



Verfahren zur Wirtschaftlichkeitsanalyse von Investitionen in IT-Sicherheit - Eine Vorstudie

Prof. Dr. Rainer Rumpel
18. Dezember 2007



1. Situation und Motivation
2. Rahmenbedingungen
3. Allgemeine Methoden zur
Wirtschaftlichkeitsanalyse
4. Anwendung der Methoden in der IT
5. Wirtschaftlichkeitsanalyse im Bereich IT-Sicherheit
6. Weitere Schritte



1. SITUATION UND MOTIVATION

1. Situation und Motivation



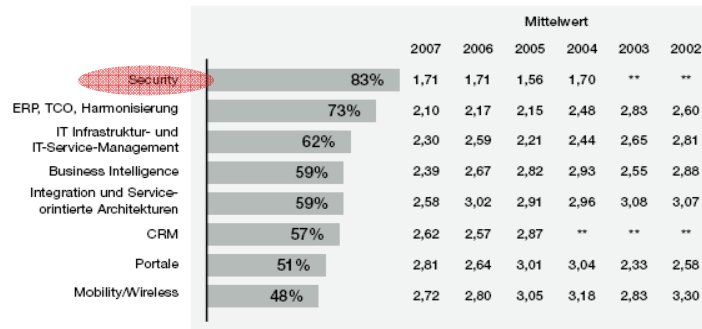
- Bislang noch relativ wenig wissenschaftlich fundierte Betrachtungen zu Kosten-Nutzen-Relation von Investitionen in IT-Sicherheit
- Gründe
 - kein direkter Nutzen erkennbar
 - Nutzen → Risikominderung
 - schwer berechenbar



■ Capgemini-Studien *IT-Trends 2007*

Abb. 01: Wichtigkeit von IT-Themen

Wie wichtig sind die folgenden Themen für Sie in den kommenden Jahren?



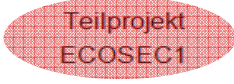
Basis: Alle Befragten (n = 96) – Prozentangaben, Mittelwerte¹; ** nicht erhoben
¹ Top-3-bis: Werte „1“ und „2“ auf der Skala von „sehr wichtig“ (1) bis „völlig unwichtig“ (6)

Capgemini 2007



2. RAHMENBEDINGUNGEN

▪ Ziele

<ol style="list-style-type: none">1. Erfassung der vorhandenen Methoden zur Wirtschaftlichkeitsanalyse in der Betriebswirtschaft2. Erfassung der vorhandenen Methoden zur Wirtschaftlichkeitsanalyse im Bereich IT (z.B. ROI)3. Analyse der vorhandenen Methoden zur Wirtschaftlichkeitsanalyse im Bereich IT-Sicherheit (z.B. ROSI)	
<ol style="list-style-type: none">4. Synthese eines praxistauglichen, transparenten Verfahrens zur Wirtschaftlichkeitsanalyse von Investitionen in IT-Sicherheit5. Exemplarische Erprobung des Verfahrens in einer Praxissituation	Teilprojekt ECOSEC2

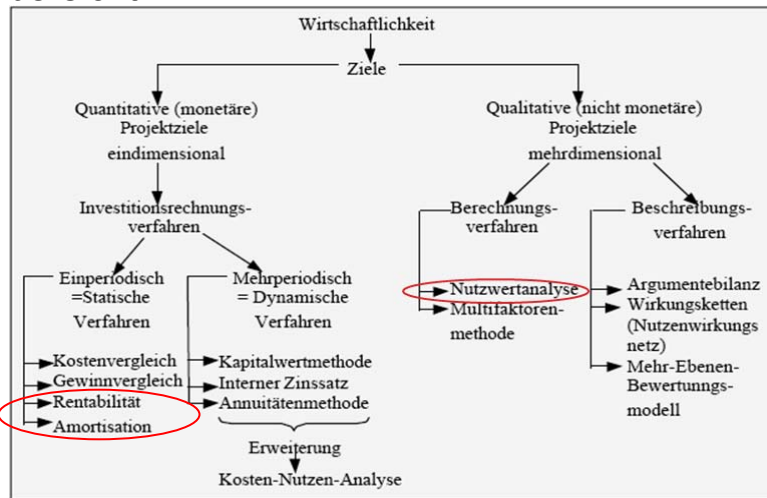
Kooperationspartner

- PERSICON Information Risk Management GmbH
- Euroconsult Deutschland GmbH
- TLG IMMOBILIEN GmbH

