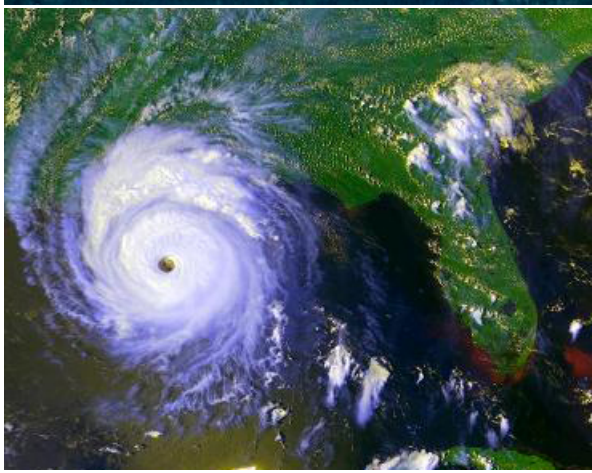
Risk Analysis

Security Engineering

David Basin
ETH Zurich

Motivation

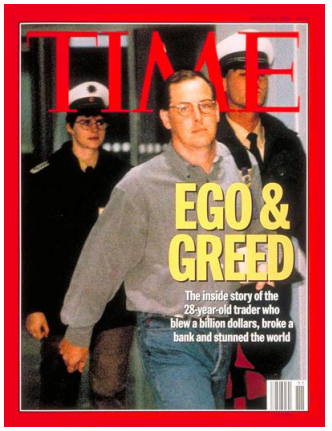
- **Bad things happen!**
  - Hurricanes, floods, wars
  - Projects don't meet objectives and deadlines
  - Bad guys break into IT systems
- What exactly are the bad things?
- How can they happen?
- How bad are they?
- How can I protect myself?
  - Decrease chances that bad thing happens
  - Mitigate the consequences
- Can I measure any of this?



Risk management scope

- Protect "the organization" and its ability to perform its mission.
  - This is an essential management function!
- Carried out at the level of
  - Enterprises: health care providers, insurances, ...
  - Administrations
  - Project teams
  - ...
- Different perspectives
  - Focus on mission
  - Focus on assets
  - Focus on IT

Example: Basel II accord



- Goal: adequate mandatory capitalization of banks

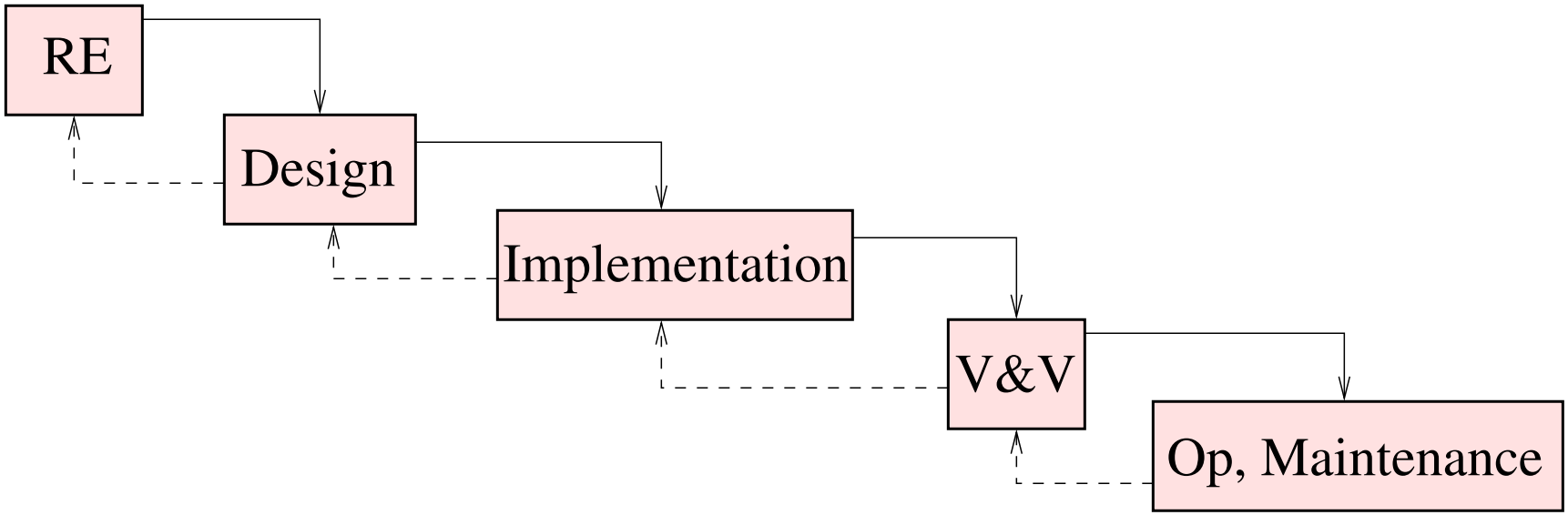
  $\Rightarrow$ improved risk management: credit risk, market risk, etc.

- ... explicit capital charge for operational risk
  - "The risk of losses resulting from inadequate or failed internal processes, people and systems, or from external events"
  - Growing number of operational loss events
    E.g. 1995 Nick Leeson/Barings Bank \$1.3 billion; 2001 Enron; \$2.3 billion, Kweku Adoboli, UBS 2011

- 7 level-1 loss types

  Internal/external fraud, damage to physical assets, business disruption & system failures, ...

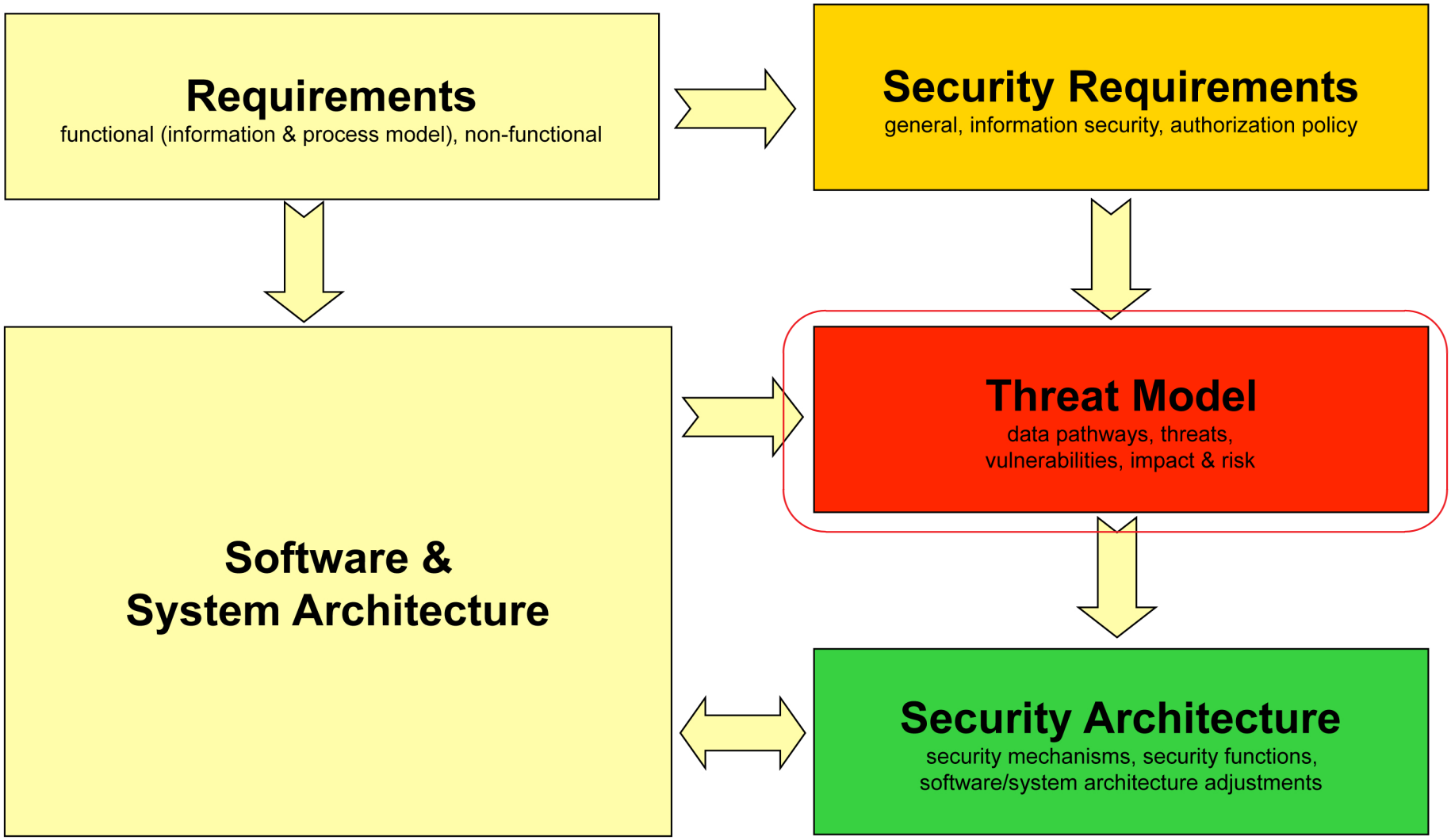
Where are we in waterfall?



