
SBA
Research

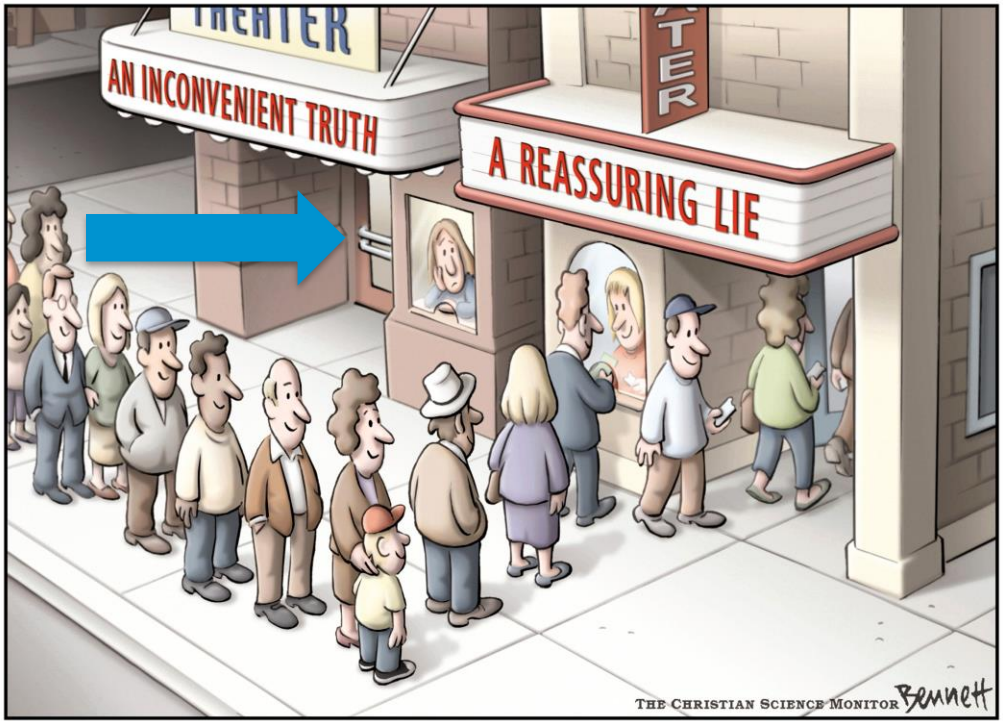
COMET

Competence Centers for
Excellent Technologies

Risikowahrnehmung und menschliche (Ir)Rationalität

Fallstricke im „Cyber“-Risikomanagement

Die unbequeme Wahrheit oder die beruhigende Lüge?



https://en.wikipedia.org/wiki/Red_pill_and_blue_pill
http://new-universe.org/zenphoto/Chapter5/Illustrations/Abrams56.jpg.php

Risikomanagement in der „Cyber“ Security

Artikel 14

Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen

(1) Die Mitgliedstaaten stellen sicher, dass die Betreiber wesentlicher Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.

Artikel 32

Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

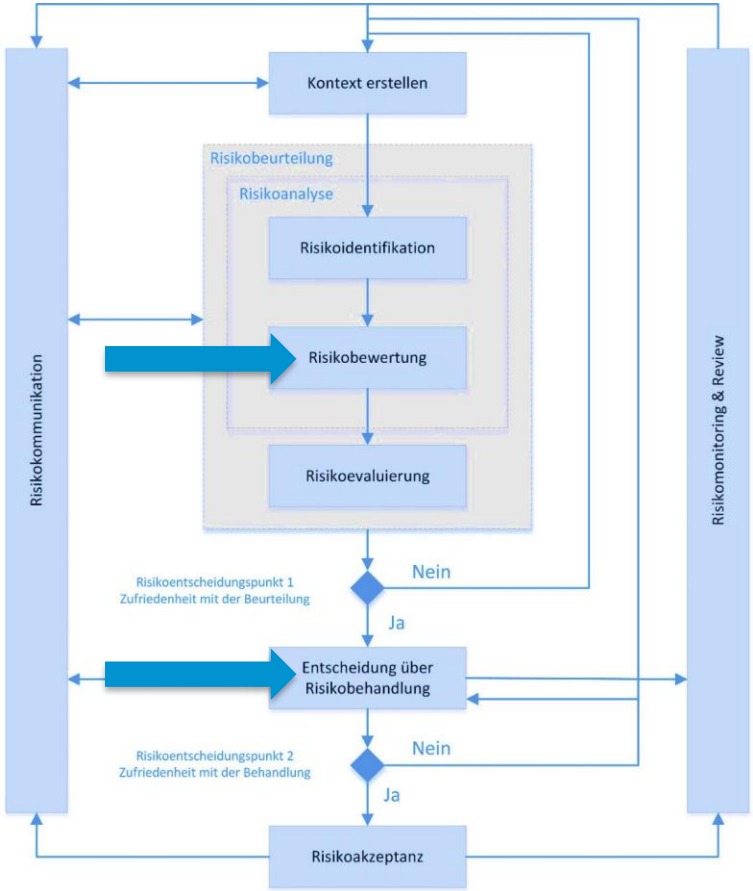
- **ISO/IEC 27001:2014**
  - „... ist der Teil des gesamten Managementsystems, der **auf der Basis eines Geschäftsrisikoansatzes** die Errichtung, die Umsetzung, d
    Überwachung, die Überprüfung, die Instandhaltung und di
    Informationssicherheit abdeckt.“

OWASP Risk Rating Methodology

Author: Jeff Williams

Discovering vulnerabilities is important, but being able to estimate the associated risk to the business is just as important. Early in the life cycle, one may identify security concerns in the architecture or design by using threat modeling. Later, one may find security issues using code review or penetration testing. Or problems may not be discovered until the application is in production and is actually compromised.