3. ALLGEMEINE METHODEN ZUR WIRTSCHAFTLICHKEITSANALYSE

3. Allgemeine Methoden zur Wirtschaftlichkeitsanalyse

Übersicht

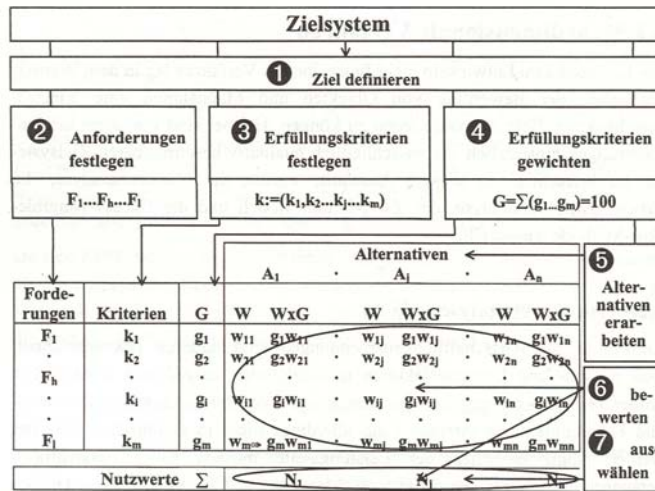


Quelle: Siebold, Y., FH Erfurt

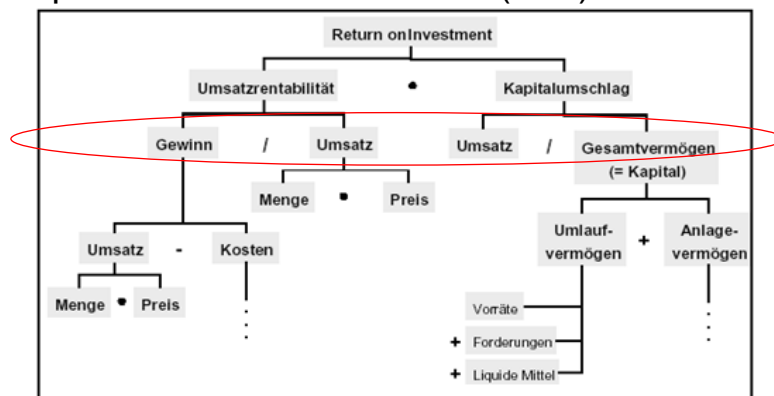


Beispiel: Nutzwertanalyse

- Verfahren zur Entscheidungsunterstützung beim Vergleich verschiedener Alternativen
- Keine Kostenbetrachtung!



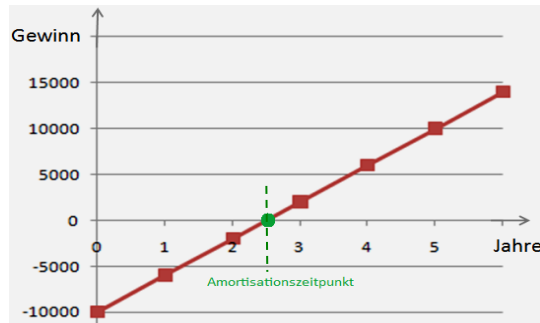
Beispiel: Return on Investment (ROI)



Quelle: Mertens, Universität Erlangen

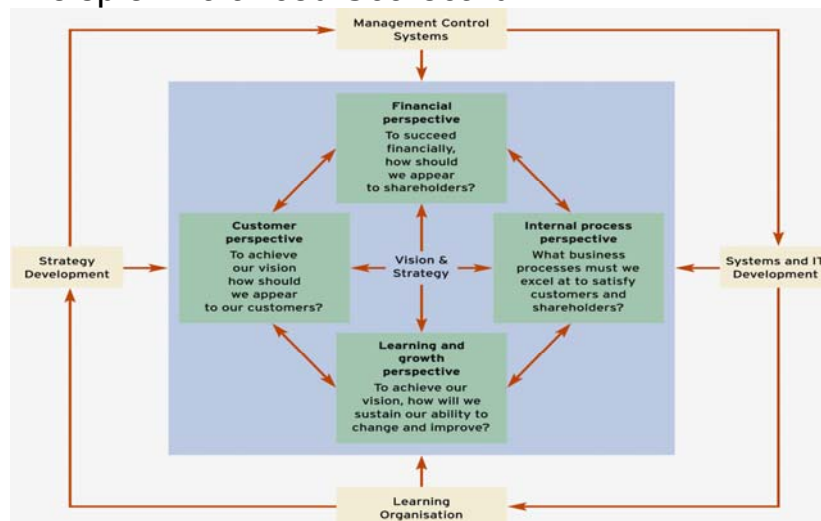
$$RoI = \frac{\text{Periodengewinn}}{\text{Investiertes Kapital}}$$

- Beispiel: Return on Investment (ROI)



- Wenn $RoI = \frac{\text{Periodengewinn}}{\text{Investiertes Kapital}} = \frac{\text{Gewinn / Jahr}}{10.000,-EUR} = \frac{4.000,-EUR / \text{Jahr}}{10.000,-EUR} = 1,$
dann gilt: **Amortisationszeit = 1/RoI = 2,5 Jahre**
Amortisationszeit = Payback Period (PP)

- Beispiel: Balanced Scorecard





- Beispiel: Balanced Scorecard
 - Erforderlich:
 - Strategische Erfolgsfaktoren
 - Welche (messbaren) Leistungselemente beeinflussen die erfolgreiche Umsetzung der Strategie(n) am stärksten?
 - Kennzahlensystem für jede Perspektive



4. ANWENDUNG DER METHODEN IN DER IT



▪ Nutzwertanalyse am Beispiel Kauf eines IT-Systems

1. Festlegen der zu erfüllenden Forderungen
Sicherheit, Problemlösungsorientierung, Service, Geschwindigkeit
2. Aufstellen der Erfüllungskriterien
Beispiel für die Forderung Sicherheit: Reparaturanfälligkeit, Möglichkeiten zur Zugangsbeschränkung, Ausfallraten
3. Gewichten der Erfüllungskriterien
Die Kriterien haben unterschiedliche Relevanz und werden daher unterschiedlich gewichtet (Summe der Gewichte = 100).
4. Erarbeiten der Alternativen
Alternative 1: lokales PC-Netz mit zentralem Server
Alternative 2: Abteilungsrechner, die mit dem Großrechner verbunden sind.
Alternative 3: Terminals, die an den Großrechner angeschlossen sind
5. Bewerten der Alternativen anhand einer geeigneten Skala
Oft werden Verhältnisskalen oder wie im Beispiel Punktskalen (1-10) verwendet.