Risk analysis is relevant for all phases

- Receives input from all phases
- Provides output to all phases
- Iterative activity

Security context



Aim of risk module

- Understand the notions of threat, vulnerability, and risk
- Understand there are different perspectives on risk
- See the need for cost-benefit analyses
- Get an idea of qualitative and quantitative risk assessments
- Understand the problems with using probabilities for risk analysis
- See the relationships to other development phases
- See how models can support this process

Road map

☞ **Motivation and goals**

- Assets, threats, vulnerabilities
- Risk
- Qualitative and quantitative risk analysis and management
- Example

IT risk management

- Enable mission success through more secure IT systems

  Management takes informed decisions based on objective evidence

- Key ideas and activities
  - identify the most probable **threats** to an enterprise
  - understand the related **vulnerabilities**
  - relate these to enterprise **assets** and their **valuation**
  - determine **risks** and suitable **countermeasures**

We focus on overall risk analysis process in this talk.
Threats and vulnerabilities are focus of a separate module.

Information security objectives (risk analysis perspective)

1. Maintain customer, stockholder, and taxpayer confidence in organization
2. Protect confidentiality and integrity of sensitive data
3. Avoid third party liability for illegal or malicious acts committed with the organization's systems
4. Ensure that organization's computer, network, and data are not misused
5. Avoid fraud
6. Avoid expensive and disruptive incidents
7. Comply with pertinent laws and regulations

Which criteria will Chief Security Officer be evaluated on at year end?
How do these differ from traditional security objectives?

It's all about balance

- Balancing functional requirements, usability, costs, risks

  Don't spend $1,000 for a firewall to protect $100 worth of data

- Differentiating relevant risks with theoretical ones
  - Cryptanalysis of ciphers vs. dictionary attacks on passwords
  - This requires a **proper threat analysis**, i.e., adversarial model

- Understanding the impact of different kinds of attacks

  Seizing a password database is significantly higher impact than tapping a single user's password.

- You have to get the numbers right!

  This requires careful analysis rather than reactive measures

Road map

- Motivation and goals

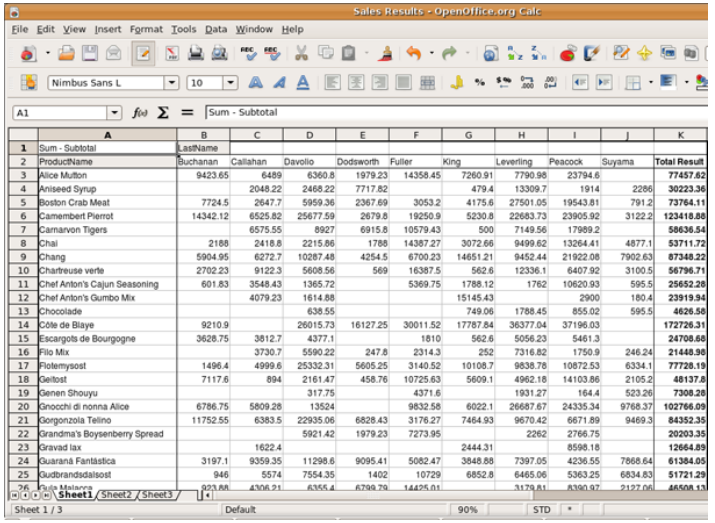
☞ **Assets, threats, vulnerabilities, countermeasures**

- Risk
- Qualitative and quantitative risk analysis and management
- Example

Assets

- Things of value to a company
  - Information: data or intellectual property
  - Products
  - Buildings
  - Systems: hardware and software
  - People
  - Reputation
  - Trust of business partners
  - Potential political fallout
- Tangible (physical like hardware or logical like software) and intangible
- Value sometimes difficult to estimate

Example: value of information



Sum - Subtotal	LastName									
ProductName	Buchanan	Callahan	Davolio	Dodsworth	Fuller	King	Leverling	Peacock	Suyama	Total Result
Alice Mutton	9423.65	6489	6360.8	1979.23	14358.45	7260.91	7790.98	23794.6		77457.62
Aniseed Syrup		2048.22	2468.22	7717.82		479.4	13309.7	1914	2286	30223.36
Boston Crab Meat	7724.5	2647.7	5959.36	2367.69	3053.2	4175.6	27501.05	19543.81	791.2	73764.11
Camembert Pierrot	14342.12	6525.82	25677.59	2679.8	19250.9	5230.8	22683.73	23905.92	3122.2	123418.86
Carnarvon Tigers		6575.55	8927	6915.8	10579.43	500	7149.56	17989.2		58636.54
Chai	2188	2418.6	2215.88	1788	14387.27	3072.66	9499.62	13264.41	4877.1	53711.72
Chang	5904.95	6272.7	10287.48	4254.5	6700.23	14651.21	9452.44	21922.08	7902.63	87348.22
Chartreuse verte	2702.23	9122.3	5608.56	569	16387.5	562.6	12336.1	6407.92	3100.5	56796.71
Chef Anton's Cajun Seasoning	601.83	3548.43	1365.72		5369.75	1788.12	1762	10620.93	595.5	25652.28
Chef Anton's Gumbo Mix		4079.23	1614.88			15145.43		2900	180.4	23919.94
Chocolade			638.55			749.06	1788.45	855.02	595.5	4626.58
Côte de Blaye	9210.9		26015.73	16127.25	30011.52	17787.84	36377.04	37196.03		172726.31
Escargots de Bourgogne	3628.75	3812.7	4377.1		1810	562.6	5056.23	5461.3		24708.68
Filo Mix		3730.7	5590.22	247.8	2314.3	252	7316.82	1750.9	246.24	21448.98
Flotemysost	1496.4	4999.6	25332.31	5605.25	3140.52	10108.7	9838.78	10872.53	6334.1	77728.19
Geitost	7117.6	894	2161.47	458.76	10725.63	5609.1	4962.18	14103.86	2105.2	48137.8
Genen Shouyu			317.75		4371.6		1931.27	164.4	523.26	7308.28
Gnocchi di nonna Alice	6786.75	5809.28	13524		9832.58	6022.1	26687.67	24335.34	9768.37	102766.09
Gorgonzola Telino	11752.55	6383.5	22935.06	6828.43	3176.27	7464.93	9670.42	6671.89	9469.3	84352.35
Grandma's Boysenberry Spread			5921.42	1979.23	7273.95		2262	2766.75		20203.35
Gravad lax		1622.4				2444.31		8598.18		12664.89
Guaraná Fantástica	3197.1	9359.35	11298.6	9095.41	5082.47	3848.88	7397.05	4236.55	7868.64	61384.05
Gudbrandsdalsost	946	5574	7554.35	1402	10729	6852.8	6465.06	5363.25	6834.83	51721.29
Gula Malacca	923.88	4306.21	6355.4	6799.79	14425.01		3179.81	8390.97	2127.06	46508.13