Risikomanagement Standards und Empfehlungen



ISO 27005/ ISO 31000

Risikomanagement – Grundvoraussetzungen

I. Risikobehandlung:

Wir **müssen** wenn Auswirkung und Eintrittswahrscheinlichkeit gegeben sind **vernünftige (und konsistente) Entscheidungen treffen** können

II. Risikobewertung:

Wir **müssen** die potentiellen Auswirkungen und Eintritts-wahrscheinlichkeiten von **Risiken richtig einschätzen** können

→ **Können wir das?**

Problem der asiatische Krankheit – Fall I

- Eine Stadt steht vor dem Ausbruch einer ungewöhnlichen asiatischen Krankheit, von der **erwartet wird, dass 600 Personen daran sterben werden**.
- Es wurden **zwei verschiedene Pläne vorgeschlagen**, die Krankheit zu bekämpfen.

Plan A	Plan B
200 Personen gerettet	Wahrscheinlichkeit von einem Drittel **(1/3),** dass **600 Personen gerettet** werden, und eine Wahrscheinlichkeit von zwei Dritteln **(2/3), dass niemand gerettet** wird

Problem der asiatische Krankheit – Fall II

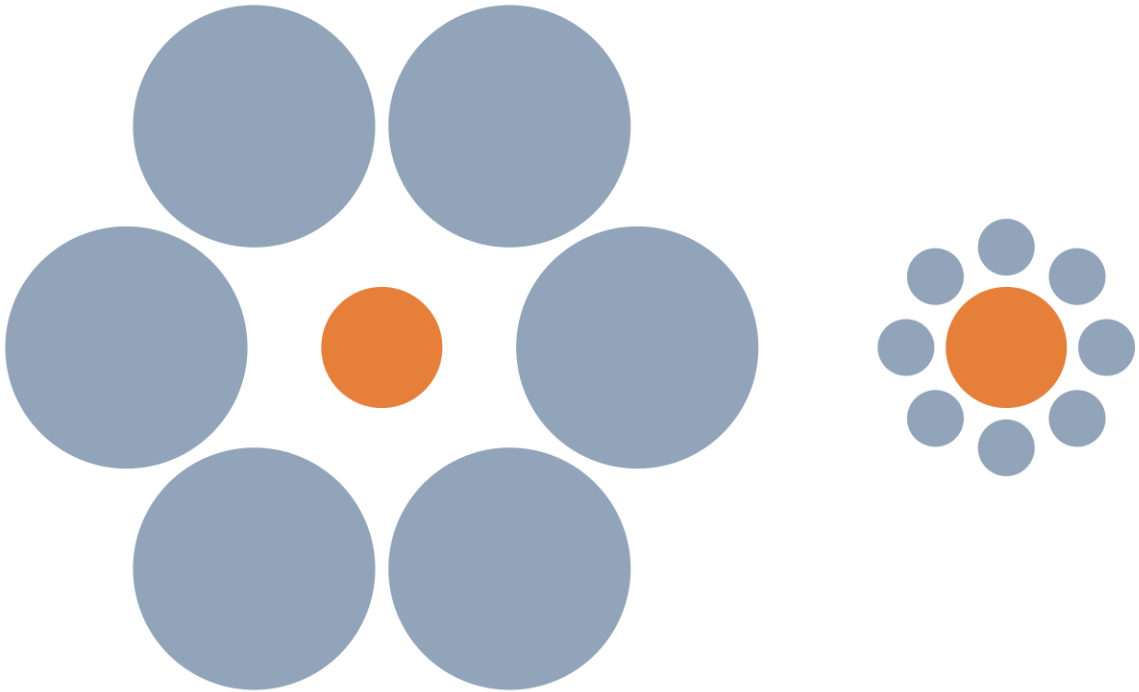
- Eine Stadt steht vor dem Ausbruch einer ungewöhnlichen asiatischen Krankheit, von der **erwartet wird, dass 600 Personen daran sterben werden**.
- Es wurden **zwei verschiedene Pläne vorgeschlagen**, die Krankheit zu bekämpfen.