Kriterien	Gewichtung G	Alternativen					
		1. PC-Netz		2. Abteilungsrechner		3. Groß-DV-Anschluss	
		Wert W	G x W	Wert W	G x W	Wert W	G x W
Reparaturanfälligkeit	24	7	168	8	192	8	192
Zugangsbeschränkung	8	7	56	8	64	9	72
Ausfallraten bei Referenzkunden	4	8	32	8	32	7	28
Wartung	4	8	32	6	24	6	24
Softwareangebot	10,5	10	105	6	63	7	73,5
Ganzheitliche Nutzung	10,5	10	105	8	84	8	84
Angemessenheit	8,75	10	87,5	9	78,75	9	78,75
vorh. Qualifikationen	5,25	10	52,5	7	36,75	7	36,75
Hotline	2	8	16	8	16	8	16
Ansprechpartner	4	7	28	9	36	9	36
Schriftliche Unterlagen	2	9	18	9	18	9	18
Verfügbarkeit des Servicepersonals	2	8	16	9	18	9	18
Hardwareplattform	2	10	20	8	16	8	16
Schnittstellenstandards	3	9	27	9	27	9	27
Vernetzungsmöglichkeit	5	10	50	10	50	10	50
Laufzeitverhalten	5	10	50	9	45	9	45
	100		863		800,5		815

Return on Investment (ROI)



CDWatch erlaubt es alle in einem Netzwerk verwendeten CDs und DVDs zentral freizugeben oder zu sperren. Gültigkeitszeitraum und Teilfreigaben ermöglichen die Organisation komplexer Softwareinstallationen über schmalbandige Anbindungen oder sogar ganz ohne Kommunikationsverbindung.

- Annahmen:
 - Anzahl Standorte: 100
 - Anzahl der verteilten Clients: 5000
- Vorgehen:
 - Ablösung der dezentralen SW-Verteilung durch CDWatch

Return on Investment (ROI)

- Nutzen (Kostenreduzierung) pro Jahr durch CDWatch

Senkung der Kommunikationskosten	124.000 €
Beschleunigung der TimetoUser	86.000 €
Reduzierung der Nachtarbeit	25.000 €
Wartungskosten	20.000 €
SUMME	215.000 €
Investitionskosten	190.000 €

D.h. der Rol im 1. Jahr ist schon größer als 100%!

D.h. die PP ist kleiner als 1 Jahr!

Problem: Ermittlung der Nutzenwerte!???



5. WIRTSCHAFTLICHKEITSANALYSE IM BEREICH IT-SICHERHEIT

5. Wirtschaftlichkeitsanalyse im Bereich IT-Sicherheit

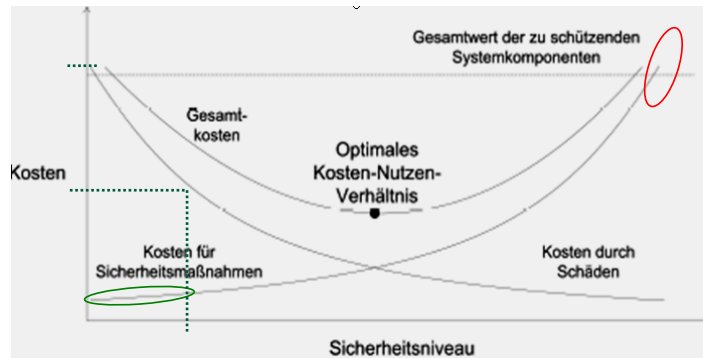


- Sicherheitsrisiken / Bedrohungen
 - Die Grundbedrohungen für IV-Systeme, denen begegnet werden muss, sind
 - der Verlust der Vertraulichkeit
 - der Verlust der Integrität
 - der Verlust der Verfügbarkeit
 - der Verlust der Authentizität
 - Ziel: Risikominderung durch Sicherheitsmaßnahmen, z.B.





■ IT-Sicherheitsinvestments



Quelle:
Hoppe/Prieß,
Herne/Berlin,
2003

- Nichtlineare Kostenfunktionen
- Deutlich mehr Sicherheit für wenig Kosten
- 100%ige Sicherheit bedeutet ∞ Kosten



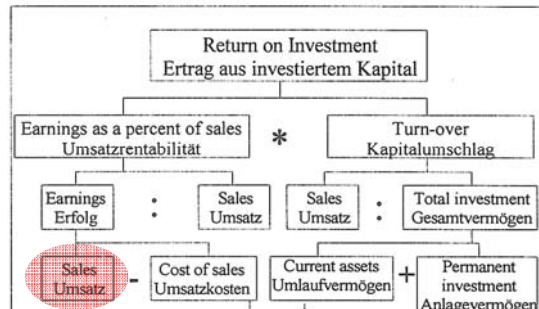
**Verwendungsmöglichkeiten einer Kosten-
Nutzenanalyse**

- Ex-ante-Betrachtung
 - Unterstützung bei der Entscheidung über eine IT-Sicherheitsinvestition mittels der Abwägung von Kosten und Nutzen
- Ex-post- Betrachtung
 - die getroffenen Entscheidungen hinsichtlich der Wirtschaftlichekeit überprüfen

ECOSEC 5. Return on Security Investment (ROSI)

Wann führt ein Sicherheitsinvestment unter Betrachtung aller Kosten zu einem ROI?