- Cost of producing it
- Price on the open market
- Value in the future
- Cost of reproducing it, if destroyed
- Benefits it brings to the enterprise in meeting business objectives
- Repercussion to the enterprise, if it were not available
- Advantage to competitor, if he could use/change/destroy it
- Cost to the company, if information were released or altered
- Loss of customer confidence or public credibility, if it is revealed

Threats, vulnerabilities, and events

Threat: Potential cause of an unwanted event that may harm the organization and its assets

- Event: exploit or attack causing harm
- If source is human: accidental/intentional (motives)

Vulnerability: A characteristic (including a weakness) of an asset that can be exploited by a threat

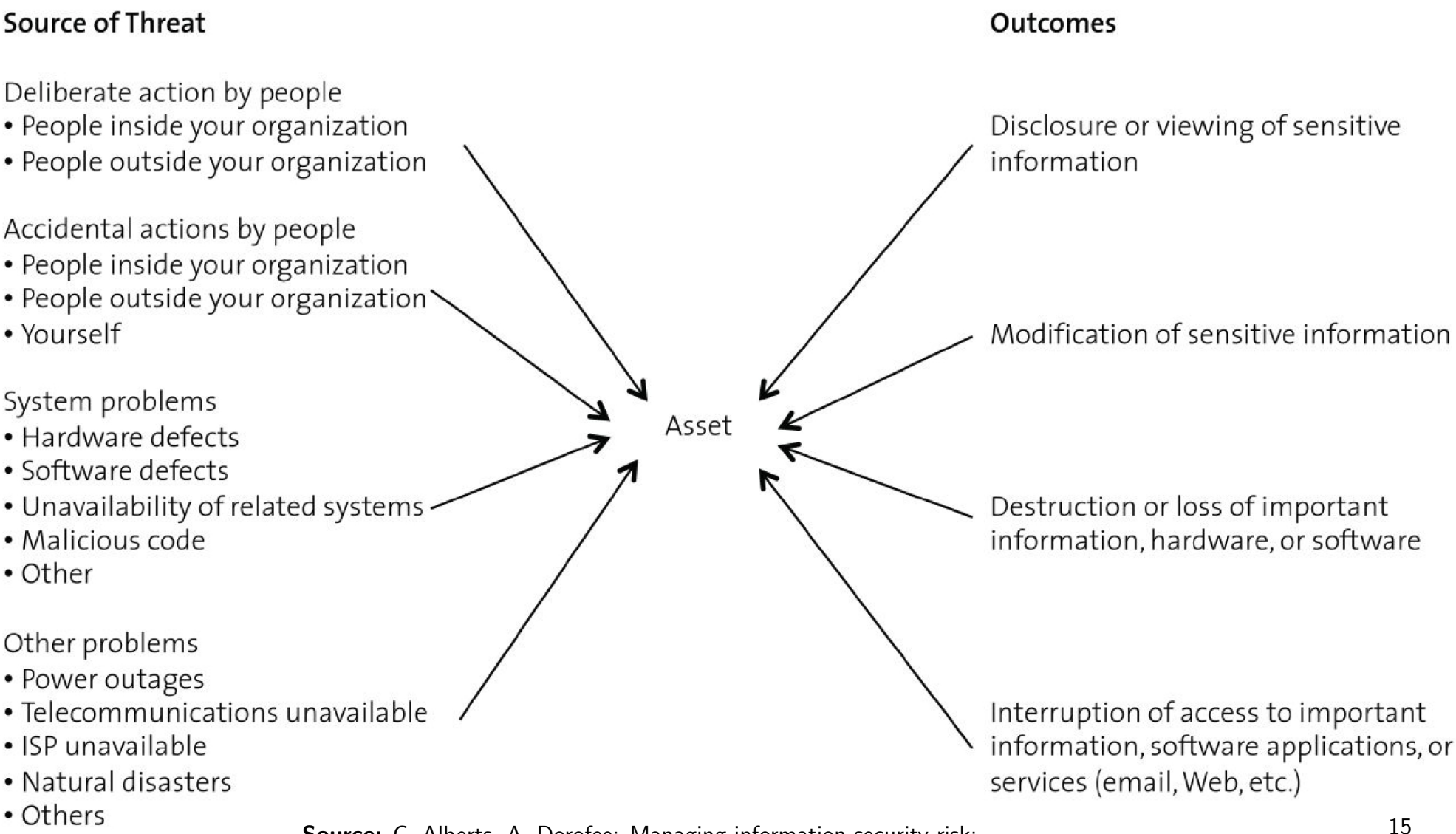
- System weakness that can potentially be exploited
- Threat is an actual way of exploiting a vulnerability

Example

- **Vulnerability:** unvalidated input
- **Threat:** a malicious entity inputs a harmful string
- **Unwanted event:** access to customer data base

Threats and consequences

For different stakeholders: determine how most important assets are threatened.



Source: C. Alberts, A. Dorofee: Managing information security risk: The OCTAVE approach, Addison Wesley 2003

Sources of threats (threat agents)

- External hackers seeking a thrill or financial gain
- External hackers (or nation states) with malicious intent

  Espionage, terrorism, information warfare, ...
- Insiders with malicious intent
- Accidental deletion of files and data
- Environmental damage, such as floods or earthquakes
- Equipment and hardware failure, such as hard disk crash.
- Organizational deficiencies

  no physical access control $\rightarrow$ accidental or intentional crooks

Not all threats based on a malicious intent. Motives can vary!

Direct impact of a materialized threat

- Destruction

  Facilities, data, equipment, communications, personnel

- Corruption or modification

  Data, applications

- Theft, removal, or loss

  Equipment, data, applications

- Unwanted disclosure of data

- Inappropriate use

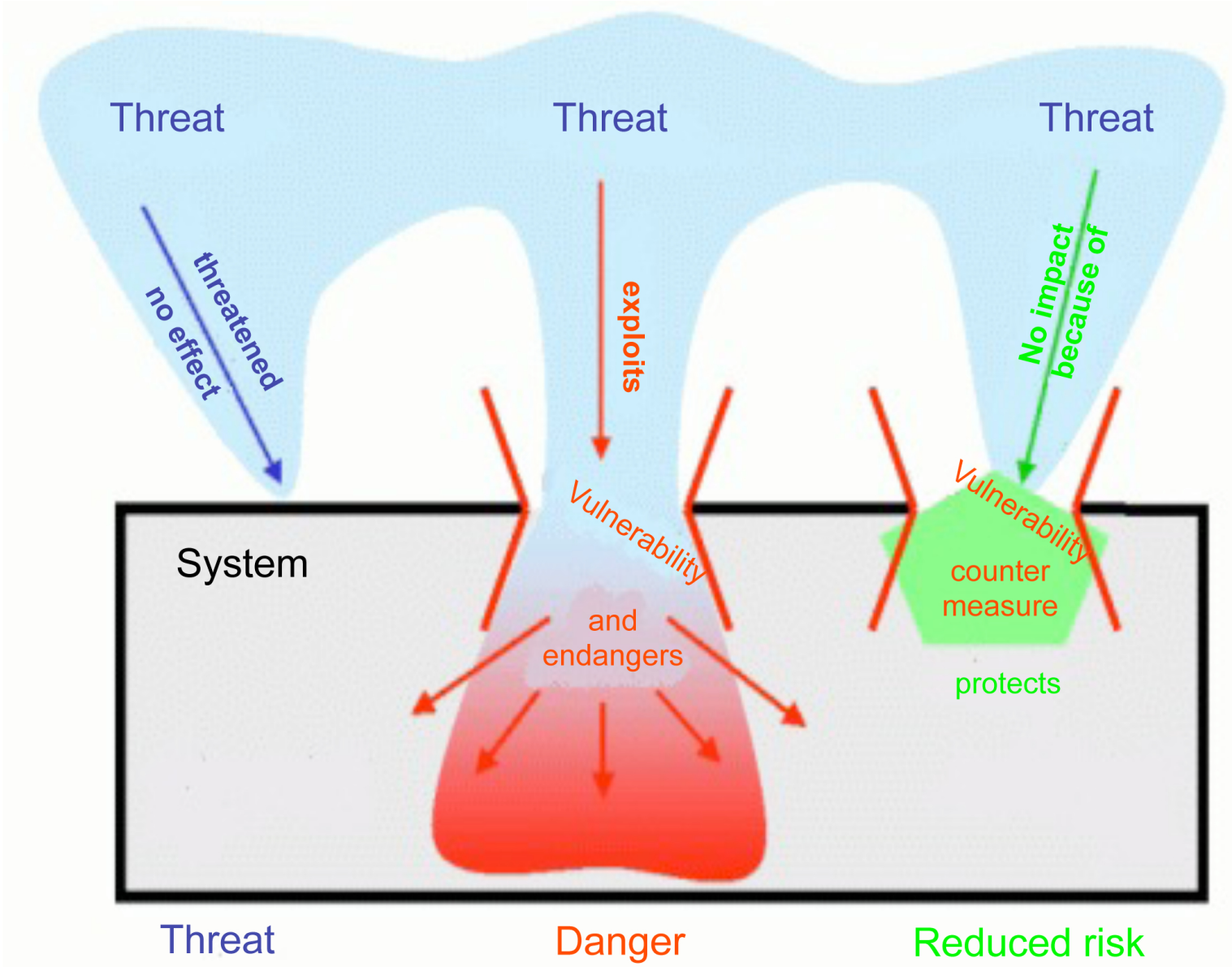
  Unlicensed software, repudiated or false data