Plan C	Plan D
400 Personen sterben	Wahrscheinlichkeit von einem Drittel **(1/3), dass niemand sterben wird**, und eine Wahrscheinlichkeit von zwei Dritteln **(2/3), dass 600 Menschen sterben**

Problem der asiatische Krankheit – Fazit

- **Fall I**: 72 % der Versuchspersonen wählten den **Plan A**, der 200 Menschen sicher rettet
- **Fall II**: 78 % der Versuchspersonen wählten den **Plan D** bei dem mit einer Wahrscheinlichkeit von (1/3) niemand sterben und von 2/3 alle sterben werden
- **Pläne A und C** und die **Pläne B und D** sind offensichtlich **identisch**. Ihre respektiven **Folgen wurden nur anders dargestellt**
  - bei den Plänen A und B als «Gewinne» und bei den Plänen C und D als «Verluste»
  - **Darstellung (*framing*) der Alternativen** als Gewinne oder Verluste hat einen **maßgeblichen Einfluss auf das Risikoverhalten** (siehe Kahneman und Tversky, Prospect Theory)

Problem der asiatische Krankheit – Fazit



https://de.wikipedia.org/wiki/Mondt%C3%A4uschung

Vorsorgeuntersuchungen I

- Test wird durchgeführt
  - **Sensitivität**:
    Wenn Patient krank → **Krankheit** wird mit **90%** Wahrscheinlichkeit **erkannt** (Test positiv)
  - **Spezifizität**:
    Wenn Patient gesund → **Gesundheit** wird mit **93%** Wahrscheinlichkeit **erkannt** (Test negativ)
  - **Prävalenz** (Häufigkeit des Auftretens der Krankheit):
    0,8% der Bevölkerung **krank**

Mein Test ist Positiv...

... und nun .?

https://www.pngegg.com/en/png-bnsoot unf https://rochesterlawcenter.com/services/last-will-testament-michigan/

Vorsorgeuntersuchungen II

- Mein Test ist positiv → Bin ich jetzt krank?

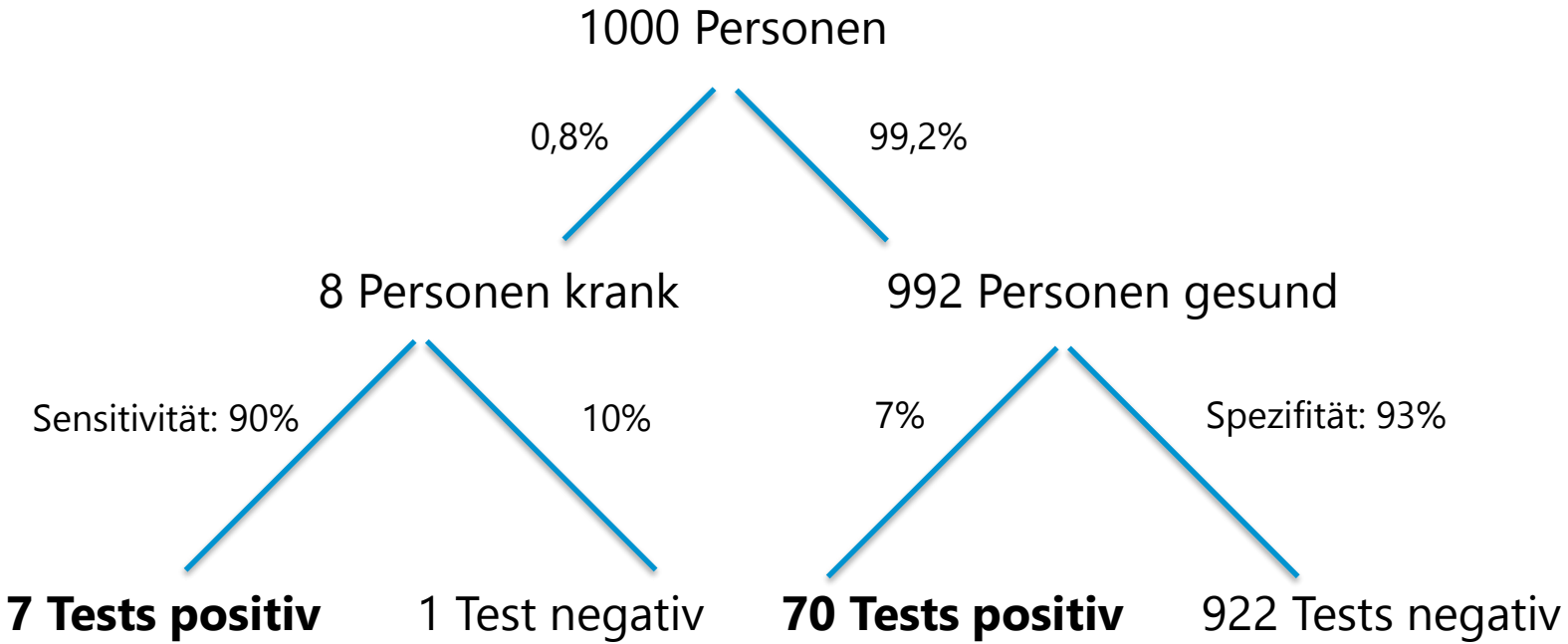
Sicher nicht (0%)	Sehr Unwahr-scheinlich (<10%)	Unwahr-scheinlich (10-50%)	Wahr-scheinlich (50-80%)	Sehr Wahr-scheinlich (>90%)	Absolut sicher (100%)

- Einschätzung von 24 Ärzten

Sicher nicht (0%)	Sehr Unwahr-scheinlich (<10%)	Unwahr-scheinlich (10-50%)	Wahr-scheinlich (50-80%)	Sehr Wahr-scheinlich (>90%)	Absolut sicher (100%)
4	4	1	7	8	0