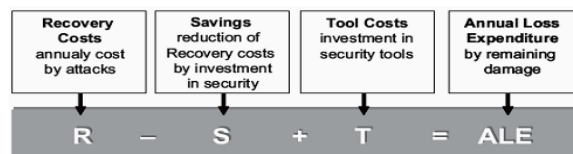
Eigentlich gar nicht!



ECOSEC 5. Return on Security Investment (ROSI)

▪ Ziel des **Return of Security Investment (ROSI)**: Darstellung des Nutzenaspekts von IV-Sicherheitsmaßnahmen mit Hilfe von Kennzahlen

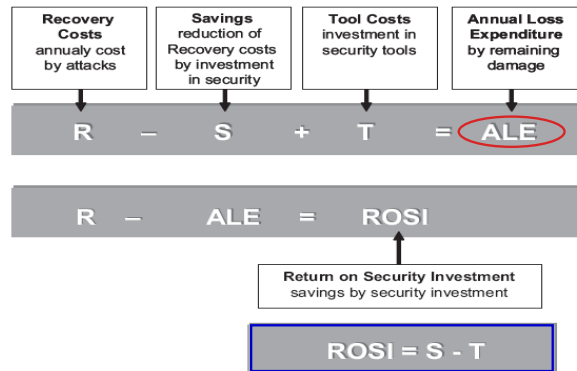
- **Recovery Costs**
 - Kosten zur Herstellung des ursprünglichen Zustands nach einem aufgetretenen Schaden (Kosten infolge Attacken)
- **Savings**
 - Reduzierung der R-Kosten durch Sicherheitsinvestments → Verringerung der Wahrscheinlichkeit eines erfolgreichen Angriffs
- **Tool Costs**
 - Kosten für Sicherheitsinvestments/-maßnahmen





▪ **Annual Loss Expenditure**

- jährliche Verlusterwartung aus verbleibenden Schäden



QUELLE: Pohlmann, N., Der IT-Sicherheitsleitfaden, Heidelberg 2004



Return of Security Investment (ROSI) – ein Beispiel

▪ Diebstahl oder Verlust von Notebooks in einem Unternehmen mit 500 Mitarbeitern

- **Recovery Costs – R:** (Zahlen aus verschiedenen Studien)
 - Anzahl gestohlener oder verlorengegangener Notebooks 6% pro Jahr = 30 Stück
 - Schaden durch den Verlust der gespeicherten Daten pro gestohlenem Notebook 10.000 €
 - Verlust der Hardware, Software und Wiederherstellung eines Ersatzgerätes 2.000 bis 3.000 € zusätzlich
- **Tool Costs – T:** Festplattenverschlüsselungsprodukt
 - Anschaffung kostet ca. 110 € pro Notebook ⇒ Einmalige Lizenzkosten: 500 * 110 € = 55.000 €
 - Kosten für Installation und Wartung im ersten Jahr 10.000 € und in den folgenden Jahren 5.000 €
- **Savings – S:**
 - 30 Notebooks * 10.000 € = 300.000 €

ECOSEC 5. Return on Security Investment (ROSI)

ROSI-Beispielrechnung für das erste Jahr:

R = 30 (3.000 € + 10.000 €) = 390.000 €
 S = 30 * 10.000 € = 300.000 €
 T = 55.000 € + 10.000 € = 65.000 €
 ALE = 155.000 €
 ROSI = 235.000 €

$$R - S + T = ALE$$

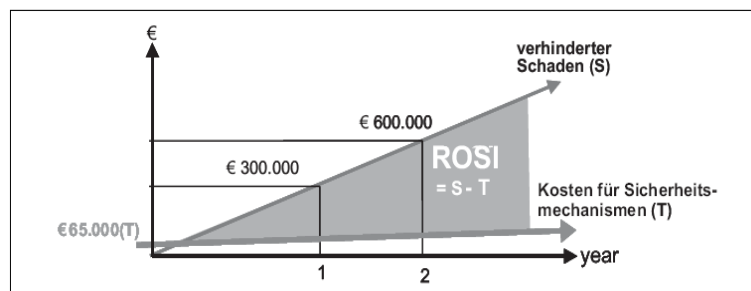
$$R - ALE = ROSI$$

$$ROSI = S - T$$

Calculation	1 st year	2 nd year	3 rd year	4 th year	In total
Time span	1 st year	2 nd year	3 rd year	4 th year	4 years
Initial costs	€ 55.000	--	--	--	€ 55.000
Implementation/ Roll-out, Admin	€ 10.000	€ 5.000	€ 5.000	€ 5.000	€ 25.000
Reduced costs??	--	--	--	--	--
Value of no losses from security breaches	€ 300.000	€ 300.000	€ 300.000	€ 300.000	€ 1.200.000
ROI 1 st year	€ 235.000				
ROI 2 nd year		€ 530.000			
ROI 3 rd year			€ 825.000		
ROI 4 th year				€ 1.1.20.000	€ 1.120.000