- Interruption of services

Countermeasures (safeguards)

- Means to detect, deter, or deny attacks to threatened assets.
  - Encryption, authentication
  - Intrusion detection
  - Auditing
- Countermeasures may have vulnerabilities and are subject to attacks, too!
- Countermeasure are not for free
  - Direct cost
  - Often impact on system function or non-functional behavior
- Subject of security design lecture

Threat categories

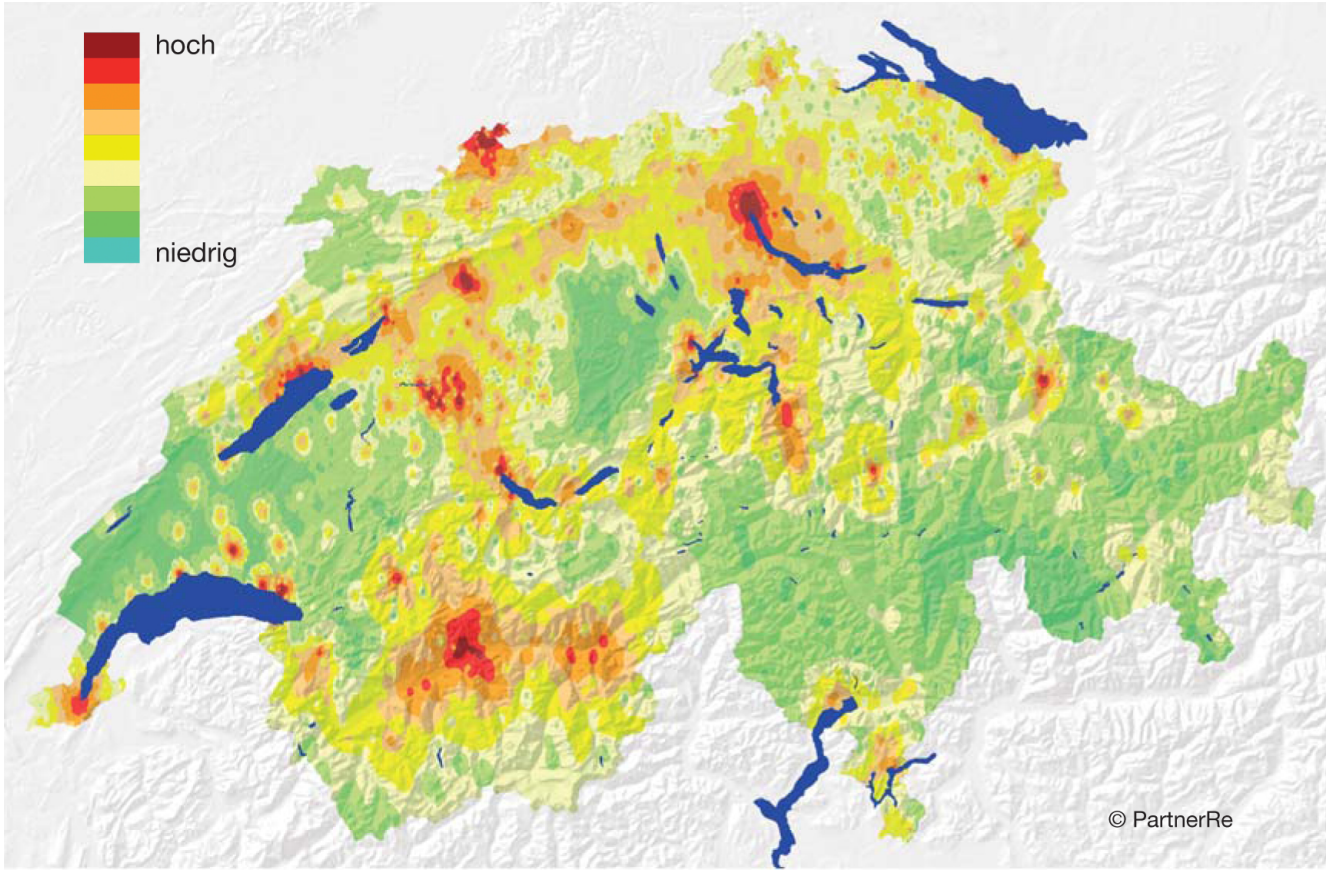


Source: www.bsi.de

Road map

- Motivation and goals
- Assets, threats, vulnerabilities, countermeasures
- ☞ **Risk**
- Qualitative and quantitative risk analysis and management
- Example

First a little quiz[1]



The risk of earthquake damage in Switzerland

Does this make sense? How is this computed?

[1] Source: Schweizerischer Erdbebendienst, ETH Zurich

The answer

Die seismische Gefährdung

Abb. 2: Erdbebengefährdung in der Schweiz. Rot: hohe Gefährdung, blau/grün: moderate Gefährdung. Quelle: SED

+

Beschaffenheit des Untergrundes

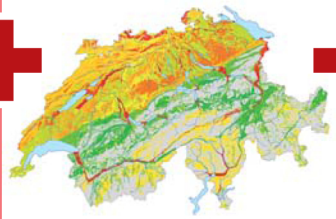


Abb. 3: Karte des lokalen Untergrundes. Besonders gefährdete Gebiete sind rot markiert. Quelle: SED

+

Betroffene Werte

Abb. 4: Verteilung der Siedlungen in der Schweiz.