62,5% glauben Wahrscheinlichkeit für Krankheit ist >=50%

Vorsorgeuntersuchungen III



Wahrscheinlichkeit für Krankheit bei einem positiven Test $= \frac{7}{7+70} =$ **9%**

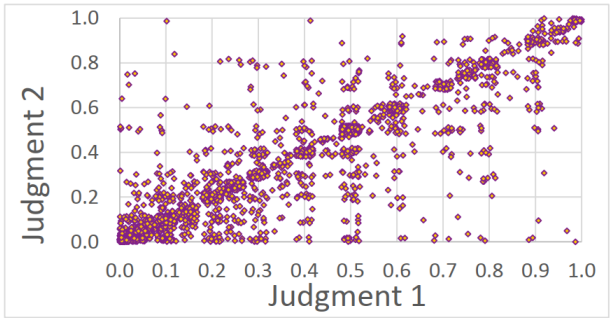
Inkonsistente Antworten bei gleichen Informationen

Inconsistency Measurement Results

#RSAC

- We have gathered estimates of probabilities of various security events from:
  - 48 experts from 4 different industries.
  - Each expert was given descriptive data for over 100 systems.
  - For each system each expert estimated probabilities of six or more different types of security events.
- Total: Over 30,000 individual estimates of probabilities
- These estimates included over 2,000 duplicate scenarios pairs.

Comparison of 1st to 2nd Estimates of Cyber risk judgements by same SME



21% of variation in expert responses are explained by *inconsistency.*

79% are explained by actual information given

Hubbard Decision Research

22

RSAConference2016

https://www.rsaconference.com/writable/presentations/file_upload/grc-w05-how_to_measure_anything_in_cybersecurity_risk.pdf

Risikomanagement – Grundvoraussetzungen

I. Risikobehandlung:

Wir **müssen** wenn Auswirkung und Eintrittswahrscheinlichkeit gegeben sind **vernünftige (und konsistente) Entscheidungen treffen** können

Können wir nur sehr bedingt

II. Risikobewertung:

Wir **müssen** die potentiellen Auswirkungen und Eintritts-wahrscheinlichkeiten von **Risiken richtig einschätzen** können

→ **Können wir das?**

Zwischenfazit

Wenn wir schon **selbst wenn alle Parameter,** Rahmenbedingungen, Zahlen und Konsequenzen sowie Wahrscheinlichkeiten **bekannt** sind

- **Nicht durchgängig** logische, **rationale und konsistente Entscheidungen** treffen können …

…wie schaut das dann erst in der **realen Welt** aus, in der **viele Risiken durch starke Ungewissheit und Unschärfe charakterisiert sind?**

- Menschen nutzen **Urteilsheuristiken** (Faustregeln), um Sachverhalte auch dann beurteilen zu können, wenn kein Zugang zu präzisen und vollständigen Informationen besteht.
- Hierbei wird meist unbewusst eine **komplexe Fragestellung durch eine einfacher zu beantwortende Fragestellung ersetzt**

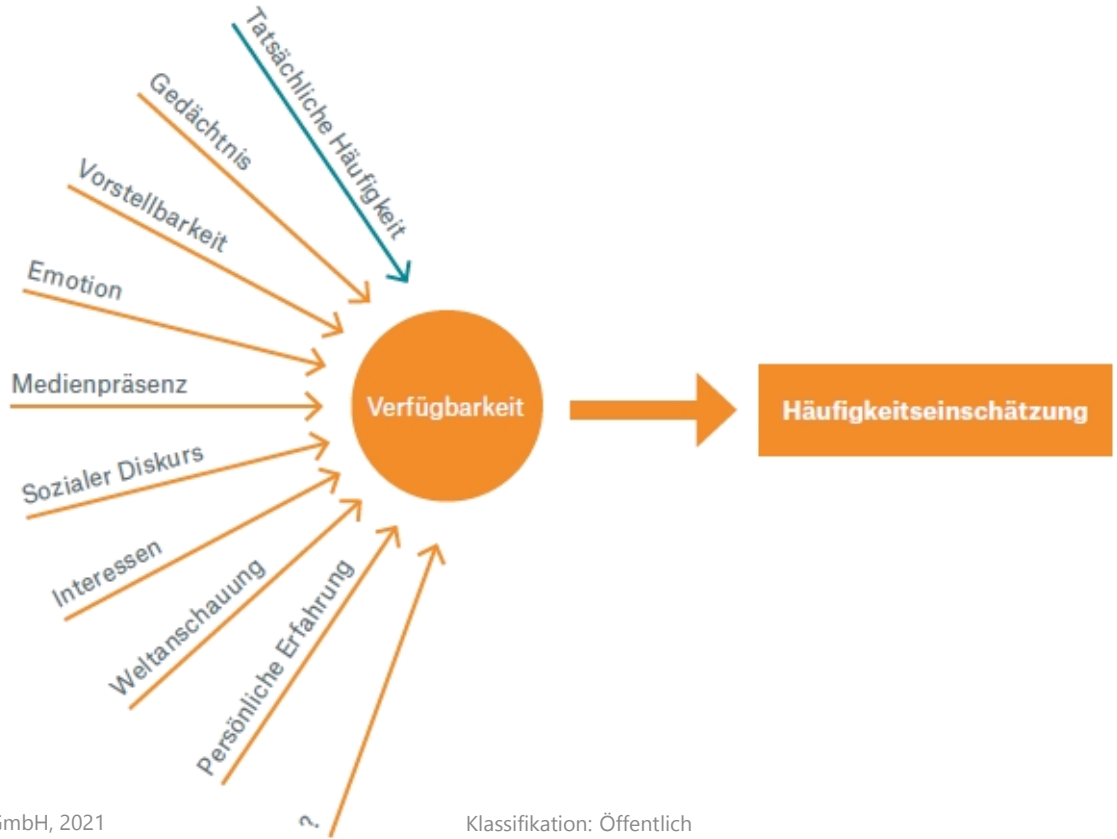
Verfügbarkeitsheuristik/Availability Bias