ECOSEC 5. Return on Security Investment (ROSI)

ROSI-Beispielrechnung



- **Achtung! Neues Risiko nicht berücksichtigt:**
 - Datenverlust aufgrund der Festplattenverschlüsselung

Hauptproblem: Mangel an empirische Daten, die möglichst über viele Unternehmen hinweg akkumuliert wurden

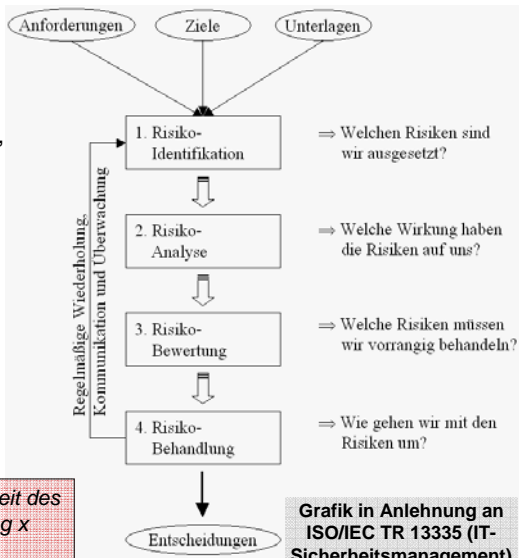
1. Abschätzung des Schadensausmaßes und der Reduzierung durch die Sicherheitsmaßnahme
 - Erfassung der Schäden schwierig, da sich erstmal niemand gern in die Karten schauen lässt (Imageverlust!?)
2. exakte Aussagen über Sicherheitsvorfälle und Häufigkeit von Schadensfällen
 - Unternehmensinterne Erfassung der Daten inzwischen durch Intrusion-Detection- und andere Monitoring-Systeme recht gut möglich

Weitere Probleme: Beurteilung des Zusammenhangs

- zwischen konkreten Angriff und speziellen Schaden
- zwischen Angriff und Wirkung einer Sicherheitsmaßnahme

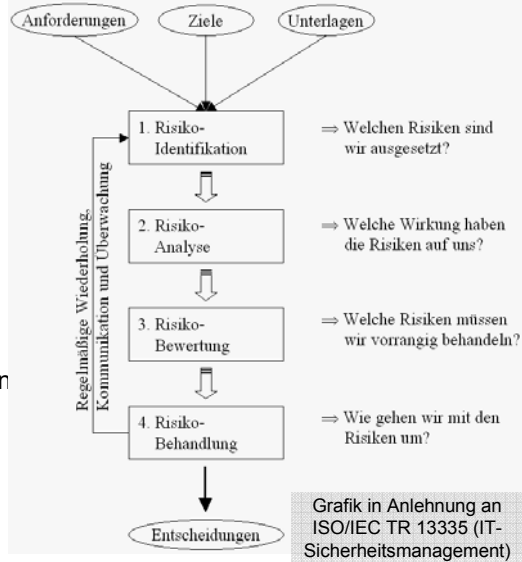
Risikomanagementprozess

- **Risikoidentifikation**
 - Bestimmung der zu schützenden **Werte (assets)**, die bestehenden **Bedrohungen (threats)** und die vorhandenen **Schwachstellen (vulnerabilities)**
- **Risikoanalyse**
 - Ursachen, Wirkungen und Abhängigkeiten feststellen.
 - Beispiel: Fehlermöglichkeits- und Einflussanalyse (FMEA)



Risikoprioritätszahl RPZ = Wahrscheinlichkeit des Schadenseintritts x Schadensauswirkung x Wahrscheinlichkeit der Entdeckung

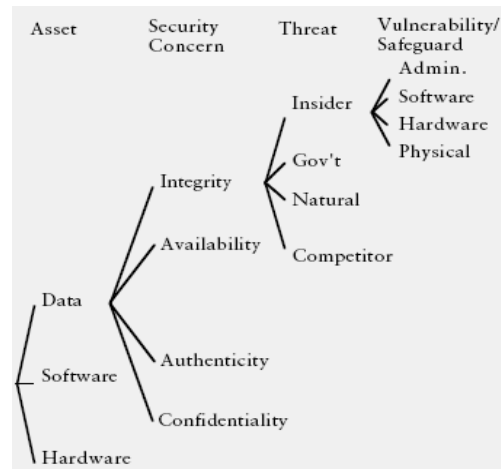
- Risikobewertung
 - Bewertung der relevanten Risiken, um Handlungsoptionen aufzuzeigen
 - Beispielverfahren: Risikotabellen, Risikomatrix, Risikoportfolio, SWOT-Analyse
- Risikobehandlung
 - Wie wird mit den Ergebnissen der vorangegangenen Schritte umgegangen?
 - Welche Maßnahmen sollen ergriffen werden?