+

Verletzbarkeit der Gebäude

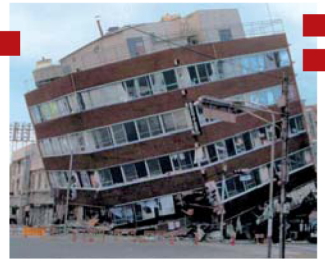
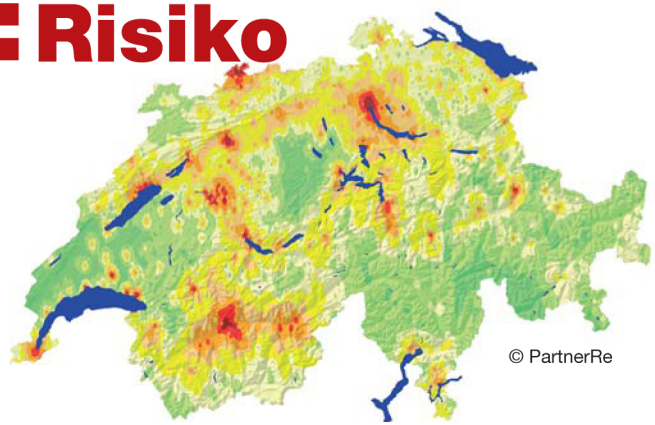


Abb. 5: Erdbebenschaden (Kobe Japan 2005). Quelle: H. Bachmann

=

Erdbeben und Schadenrisiko

Risiko



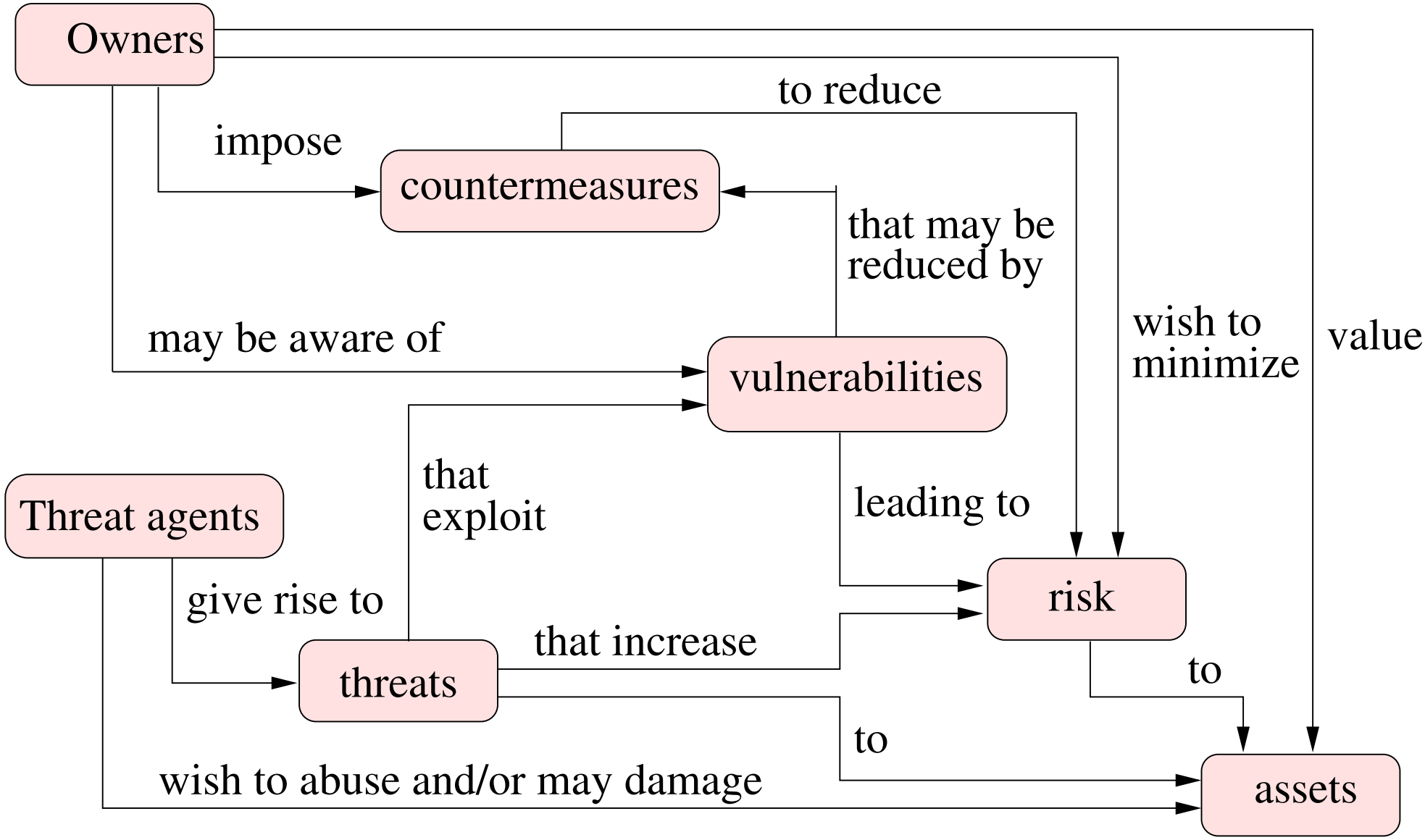
© PartnerRe

How can you **reduce** your personal risk?

- Live where there are no earth quakes or the ground is stable,
- build buildings of little value (so you don't care),
- or build strong buildings!

Other possibilities: **accept** the risk or **transfer** it, e.g., by insurance.

Concepts and relationships



Source: Common Criteria

Risk I

Risk is the possibility to suffer harm or loss.

Risk also is a measure of failure to counter a threat.
(you might well choose to ignore certain threats)

- An organization's risks are a function of:
  1. A **loss associated with an event**, e.g., disclosure of confidential data, lost time, lost revenues
  2. The **likelihood that event occurs**

     N.B. statisticians distinguish between **likelihood** and **probability**. In security, these terms often used interchangibly.
  3. The **degree** to which the **risk outcome can be influenced**, i.e., controls that will influence the event

- Different stakeholders have different perspectives on risk.

Risk II

Risk measures expected loss resulting from a threat successfully exploiting a vulnerability.

- By quantifying the risk, we can justify spending money on controls
- For risk analysis:

  RISK $= \Sigma$ EXPECTED IMPACT or VALUE (\$) $\times$ PROBABILITY

  with quantitative or qualitative ratings
- Annual Loss Expectancy (ALE):

  $$\Sigma \text{ Annual Rate of Occurrence (ARO)} \times \text{damage}$$

Example ALE

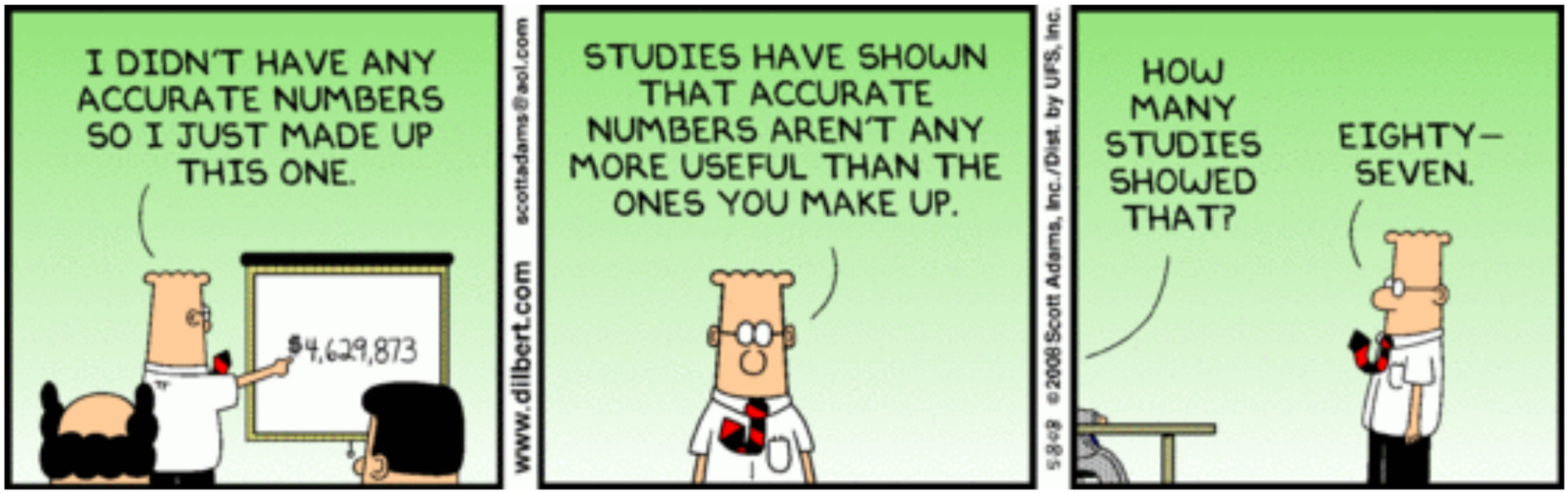
- $3 million business center located in a flood area
- Flood rate of occurrence: once every 50 years (ARO=.02)
- ALE = $3 million $\times$ .02 = $60,000

