)	2.33 (1.89)	1.99(92)**
Sub Group C	2.08 (1.78)	2.66 (1.97)	4.75(298)*****
Definition of physical security			
Sub Group A	3.14 (2.00)	3.48 (1.95)	3.29 (542)**
Sub Group B	3.32 (1.99)	3.15 (2.00)	0.67 (92)
Sub Group C	3.29 (1.98)	3.52 (1.94)	1.81 (298)*
Awareness:			
Security vs functionality			
Sub Group A	3.43 (0.58)	3.53 (0.58)	4.43 (542)*****
Sub Group B	3.34 (0.61)	3.46 (0.59)	1.98 (92)*
Sub Group C	3.53 (0.62)	3.63 (0.67)	4.00 (298)****
Reporting			
Sub Group A	3.80 (0.70)	3.79 (0.71)	-0.25 (542)
Sub Group B	3.72 (0.82)	3.81 (0.76)	1.32 (92)
Sub Group C	3.78 (0.70)	3.93 (0.74)	4.04 (298)*****
Behavior:			
Write down passwords on paper			
Sub Group A	4.12 (1.07)	4.24 (0.95)	2.98 (542)****
Sub Group B	4.17 (1.16)	4.28 (0.93)	1.23 (92)
Sub Group C	4.28 (1.00)	4.36 (1.90)	1.74 (298)*
Report incidents			
Sub Group A	3.91 (1.28)	4.06 (1.13)	-2.59 (542)*
Sub Group B	3.98 (1.26)	4.06 (1.09)	-0.70 (92)
Sub Group C	3.92 (1.32)	4.19 (1.11)	-4.02 (298)*****

Limitations

- Short time distance between measurements and the ISA intervention
- An independent social engineering test could have strengthened the validity

Some lessons learned

- In field experiments you can not control for all factors, i.e. the Hawthorne effect
- Management commitment is important!
- It is difficult to make good questions, a pilot could be useful, but we did not have time for that – we had a small internal review among security group members
- Patience is gold
- We used SPSS (similar freeware is PSPP)
  - It worked well
  - Easy help functions, explaining the theory

- A later follow up study documented that some effects were temporary; this indicates a need for continuous learning

Some more studies giving advice on where to put the efforts?

- Mapping security according to defense in depth and defense in depth
- Regulation of information security and the impact on top management commitment
- Do organizational security measures contribute to the detection and deterrence of IT-system abuses?

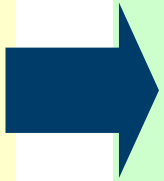
How can we evaluate the effectiveness of information security measures aimed at strengthening human security behavior?

- What we knew:
  - Social hacking and penetration testing
  - Audits and review
  - Risk analysis
  - Not much about evaluating economic effects

- Contribution of the dissertation:
  - Taxonomy
  - Method for measuring employee compliance with security policy
  - Intervention study and evaluation of new training

How effective are these information security measures?

- What we knew:
  - Malicious attacks and computer crime
  - Humans can easily be fooled by social engineering attacks
  - Technical measures do not give 100% protection
  - Imperfect implementation and limited management commitment reduces the effectiveness of measures
  - Laws have some effect on management commitment



- Contribution of the dissertation:
  - Laws and good supervisory practices influence on formal security system and management attitudes and commitment
  - A good formal system help employees detect security violations
  - Employees' ability to detect and report can be further improved by awareness training

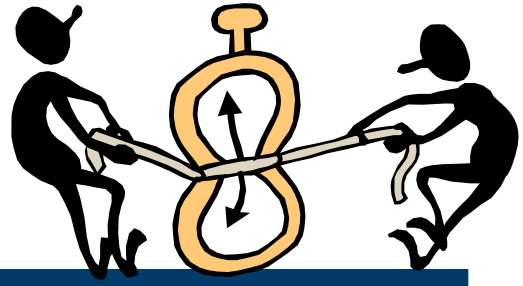
How should these information security measures be integrated in the organization?

- What we knew:
  - The practical implementation issues are covered by consultants
  - Researchers prefer to develop new concepts, models and systems
  - How enterprises have implemented formal security systems with emphasis on building fortresses

- The contribution of the dissertation:
  - Focus on the soft core behind the stronger formal security system and perimeter security
  - Learn from the field of safety management and apply a socio-technical approach

Limitations

- Data – quality, response rate, randomisation etc.
- Strengths and weaknesses with different methods for collecting data
- The filtering by the researcher (knowledge, experience etc)



Further research

- More research on the human factor!
- Develop good methods for teaching appropriate attitudes towards information security
- The role of business management in relation to information security
- Information security economy