A Closer Look at Information Security Costs

WEIS 2012

Matthias Brecht, University of Regensburg
Thomas Nowey, Krones AG
2012-06-26

Theoretical Models Assume Costs and Benefits as Given

- Example of Cost-Benefit-Calculation (Faisst et al, 2007):

$$\text{Net Present Value} = -I_0 + \sum_{t=1}^{T} \frac{\Delta E(L_t) + \Delta OCC_t - C_t}{(1+i_{calc})^t}$$

with

I_0 = initial investment for security measure

$\Delta E(L_t)$ = reduction of expected loss in t

ΔOCC_t = reduction of opportunity costs in t

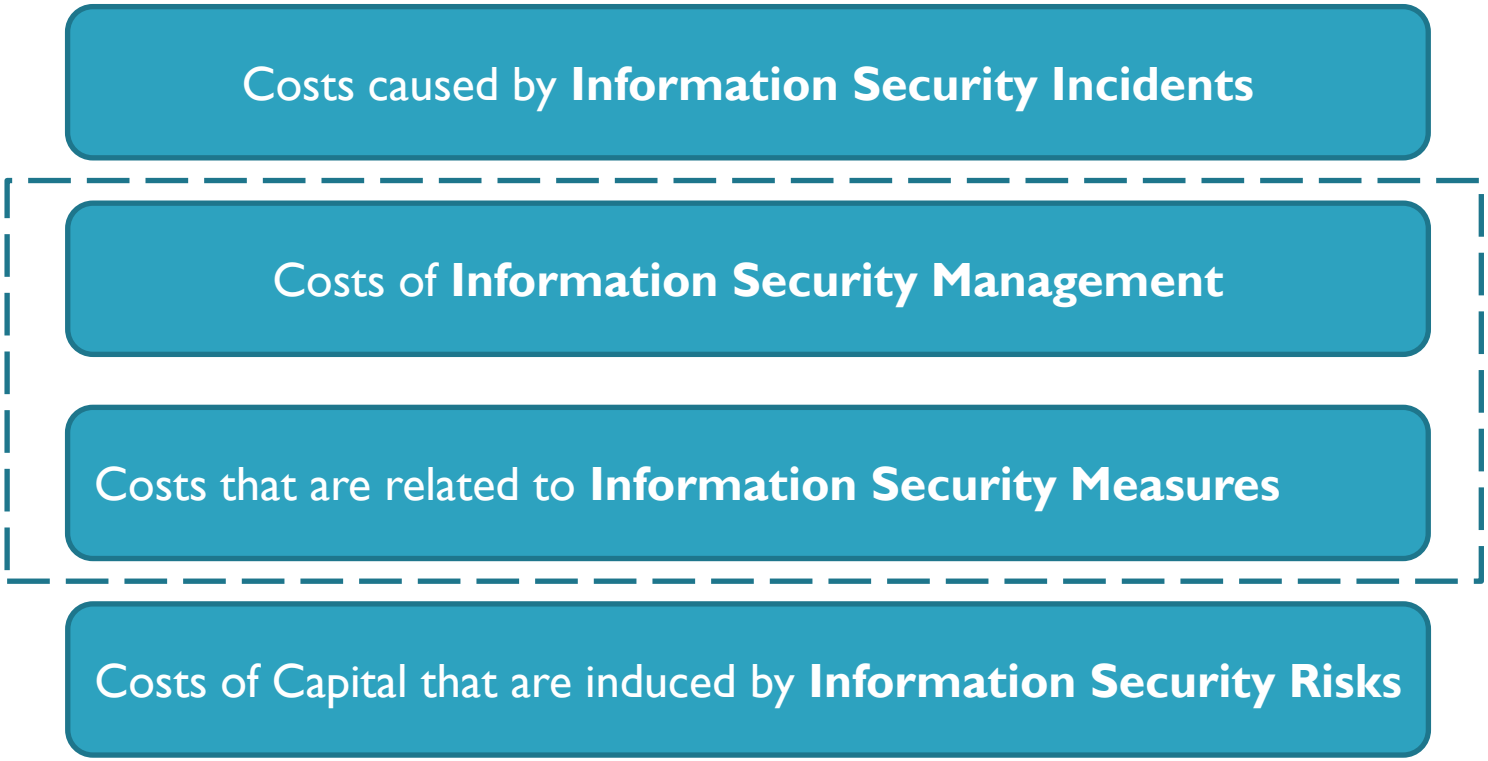
C_t = cost of security measure in t

i_{calc} = discount rate

Goals of This Talk

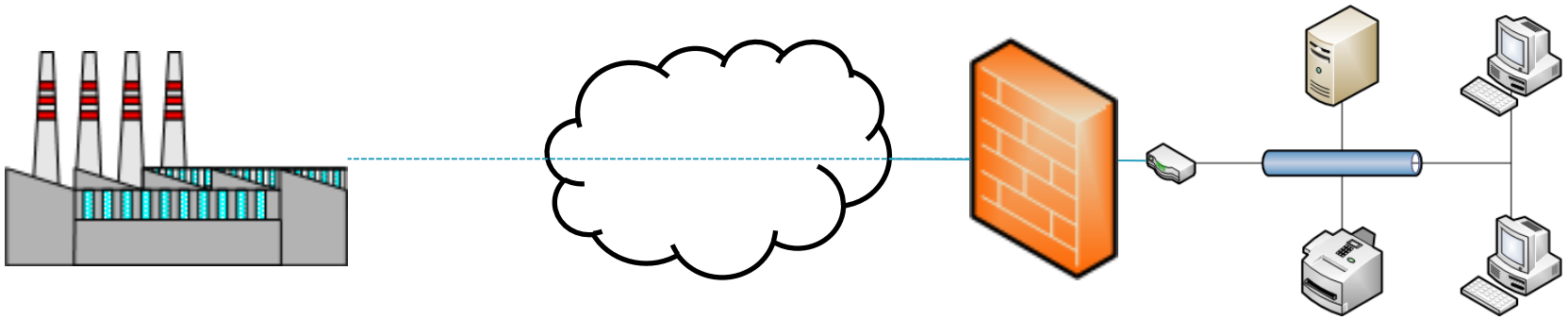
1. Assessing information security costs is difficult
2. Approaches for categorising and determining information security costs are a prerequisite for the application of economic models and research results to practice
3. The right approach depends on scope and application
4. An ISMS-oriented approach is required
5. Further research is necessary

How Can We Define Information Security (IS) Costs?



Working definition: Costs that are associated with all kinds of measures or activities within an organisation that are aimed at reducing information security risks for its information assets.

Example 1: Investing in a Firewall



Cost

- Hardware
- Software
- Operations
- Training
- …

Benefit

- Filter NWTraffic
- VPN Access
- Traffic Shaping
- Monitoring
- …

Example 2: Introducing Identity Management

Q1: How should we categorise costs?

Identity Management

Q2: Are all of those security costs?

Cost

- Project Management
- Tools
- Changed Processes
- Training
- …

Benefit

- Access Control
- Automated Provisioning
- Compliance
- User Satisfaction
- …

Related Work

- Cost-Benefit-Evaluation (e.g. Berinato; Soo Hoo; Faisst)
  - ROSI, optimal investment levels, decision analysis
  - Formulas, rules, no data