Observe that we are working with **expected values**.
If the flood occurs, its damage is not $60,000 but $3 million

Example ALE

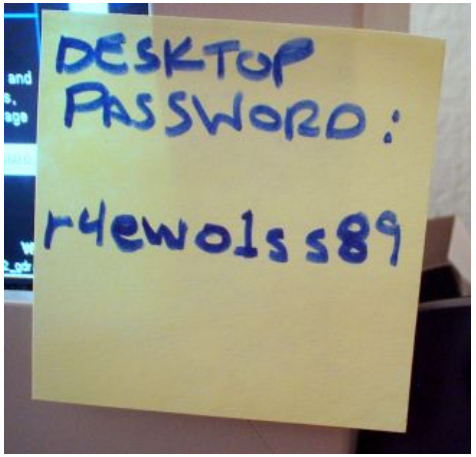
Loss type	Damage	ARO	ALE
SWIFT fraud	$50,000,000	.005	$250,000
ATM fraud (large)	$250,000	0.2	$100,000
ATM fraud (small)	$20,000	0.5	$10,000
Teller takes cash	$3,240	200	$648,000

Where would you invest first to improve security?


I DIDN'T HAVE ANY ACCURATE NUMBERS SO I JUST MADE UP THIS ONE.
$4,629,873
www.dilbert.com scottadams@aol.com
STUDIES HAVE SHOWN THAT ACCURATE NUMBERS AREN'T ANY MORE USEFUL THAN THE ONES YOU MAKE UP.
5-8 © 2008 Scott Adams, Inc./Dist. by UFS, Inc.
HOW MANY STUDIES SHOWED THAT?
EIGHTY-SEVEN.

Risk enablers/vulnerabilities

- Software design flaws
- Software implementation errors
- System misconfiguration, e.g., firewalls, WLANS, ...
- Inadequate security policies or enforcement
- Poor system management
- Lack of physical protection
- Lack of employee training



Human errors behind most risk enablers

Handling risk: strategies for risk reduction

- **Avoid** the risk, by changing requirements for security or other system characteristics (followed by redesign/implementation)
- **Transfer** the risk, by allocating it to other systems, people, organization's assets or by buying insurance
- **Assume** the risk, by accepting it and controlling it with available resources

Corresponding costs must be taken into account

Road map

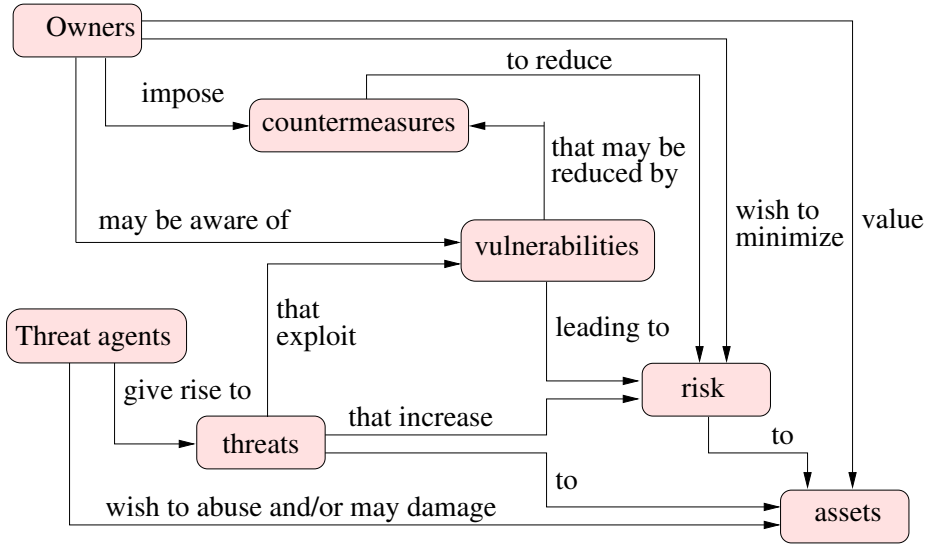
- Motivation and goals
- Assets, threats, vulnerabilities, countermeasures
- Risk
- ☞ **Qualitative and quantitative risk analysis and management**
- Example

Risk analysis and management

Risk analysis is the process of examining a system and its operational context to determine possible exposures and the harm they can cause.

- A study of risk that a business or system is subject to, e.g., exposure and potential losses.
- Risk management involves the identification, selection, and adoption of security measures justified by
  - The identified risks to assets
  - The employment of measures to reduce these risks to acceptable levels
  - The cost of these measures

Generic procedure



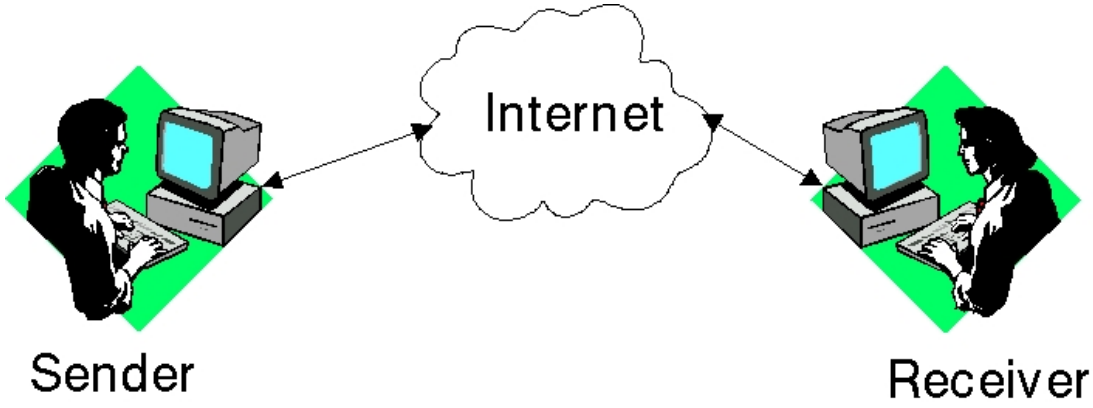
1. Identify **assets** to be reviewed
2. Ascertain **threats** and the **corresponding vulnerabilities** regarding that asset
3. **Calculate** and **prioritize** the risk
4. Identify and implement **countermeasures**, controls, or safeguards—or accept the risk

   For countermeasures: check that they don't introduce new risks.
5. **Monitor** the effectiveness of the controls and assess them

Plethora of methods around!

Let's look at several examples first, in the small.

Example
protecting email



1. What are the information assets?

   Possible answers: mail content (confidentiality, integrity), sender/recipient identities, service availability, ...

2. What are the risks?

   - Others reading or tampering with your mail, observing with whom you communicate, and disrupting service.
   - Chance of abuse depends on who you are, what you send, and how interesting it is to others.

Email: analysis and a possible solution

Evaluation of PGP as a possible good solution:

3. Effectiveness: high, provided it is used correctly.

4. New risks and tradeoffs:

   - Key exchange time consuming and requires some sophistication.
   - Limited support on different mail clients
     e.g., Enigma plugin for Thunderbird supporting OpenPGP.
   - Users must learn, and properly apply, new mailer functionalities and understand the principles behind PGP (Web of Trust).

Conclusion: PGP is good solution for ensuring confidentiality of sensitive information mailed between knowledgeable partners.

Exercise: Contrast with S/MIME+X509-based solutions.

Example: face scanning in airports

Since 9/11, face scanning and matching against databases of known terrorists has been proposed to improve airport security.

1. What are the assets (information or otherwise)?

   Air travelers and those on the ground.