- **Oft unbewusst, eingesetzt**, wenn die **Häufigkeit bzw. Wahrscheinlichkeit** eines **Ereignisses beurteilt** werden soll, aber gleichzeitig die Zeit, Möglichkeit oder Wille fehlt, um auf präzise (z. B. statistische) Daten zurückzugreifen.

- In solchen Fällen wird das Urteil stattdessen **davon beeinflusst, wie verfügbar** (leichter greifbar / besser vorstellbar) **dieses Ereignis** oder Beispiele ähnlicher Ereignisse **im Gedächtnis sind.**
  - Ereignisse, an die wir uns sehr **leicht erinnern** (bzw. besser vorstellen können)**, scheinen uns daher wahrscheinlicher** zu sein als Ereignisse, an die wir uns nur schwer erinnern können.

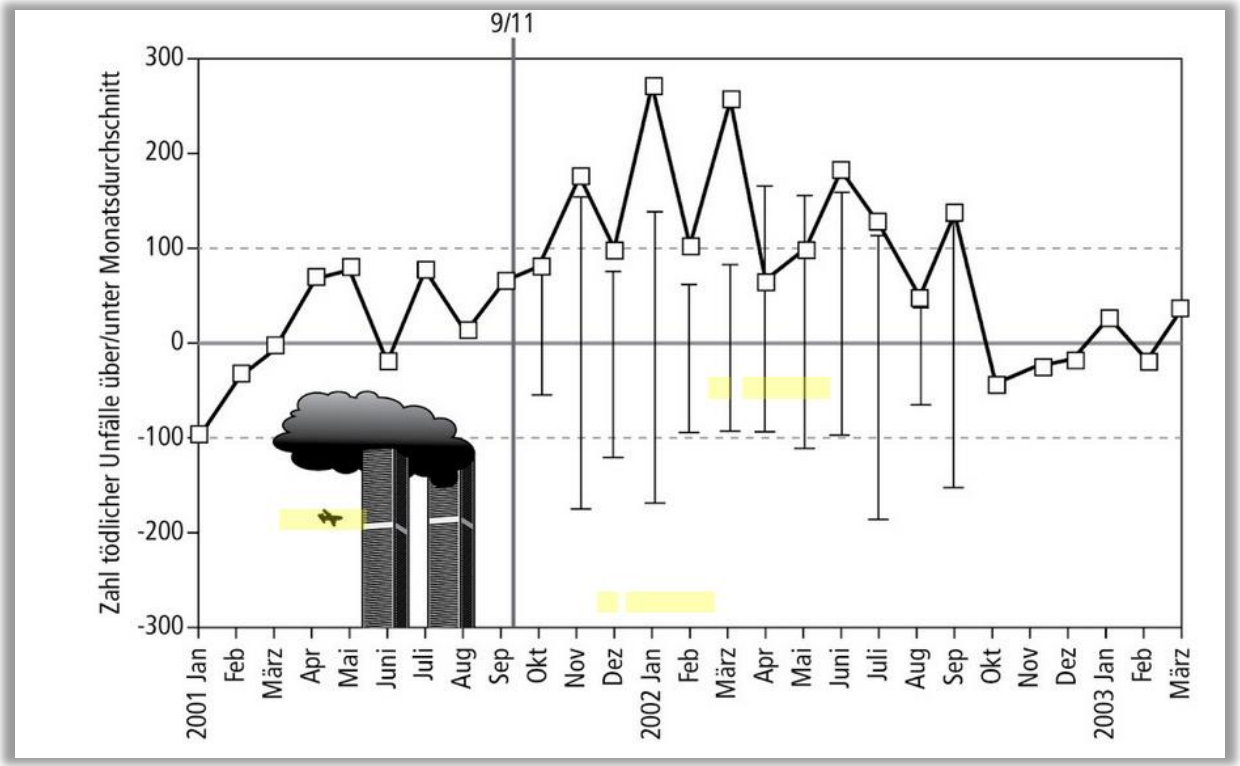
https://de.wikipedia.org/wiki/Verf%C3%BCgbarkeitsheuristik

Verfügbarkeitsheuristik/Availability Bias



https://www.risknet.de/themen/risknews/psychologische-einfluesse-auf-die-individuelle-einschaetzung-von-risiken/26702eab53afbc939ebeeb09752a4d8d/

Straßenverkehrstote nach 9/11



Risiko, Gerd Gigarenzer

Anker Effekt

- Menschen lassen sich bei Schätzungen **von Umgebungsinformationen beeinflussen**, ohne dass ihnen dieser Einfluss bewusst wird.
  - Die Umgebungsinformationen haben **Einfluss selbst dann, wenn sie für die Entscheidung eigentlich irrelevant sind.**

- Die Entscheidung orientiert sich an einem **willkürlichen Anker** → Folge ist eine **systematische Verzerrung in Richtung des Ankers**.