- Cost of Cyber-Crime (e.g. Florencio & Herley)
  - Empirical research, usually on a macro level
  - Huge variance of results from millions to billions

- Surveys on Information Security Costs (e.g. Penn; Sullivan)
  - Information security spending surveys, mostly as percentage of IT-Budget
  - Company or state level, no drill-down

- Costs of Quality (e.g. Feigenbaum; Schiffauerova & Thomson)
  - P-A-F Prevention- Appraisal-Failure
  - Activity oriented; purpose, situation, environment, individual needs

Applications of Cost Quantification

Application	Implications
Budgeting	Provide a basis for allocation of resources
Cost Accounting	Enable consistent cost accounting throughout the enterprise
Risk Management	Facilitate prepration of risk management decisions
Cost-Benefit-Analysis	Enable economic assessment of measures/projects
Benchmarking	Ensure comparability with other organisations
Surveys/Research	Enable identification of trends and preferences

Scope of Cost Quantification

Single measure	Whole company
IT-Security	Information Security
Technical control	ISMS

Trends in Information Security – It's Not About Anti-Virus

- From IT-Security to Information Security
- People focus – consumerization of IT requires individual responsibility
- Process focus – IS needs to follow well defined processes
- Architecture focus – single measures need to be orchestrated
- External Partys become more important

Challenges in Quantifying IS Costs

- Information Security Management is a cross-functional task
  - Process/activity focus, no mapping to a category of cost-accounting
- Differing goals and information needs
  - See slide 8
- Hidden costs e.g. for security outsourcing
  - e.g. managing and monitoring outsourcing relationship
- Finding the right baseline (especially for benchmarking)
  - e.g. sales, earnings, it-budget
  - Importance of IT is not necessarily equal to importance of IS