2. What are the risks?

   Terrorists will board planes and may cause harm.

3. Effectiveness: very low

   Suppose system positively identifies 50% of all known terrorists but has 1% rate of false positives. Suppose there is one terrorist per million. Then for every terrorist recognized, so are 20,000 innocent civilians. At this rate, the security personnel will be overwhelmed and stop believing the alarms.

Face scanning (cont.)

4. New risks and tradeoffs.

   The face database must be secured. If integrity is not protected, faces can be deleted. If confidentiality not protected, terrorists can determine if they are in database and take appropriate actions (e.g., send an accomplice or change appearance).

   The privacy of airport visitors is compromised.

   System may instill a false sense of security, lessening overall security. Moreover, it involves high costs and inconvenience.

Exercise: Risk analysis for use of intrusion detection system in enterprise computing.

(Fully) Quantitative risk analysis

- **Goal**: assign independently obtained, objective, **numeric values** to all components of a risk analysis
  - Asset value and potential loss
  - Safeguard effectiveness
  - Safeguard cost
  - Probability
- **Pros**:
  - Effort put into asset value determination and risk mitigation
  - Cost/benefit analysis
  - Numbers good for comparisons and communication
- **Cons**: critical knowledge base, costly

Quantitative risk analysis

- **Rational**: Businesses want to measure risks in terms of money

  This aids decision support

- Difficult for many logical and intangible assets
  - In-house software
  - Customer goodwill and reputation
- Reliance on historical data

  Nature of future attacks/attackers are, in principle, unpredictable

- Problems comparing approximate quantities:

  How does a security measure costing \$10,000 affect a $\sim 10^{-5}$ probability of attack?

- Monetary values give a false impression of precision

Qualitative risk analysis

- "What if" questions with **ordinal numbers** (rankings)
- Instead of probabilities, use categories (high, medium, low)
- **Pros**:
  - simpler as need not determine exact monetary values of assets or probability of different threats succeeding
  - easy to involve different parties

  Cons:
  - even more subjective
  - no single number for decision support
  - no basis for cost-benefit analysis

The jury is still out

- Rankings are questionable
- Even more so: concrete probabilities
- However, insurance companies manage to work with expected values
- So do reliability engineering, who work with operational profiles (operations+ probabilities)

Road map

- Motivation and Goals
- Assets, threats, vulnerabilities, countermeasures
- Risk
- Qualitative and quantitative risk analysis and management

☞ **Example**

Qualitative risk analysis

- Determine the scope, assemble the team, and identify assets
- Identify threats (and vulnerabilities)
- Prioritize threats, determine impact priorities and total impact

$$\text{high probability} \times \text{low impact} = \text{medium risk}$$

- Identify safeguards
- Cost-benefit analysis and prioritization of safeguards
- Report

Example procedure for matrix-based qualitative RA

- Identify assets, A
- What would be the impact if some assets were compromised?
  - Identify relevant assets, R with $R \subseteq A$
  - Violation of CIA
  - Different levels of impact: direct financial loss, reputation, ...
- Identify threats T to R
  - Actors, motives, their capabilities and possibilities, vulnerabilities
  - Use the techniques from threat modeling module
- For each $r \in R$ and each $t \in T$, determine
  - the attributes of r that are affected, their value, and consequently, the impact on the mission
  - low/medium/high probabilities $p(t)$
- Determine safeguards and their costs and benefits

Matrix procedure (cont.)

Let's look at 3 phases, in more detail:

- Asset (identification and) valuation
- Risk evaluation
- Risk management

Phase 1: Asset Valuation[2]

	Financial Loss	Legal Impact	Value to Competitor	Embarr-assment
Disclosure				
Unavailability				
Destruction				

Value asset groups in terms of the impact on business operations, for breaches of CIA.

[2] **Source for pages 46–50, 53–54**: T. Peltier: Information security risk analysis, Auerbach, 2001

Valuation: Financial Loss

Financial Loss	Valuation Score
Less than $2,000	1
Between $2K and $15K	2
Between $15K and $40K	3
Between $40K and $100K	4
Between $100K and $300K	5
Between $300K and $1M	6
Between $1M and $3M	7
Between $3M and $10M	8
Between $10M and $30M	9
Over $30M	10

Figures are company specific.
In many cases, categories low, medium, and high may suffice.

Valuation: Legal Impact

Legal Impact	Valuation Score
Under $5K	1
Between $5K and $10K	4
Between $10K and $50K	5
Between $50K and $1M and/or CIO liable for prosecution	8
Over $1M and/or board members liable	10

Valuation: Value to Competitor

Value to Competitor	Valuation Score
Less than $50K	1
Between $50K and $100K	4
Between $100K and $10M	5
Over $10M	7

Valuation: Embarrassment

Enterprise Embarrassment	Valuation Score
Restricted to project or work site	1
Spreads to other areas of operating group/division	2
Spreads throughout enterprise	3
Public made aware through local press coverage	5
Adverse national press	7
Stock price impacted	10

Phase 2: Risk evaluation

- Combine asset valuations and determine "importance threshold"
  - Don't bother management with negligible risks.
  - Concentrate on the critical few
- Determine threats, probabilities, and impact (qualitatively!)
- Impact is a function of the weighted compromised attributes of the asset with respect to a particular threat
- The impact will later be weighted against possible remedies
  - Consider both with and without existing safeguard in place
  - E.g., no problem with integrity because errors are quickly discovered and easily corrected

Probabilities and impact — NIST categorization

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls exist to prevent or significantly impede the vulnerability from being exercised.

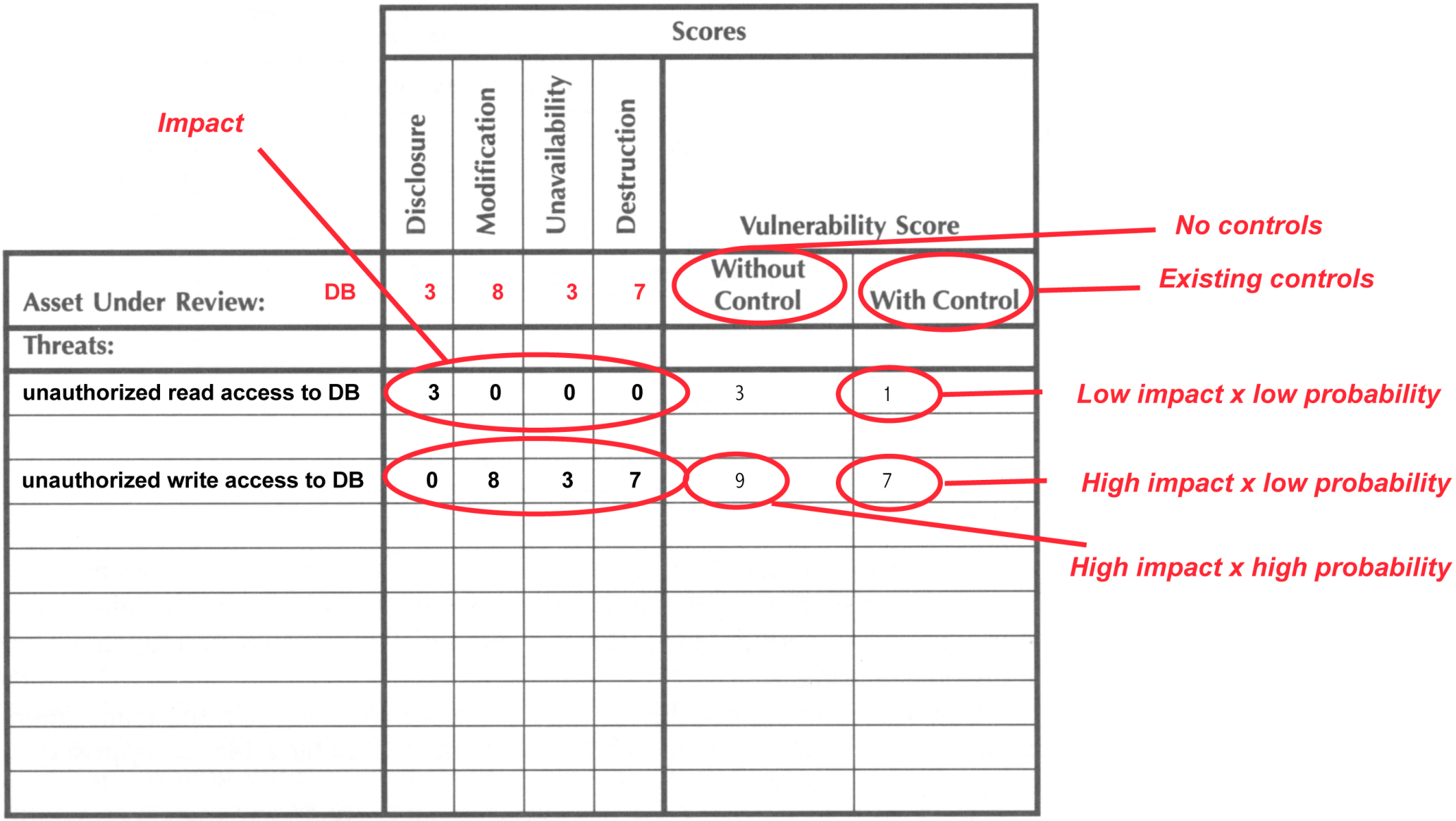
Magnitude	Impact Definition
High	Exercise of vulnerability (1) may result in highly costly loss of major assets or resources; (2) significantly violate, harm, or impede organization's mission, reputation, or interest; or (3) result in human death or serious injury.
Medium	Exercise of vulnerability (1) may result in costly loss of assets or resources; (2) violate, harm, or impede organization's mission, reputation, or interest, or (3) result in human injury.
Low	Exercise of vulnerability (1) may result in loss of assets or resources; (2) noticeably affect organization's mission, reputation, or interest.