Anker Effekt

- Auch Experten sind davor nicht gefeit:
  - …Birte Englich und Thomas Mussweiler konnten zeigen, dass der **Urteilsspruch von Richtern**, die alle mehr als 15 Jahre Berufserfahrung hatten, sich **signifikant an der willkürlichen Empfehlung eines Laien** (Informatikstudent im ersten Semester) oder **sogar an einer (mit gezinkten Würfeln ermittelten) Zufallszahl orientierte**.
    Die Stärke des Ankereffektes beim Würfeln war 50 %.

- Warum sollten Sicherheitsexperten beim Bewerten (der Auswirkungen) von Risiken nicht den gleichen Verzerrungen unterliegen?

https://de.wikipedia.org/wiki/Ankereffekt#Auch_Experten_unterliegen_dem_Ankereffekt

Wovor fürchten wir uns und welche Risiken über- bzw. unterschätzen wir?

People exaggerate risks that are:	People downplay risks that are:
Spectacular	Pedestrian
Rare	Common
Personified	Anonymous
Beyond their control, or externally imposed	More under their control, or taken willingly
Talked about	Not discussed
Intentional or man-made	Natural
Immediate	Long-term or diffuse
Sudden	Evolving slowly over time
Affecting them personally	Affecting others
New and unfamiliar	Familiar
Uncertain	Well understood
Directed against their children	Directed towards themselves
Morally offensive	Morally desirable
Entirely without redeeming features	Associated with some ancillary benefit
Not like their current situation	Like their current situation

Table 1. Conventional Wisdom About People and Risk Perception

https://www.schneier.com/academic/paperfiles/paper-psychology-of-security.pdf

Risikomanagement – Grundvoraussetzungen

I. Risikobehandlung:

Wir **müssen** wenn Auswirkung und Eintrittswahrscheinlichkeit gegeben sind **vernünftige (und konsistente) Entscheidungen treffen** können

Können wir nur sehr bedingt

II. Risikobewertung:

Wir **müssen** die potentiellen Auswirkungen und Eintritts-wahrscheinlichkeiten von **Risiken richtig einschätzen** können

Können wir nur sehr bedingt

→ **Können wir das?**

Fazit

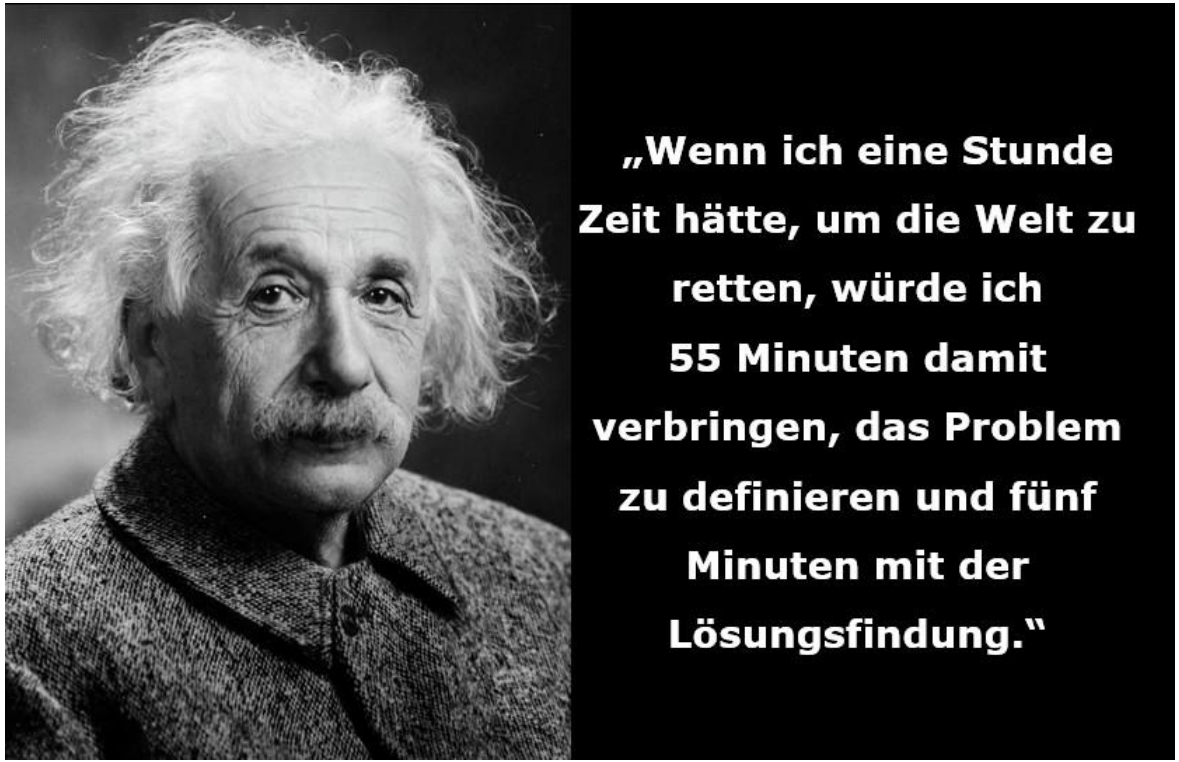
Risikomanagement spielt eine **essentielle Rolle in der „Cyber" Security**