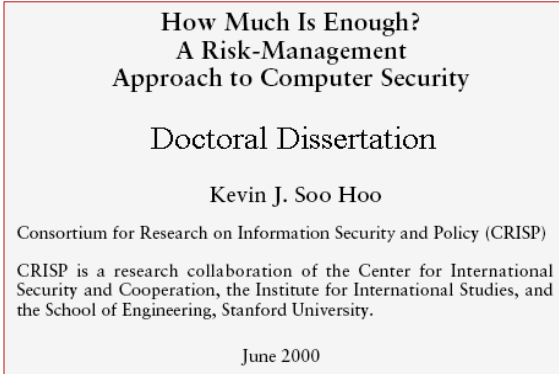


Grafik in Anlehnung an ISO/IEC TR 13335 (IT-Sicherheitsmanagement)

Probleme der klassischen Risikoanalyse

- Komplexität
- Arbeitsaufwand
 - Beispiel: $3 \cdot 4 \cdot 4 \cdot 4 = 192$ Szenarien
- Güte der Input-Daten

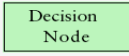
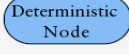
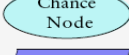

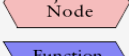
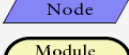
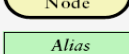
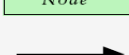
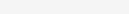




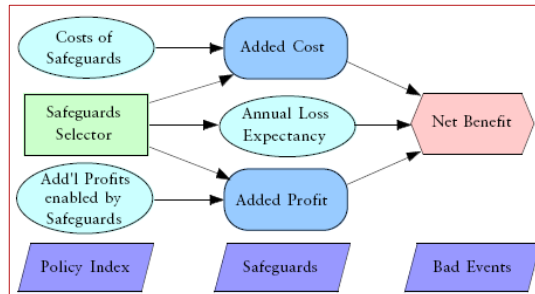
- Soo Hoo bedient sich der Technik der "Decision Analysis" verbunden mit einer Modellierungstechnik, die auf sogenannten "Influence Diagrams" basiert.

**Einfluss-
diagramme**

Legende

	Decision Node	Decision Nodes hold the various decision alternatives under consideration.
	Deterministic Node	Deterministic Nodes are used for deterministic input values as well as intermediate calculations.
	Chance Node	Chance Nodes are used to represent probabilistic input values.
	Index Node	Index Nodes contain lists that describe the various dimensions of the variables in the analysis.
	Objective Node	Objective Nodes represent significant results in the analysis where value assessments are done.
	Function Node	Function Nodes are generated when customized user functions are defined to facilitate calculations.
	Module Node	Module Nodes house diagrams of their own and are used to create hierarchical influence diagrams.
	Alias Node	Alias Nodes, in this case a decision node, are used to clarify influence in a diagram where the original node is located in a different module.
	Influence Arrows	Influence Arrows are used to graphically illustrate the flow of information through the model, i.e., the informational dependencies of model variables.

Einflussdiagramm (Decision diagram) -Begriffe

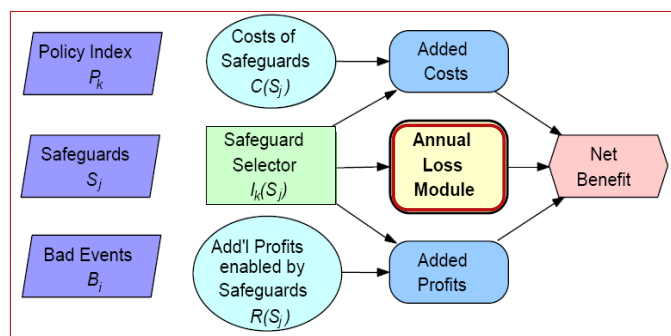


- Policy: Bündel von Sicherheitsmaßnahmen
- Safeguard: Sicherheitsmaßnahme
- Bad Events: Schadenskatalog
 - umfasst Informationsdiebstahl, Informationsmodifikation, Informationsvernichtung, Systemausfall, Diebstahl durch Beschäftigte, Schwächung der Systemleistung usw.
- Net benefit: Netto-Ertrag

Vergleich von verschiedenen Policys im Hinblick auf ihren Netto-Nutzen

1. Modellierungsschritt – Bestimmung der Parameter

Beispiel anhand eines hightech-orientierten Unternehmens mit 10.000 Beschäftigten und 500 Mio.\$ Jahresumsatz



5. ROSI-Ansatz von Kevin J. Soo Hoo

Costs of Safeguards $C(S_j)$

Safeguard Selector $I_k(S_j)$

Add'l Profits enabled by Safeguards $R(S_j)$

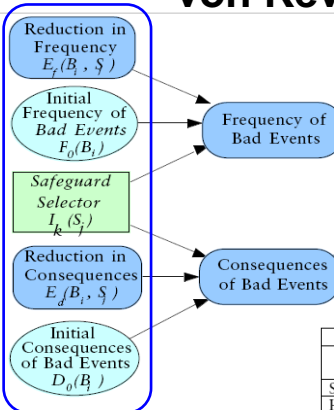
Input-Variablen

- Kosten der Sicherheitsmaßnahmen
- Mittels des Safeguard Selectors wird ausgewählt, welche Sicherheitsmaßnahmen in welches Bündel mit aufgenommen werden sollen.