Combine impact and probability

Probability		Impact: Low	Impact: Medium	Impact: High
	High	3	6	9
	Medium	2	5	8
	Low	1	4	7

Result is an overall **vulnerability score**.
No general agreement on best "combination function".

Integrated view



Here combining numeric impacts & probability categories

Phase 3: Risk Management

- Goal: recommend safeguards where necessary
- Phase I yields assets important to the enterprise
- Phase II yields relevant threats

  Taking into account the existing infrastructure
- Phase III then considers possible countermeasures, their cost, and their potential benefit
  - Budget is finite. Not all risks are worth countering. Prioritize!
  - We will look at countermeasures and redesign in upcoming security design module

Example — discussion

- Most risk analyses work in a similar manner

  Some take into account cost/benefit for the intruder

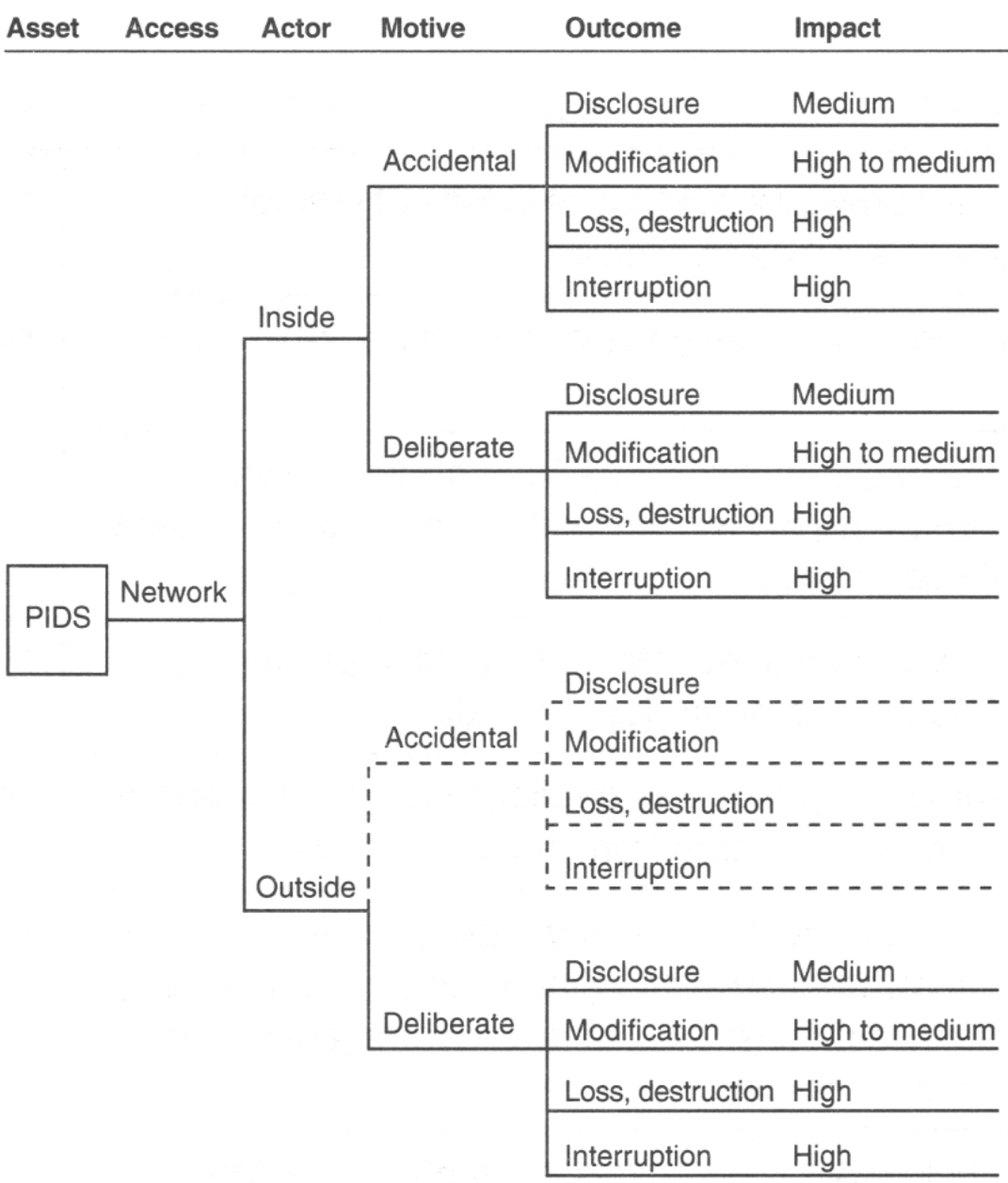
- Probabilities
  - Hard or impossible to obtain
  - Rough categorization may not really help
  - Multiplication of probabilities with impact (qualitatively)?

- As with most scenario analyses, the numbers are less important than the mere activity of thinking about problems

- It is crucial to know about potential threats and vulnerabilities

  Use catalogs such as CERT advisories, BSI Grundschutz

Example: OCTAVE — no probabilities



Risk Mitigation Plan

- Introduce user training for PIDS and require refresher training training to bring users up to date on improvements and identify and correct bad habits.
- Notify ABC Systems of any security issues to facilitate recovery.
- Enforce password discipline. Report password abuse.
- Establish vulnerability management policies and procedures.

Measures:

- Start tracking who attends training.
- Have IT begin monthly reports on internal security violations after everyone has been reminded of the policies and sanctions.
- Report status on this plan monthly at managers' meeting.

Source: C. Alberts, A. Dorofee: Managing information security risk: The OCTAVE approach, Addison Wesley 2003

Summary

- Risk is a function of assets and threats
  - Value of assets, probability of a threat materializing
  - Existing safeguards
- Not all threats equally dangerous and countermeasures are not for free

  Rely on lists of existing threats and vulnerabilities!
- Most risk analysis procedures rely on some structured means of identifying and evaluating the above items
- Quantitative assessments are difficult
  - Assignment of probabilities/impacts
  - BSI baseline protection and OCTAVE don't even consider probabilities