- In verschiedensten Gesetzen, Regularien und Standards gefordert bzw. empfohlen
- Wichtig für **Priorisierung und Fokussierung** des eigenen **Sicherheitsengagements**
- Aber: Forschung und **Erfahrungen aus anderen Disziplinen zu menschlicher (Ir)Rationalität** und Problemen bei der Risikobewertung **zu wenig berücksichtigt**

Menschlicher **Umgang mit Risiken** ist **oft nicht rational und objektiv**

- Menschen lassen sich (oft) durch **Emotionen und Bauchgefühl bzw. Heuristiken** lenken
- **Schwierig valide und konsistente Entscheidungen** zu treffen
- Wichtig sich der „**Begrenztheit & Limitierungen" des eigenen Verstandes** bewusst zu sein
- Sehr spannendes und aktives Forschungsfeld (u.a. Verhaltensökonomie, Psychologie)

… und nun?



https://www.saurugg.net/wp-content/uploads/2018/08/einstein-zeit.jpg

Ideen und Vorschläge I
Zur Verbesserung der Risikomanagement Methodologie

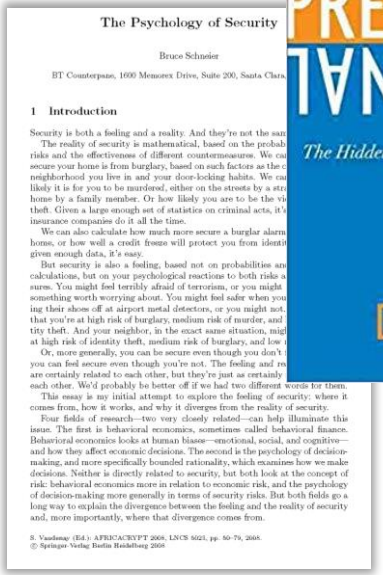
- **Kalibrierung** von Experten
  - Lernen Confidence und eigene Unsicherheit/Ungewissheit richtig einzuschätzen
- Eigene **Unsicherheit/Ungewissheit angeben**
  - Keine single point estimates (23%) sondern eher Bereiche (15%-35%) in denen der tatsächliche Wert mit einer gewissen Konfidenz (e.g. 90% Intervall) liegt
  - Konfidenzintervall bei Schätzung angeben („Wie sicher bin ich dass es richtig ist?“, siehe auch Auswertung Cyber Riskomatrix 2017 mittels Box Plots)
- **Messung der Validität/Erfolg** der eigenen Risiko Analysen (bzw. der eigenen Vorhersagen, Taleb in „Skin in the game“)
  - Vergleich der Einschätzungen mit historischen Daten („**Retrospektive Risiko Analyse**“)
- **Quantitative Methoden** + Modelle wie FAIR etc.
  - Diese sind stabiler gegen subjektive Schwankungen, siehe auch Gigrarenzer Bauchgefühl
- **Multiple <u>independent</u> estimates by multiple (independent) experts** (maybe even from different fields)
  - Calculate average → leverage wisdom of the crowd and mitigate consensus/group think problems

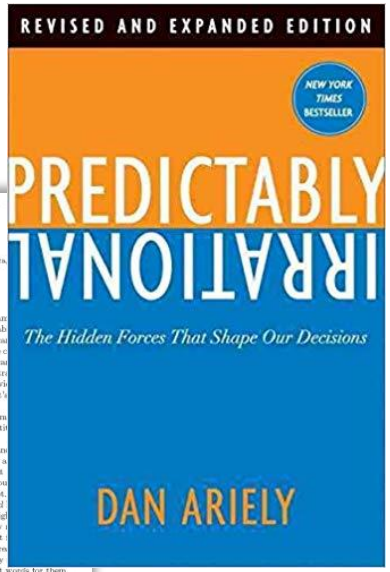
Ideen und Vorschläge II
Zur Verbesserung der Risikomanagement Methodologie

- **Prä Mortem Analyse** [1)]
- **BIA und BCM** → nicht versuchen die Wahrscheinlichkeit zu bewerten weil Auswirkung meist viel greifbarer
  - **Manche Risiken müssen mitigiert werden, egal wie unwahrscheinlich sie sind/scheinen** (Taleb)
- Idee Robust Contol System Networks
  - **Fokus auf Fragilität und nicht auf Risiko** → Die Fragilität eines Systems/Landschaft lässt sich besser feststellen/beobachte
- **Advocatus Diaboli**/Devil's Advocay
  - genutzt um der voreingenommenen Informationssuche im Rahmen von Urteils- und Entscheidungsprozessen in Gruppen entgegenzuwirken
  - zufällig ausgewähltes Gruppenmitglied die Rolle des Advocatus Diaboli dessen Aufgabe es ist, Vorschläge der Gruppe zu kritisieren und Schwachstellen zu finden
- **Prediction Markets**
  - virtuelle Marktplattformen, die den Ausgang von Ereignissen vorhersagen sollen. Existieren in Form von Online-Wettbörsen oder virtuellen Wertpapiermärkten