Safeguard	Status Quo	Minor Improvement	Major Improvement	Maximum Improvement
Security Awareness	0	0	1	1
HW/SW Network Upgrade	0	1	1	1
Response Team	0	0	0	1
Nightly Back-ups	0	1	1	1
Encryption	0	0	1	1
Central Access Control	0	0	0	1
Firewalls	0	0	1	1
Screen Locking Software	0	1	1	1
Security Management Team	0	0	1	1
Comm Content Screening	0	0	0	1
Anti-Virus Software	0	1	1	1
Intrusion Detection System	0	0	0	1

Beispiel für den Safeguard Selector
0 → nicht angewendet 1 → angewendet

5. ROSI-Ansatz von Kevin J. Soo Hoo



ALE = Jahressumme der Schäden

Die zur Berechnung benötigten Daten (Schadensausmaß, Schadenshäufigkeit) werden aus

Vergangenheitsdaten oder durch Expertenurteile bestimmt.

Beispiel für eine Expertenbewertung der Reduktion der Schäden durch Sicherheitsmaßnahmen

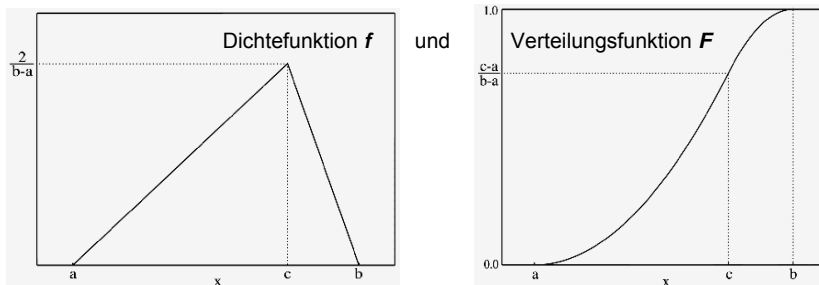
Table 5. Safeguard Reductions in Bad Event Consequences

	Info Theft	Info Mod.	Info Destr.	System Outage	Employee Theft	System Degrad.
Security Awareness	0	0	0	0	0	0
HW/SW Network Upgrade	0	0	0	0	0	0
Response Team	0	0.2	0.2	0.7	0	0.65
Nightly Back-ups	0	0.6	0.95	0	0	0
Encryption	0.95	0.95	0	0	0	0
Central Access Control	0	0	0	0	0	0
Firewalls	0	0	0	0	0	0
Screen Locking Software	0	0	0	0	0	0
Security Management Team	0	0	0	0	0	0
Comm Content Screening	0	0	0	0	0	0
Anti-Virus Software	0	0	0	0	0	0
Intrusion Detection System	0	0	0	0	0	0



Umgang mit der Unsicherheit der Daten

- Statistische Entscheidungstheorie / Entscheidungsanalyse
- Statt exakter Eingangsdaten eine **kontinuierliche Wahrscheinlichkeitsverteilung**
 - Beispiel: **Dreiecksverteilung** (a, b, c), einfache Alternative zur Normalverteilung (Gauß)



Ranking der Alternativen

- Werkzeug: Stochastische Dominanz (Porter, 1973)

Gegeben

$X \in [a, b]$ (Zufallsvariable)

Alternative 1: $A_1[X] = P_1[X \leq x] = \int_x^x f_1(\tau) d\tau$

Alternative 2: $A_2[X] = P_2[X \leq x] = \int_x^x f_2(\tau) d\tau$

First Degree Stochastic Dominance

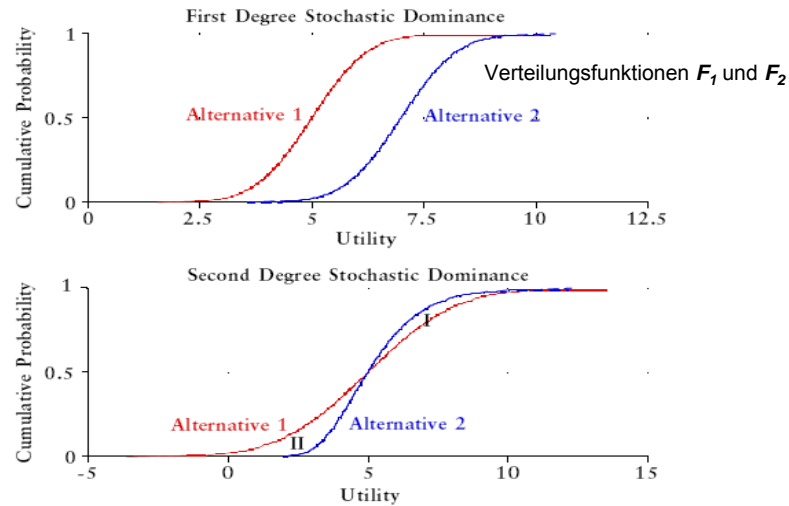
$A_2[X]$ dominiert $A_1[X]$ genau dann, wenn für alle X gilt: $A_2[X] \leq A_1[X]$ und für wenigstens ein X gilt: $A_2[X] < A_1[X]$

Second Degree Stochastic Dominance

$A_2[X]$ dominiert $A_1[X]$ genau dann, wenn für alle X gilt: $\int_x^x A_1(\tau) d\tau \leq \int_x^x A_2(\tau) d\tau$ und für

wenigstens ein X gilt: $\int_x^x A_1(\tau) d\tau < \int_x^x A_2(\tau) d\tau$

Stochastische Dominanz



Umgang mit der Unsicherheit der Daten

- Werte aus CSI/FBI-Studien von drei Vorjahren zur Schadenshäufigkeit → Dreiecksverteilung!