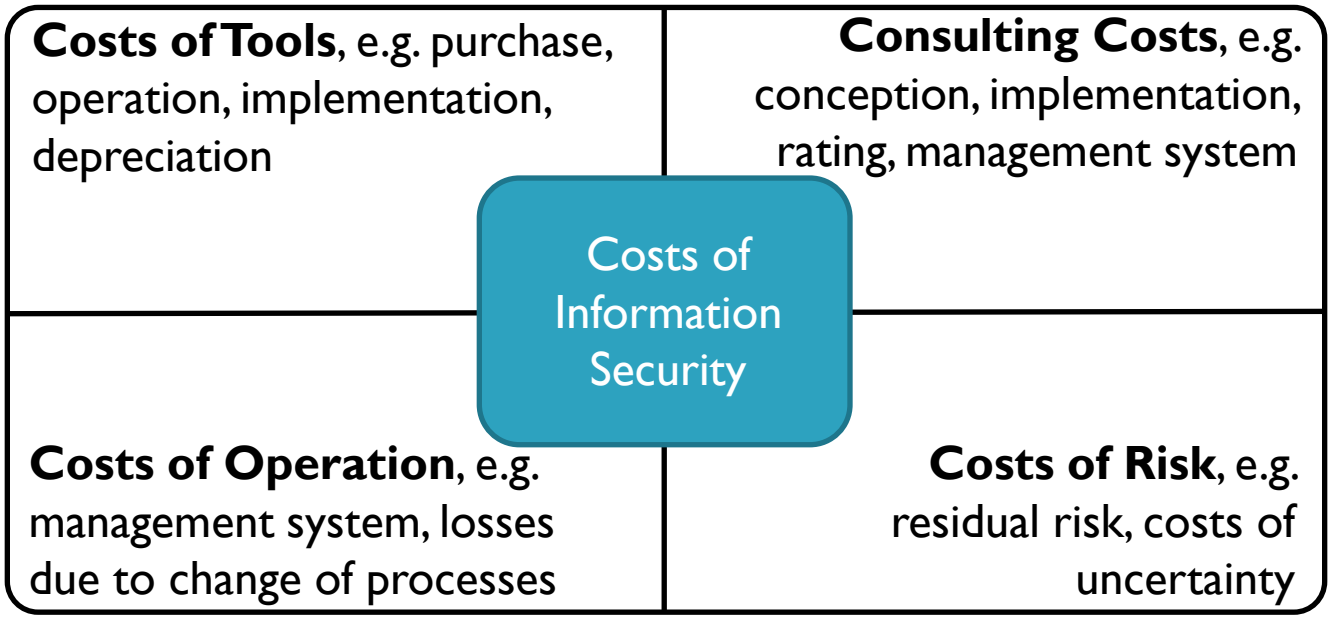
Existing Approaches for Categorising IS Costs

- Balance Sheet Oriented Approach / Accounting
  - e.g. Gartner or other Benchmarking initiatives by Consulting Firms
  - Categories (Gartner): Personnel Costs(40 %), Hardware Costs (21 %), Software Costs (29 %), Outsourcing/MSS Costs (10 %)
  - Pro: easy to determine
  - Con: focus it-security, comparability questionnable

- Security Measure Life-Cycle Approach
  - e.g. TCO
  - Categories:
    Costs of Purchase, Costs of Setup, Costs of Operation, Costs of Change
  - Pro: well-suited for cost-benefit-calculations of single measures
  - Con: IT-focus, not suitable for benchmarking

Existing Approaches for Categorising IS Costs

- IT-Security process oriented approach
  - e.g. Humpert-Vrielink & Vrielink (figure below)
  - Categories: see below
  - Pro: process-oriented, covers some high-level aspects
  - Con: focus on single measures, not fully compatible with definition, not suitable for benchmarking