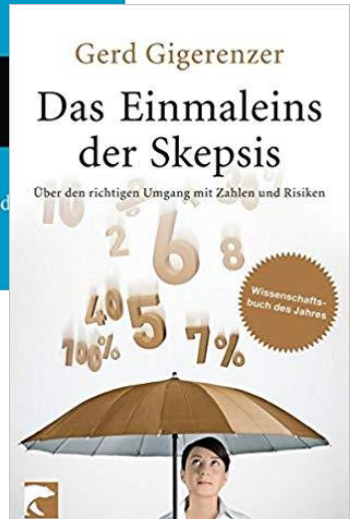
[1)] https://hbr.org/2007/09/performing-a-project-premortem (Gary Klein, der Erfinder der Technik), https://komfortzonen.de/workshop-tools-pre-mortem/
https://www.youtube.com/watch?v=MzTNMalfyhM (sehr gute Erklärung von Daniel Kahnemann zur Pre-Mortem-Analyse)

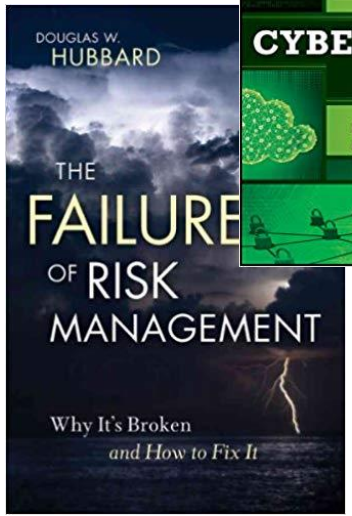
Literatur I
Fokus Psychologie sowie Urteils- und Entscheidungsfindung

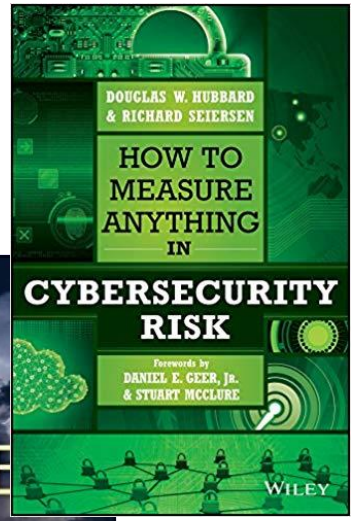




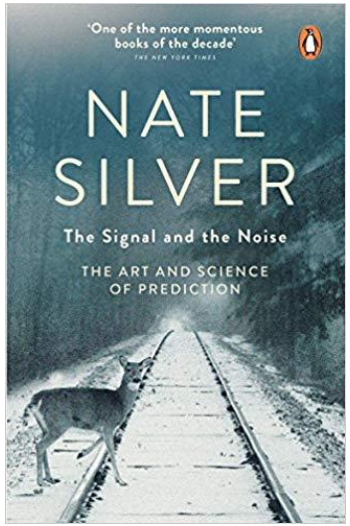
Literatur II
Fokus Risikowahrnehmung und Risikomanagement

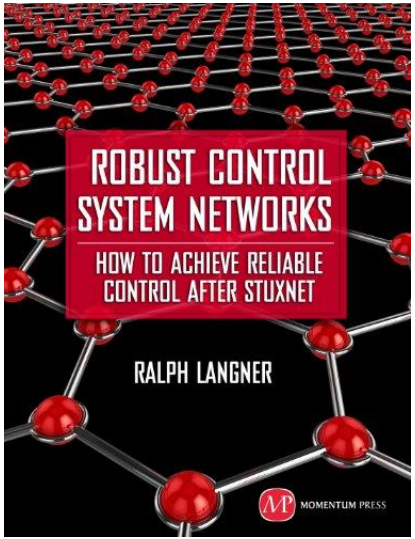


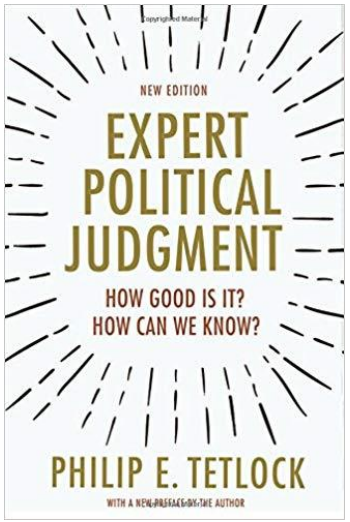




Literatur III
Fokus Heuristiken und Vorhersagefähigkeit







Competence Centers for
Excellent Technologies

Philipp Reisinger

SBA Research gGmbH

Favoritenstraße 16, 1040 Wien

+43 660 543 62 74

Preisinger@sba-research.org