Bad Events	Annual Frequency Estimate
Information Theft	Triangular (0.18, 0.21, 0.25)
Information Modification	Triangular (0.40, 0.44, 0.55)
Information Destruction	Triangular (0.13, 0.10, 0.14)
System Outage	Uniform (0.25, 0.32)
Employee Theft	Triangular (0.12, 0.14, 0.15)
System Degradation	Triangular (0.83, 0.84, 0.90)

- Es bedeuten:

0,83 geringste berichtete Häufigkeit
0,84 mittlere berichtete Häufigkeit
0,90 höchste berichtete Häufigkeit

5. ROSI-Ansatz von Kevin J. Soo Hoo

Nun können die jährlichen Verlusterwartungen für jedes Maßnahmenbündel berechnet werden:

$$ALE_k \quad \forall k \in \{0,1,2,3\}$$

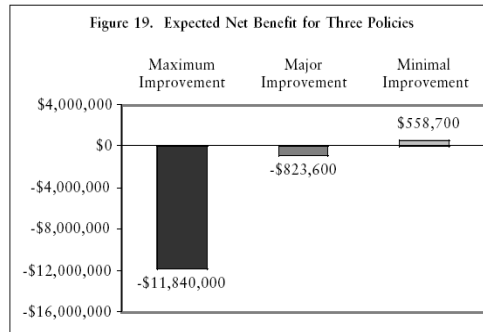
Anschließend kann der Nutzen für jedes Maßnahmenbündel durch den Vergleich mit dem Status Quo (ALE_0) berechnet werden.

$$\text{Nutzen}_k = ALE_0 - ALE_k$$

$$\text{Netto-Nutzen} = \text{Nutzen}_k - \text{zusätzliche Kosten}_k + \text{zusätzlicher Nutzen}_k$$

Aus dem Verhältnis zwischen Nutzen und Kosten ergibt sich dann

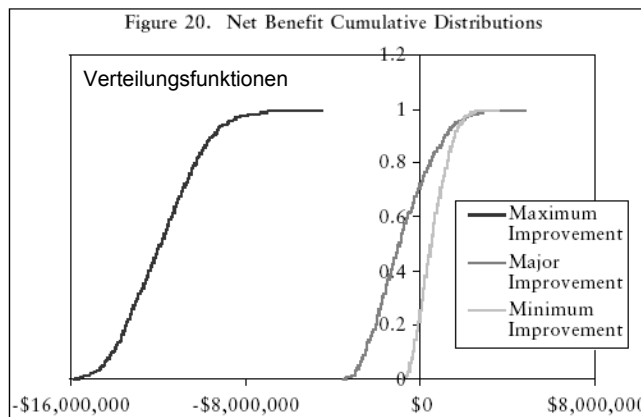
$$\text{ROSI} = \frac{\text{Netto-Nutzen}}{\text{Kosten der Sicherheitsmaßnahmen}}$$



Erwarteter Netto-Nutzen für die Maßnahmenkataloge

5. ROSI-Ansatz von Kevin J. Soo Hoo

- Eindeutige stochastische Dominanz der Alternative „minimales Sicherheitsbündel“





Bewertung des Ansatzes

- Modell ist rein quantitativ orientiert → ALE-Betrachtung
- Mit Hilfsmitteln der statistischen Entscheidungstheorie (Entscheidungsanalyse) wird geprüft, welche Alternative stochastisch dominant ist
- Die Schwierigkeit, geeignete Ausgangsdaten zu finden, wird durch die Integration von Wahrscheinlichkeitsverteilungen abgemildert, jedoch nicht beseitigt



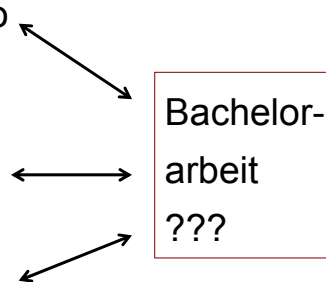
6. WEITERE SCHRITTE



1. Analyse des Modells von Gordon, Loeb (The Economics of Information Security Investment, ACM Transactions on Information and System Security, 5(4):438-457, November 2002)
 - (Auch) wahrscheinlichkeitstheoretischer Ansatz
 - Kombiniert mit Differentialkalkül
 - Sehr interessant, aber bislang ohne Anwendungsbeispiel



2. Vergleich der Modelle von Soo Hoo und Gordon/Loeb
 - **Prüfung der Anwendbarkeit**
3. Ggf. Entwicklung eines für die Anwendung optimierten Verfahrens
4. Entwicklung eines praxistauglichen Tools zur Berechnung des ROSI und/oder der optimalen Investitionshöhe / des optimalen Maßnahmenbündels





Vielen Dank für Ihre Aufmerksamkeit!
Die Folien können Sie jederzeit per E-Mail abrufen.

Prof. Dr. Rainer Rumpel
Berufsakademie
Fachbereich der FHW Berlin
Neue Bahnhofstrasse 13-15
10245 Berlin
Fon: +49 (0)30 29384-498
Fax: +49 (0)30 29384-406
EMail: rainer.rumpel@ba-berlin.de
<http://www.fhw-berlin.de/berufsakademie>