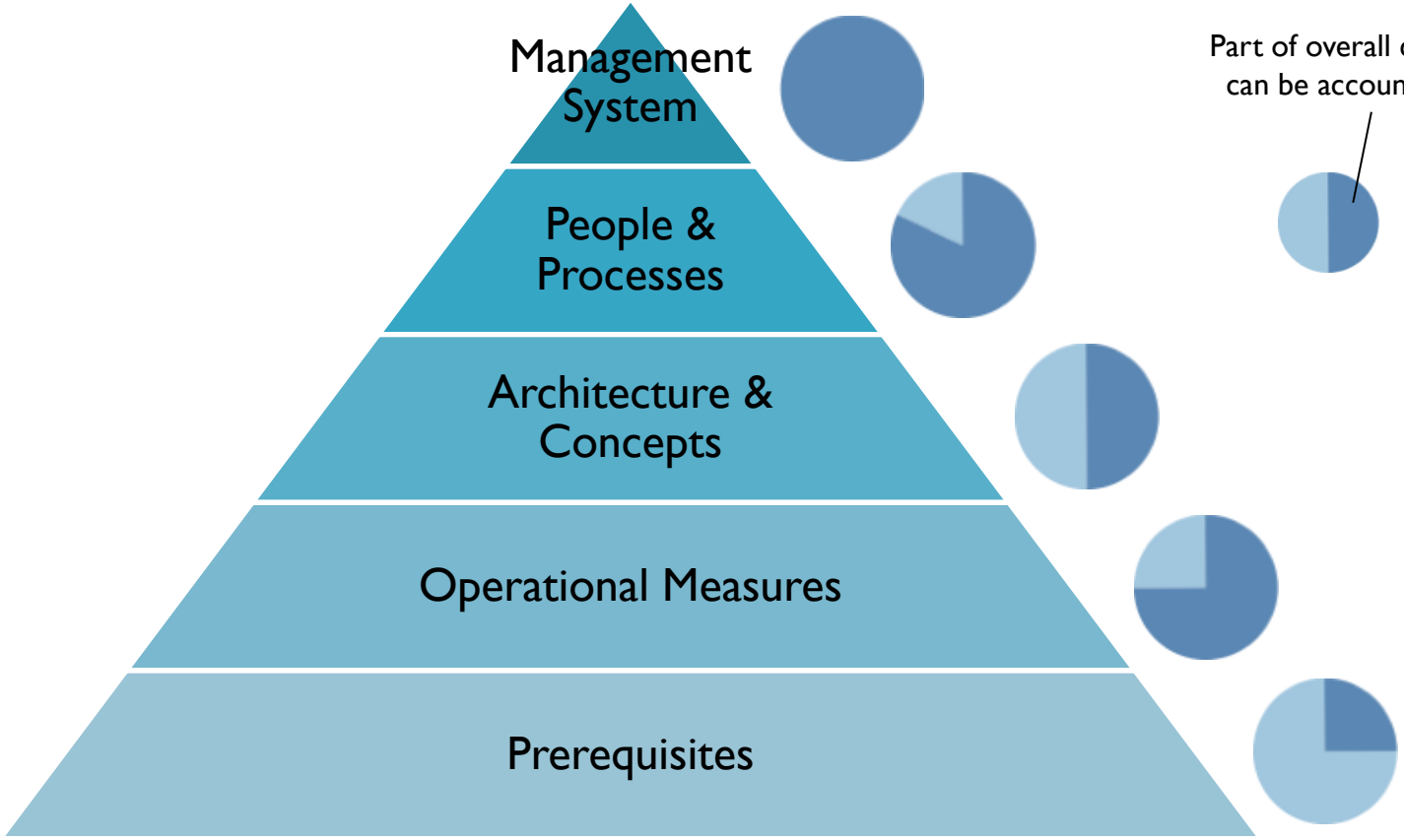


Towards new Approaches for Categorising IS Costs

- Two approaches for categorising IS costs
  - ISMS-Layers
  - ISMS-Controls

- Especially for benchmarking purposes we propose two metrics
  - **Determinability:** describes how difficult the determination of the related costs is in practice
  - **Information Security Cost Ratio:** describes the real percentage of the costs that may be accounted to information security

ISMS-Layers Approach



Pro: considers all aspects of Information Security Management
Con: possibility to drill-down required, no data, not for single measures

ISMS-Controls Approach (Based on ISO/IEC 27001)

Section	Control/Management Task	Determin-ability	IS Cost Ratio
Main Part (Mandatory)	Risk Management	easy	medium
	…		
	Internal Audits	very easy	very high
	…		
Appendix A (Controls)	A.5 Security Policy	easy	very high
	…		
	A.8 Human Resources Security	hard	low
	…		
	A.11 Access Control	medium	high
	...		

Pro: 7840 certificates worldwide (April 2012, www.iso27001certificates.com)
Con: does not consider architectural layer, not for single measures

Comparison of Approaches for Categorising IS Costs

	Balance	Meas. LC	IT-Sec Process	ISMS Control	ISMS Layers
Single measures	o	+	o	-	-
Whole organisation	o	-	o	+	+
IT-Security centric	+	+	+	o	-
Information Security centric	o	-	o	+	+
Cost-Benefit-Analysis	o	+	o	-	-
Benchmarking	o	-	-	+	+
Comparing measures	o	+	o	o	-
Compatibility with ex. data	+	+	o	-	-
Determinability	o	-	o	+	+
IS Cost Ratio	o	-	o	+	+

Ideas for Future Research

- Empirical evaluation
  - Collecting data and comparing the different approaches
  - Determination of IS Cost Ratio and Determinability
  - How are different categories of security costs correlated with individual risk exposure or with individual risk appetite?
  - Technical measures vs. audits and awareness – what is more effective?

- Improve approaches
  - Determination and evaluation of possible combinations
  - Analyse effects of different baselines/reference parameters
  - Absolute costs vs change in costs
  - Define basic security processes and services

- Determine efficiency of resource allocation

Questions?

thomas.nowey@krones.com