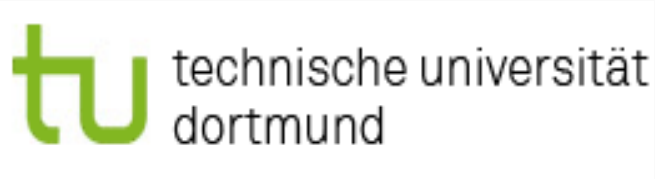


PROBLEM ANALYSIS OF IT-SECURITY RISK ASSESSMENT METHODS – AN EXPERIENCE REPORT FROM THE INSURANCE AND AUDITING DOMAIN

Stefan Taubenberger (MunichRe/OU), Jan Jürjens (TUD),
Yijun Yu (OU) and Bashar Nuseibeh (OU) , June 9th, 2011

A few words on risk

“This committee labored for 4 years and then gave up, saying in its final report, that maybe it’s better not to define risk. Let each author define it in his own way, only please each should explain clearly what way that is.” (Stan Kaplan – The Words of Risk Analysis, 1997)

“Risk is a condition of individuals – humans and animals – that are self aware. Organizations, companies and governments are not self-aware, so they are incapable of being at risk.”(Glyn A. Holton – Defining risk, 2004)

“Risk, after all, reflects economic change and human inventiveness: there are undoubtedly new types of risk being created at this very moment that will require new thinking (and terminology) on how they are approached.” (Robert N. Charette - A Risk of Too Many Risk Standards?, 2006)

“The most pernicious thing about modern risk management is the illusion of precision.” (Satyajit Das – perfect storms, 2007)

Risk is about experiences and coherences as well as chances.

Problem domain – Statement about information security risk

- **IT Auditing domain:** Auditors have to concentrate on areas that are to be expected more risky as they have a limited time to conduct audits. The challenge is to conduct the IT risk evaluation of a company in a cost and time efficient way and to identify significant risks.
- **Business insurance domain:** An company that applies for e.g. business interruption insurance will be insured if IT risks are limited and controlled regarding their business model. The legal entity has to be assessed regarding IT risks and implemented countermeasures. Assessments have to be cost and time efficient as well as precise to be able to acquire profitable business.

Interested in the presence and absence of risks as well as the security process capabilities of a company!

Information security risk and input for risk assessment methods

Information security risk: "The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization" ISO 27005:2008

"**Risk** is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system." NIST 800-30

Typical approach to the problem:
Quantitative and qualitative risk assessment approaches/standards are applied using probability and impact estimates. These approaches are focused on assets, events and probabilities by checking events and vulnerabilities or are using best practice controls.

Quantitative and qualitative assessments are dependent on correct data for probabilities and impact as well as the correct identification of events, vulnerabilities, impact and dependencies.

Problems in the different phases of a risk assessment

Identification:

- Threats and vulnerabilities are identified based on expert knowledge and corresponding **explicit and implicit knowledge**; **Concept of you know one if you see one** is based on experience
- **No detailed guidance** available especially on how to link threat sources with vulnerabilities, how to derive or evaluate any probabilities.
- **Environment changes constantly** (not static) therefore historic data does not present a true view (validity of probability distributions) e.g. 9/11, subprime crisis ... (The black swan example)
- **Dependencies** between elements are not considered nor indicated; evaluation is conducted on single elements/assets like systems, data (decomposition)
- Intercompany dependencies: events in these companies are not considered

Completeness and comprehensiveness of the threat list or vulnerabilities unknown or can not be verified. Use standards lists.

Problems in the different phases of a risk assessment

Data

- **No extensive public data** about threats/vulnerabilities and their occurrence rates and impacts as well as verification of data difficult
- **Internal and external historic data might not be correct** because e.g. the event has not occurred in this industry, scope or situation; may be incomplete or may represent a “lucky” history
- **Estimates are used** without knowing the basic population
- **Data** is simply **not available** – best guesses are used

How can we ensure or verify that the data used for assessments are correct, valid as well as available.

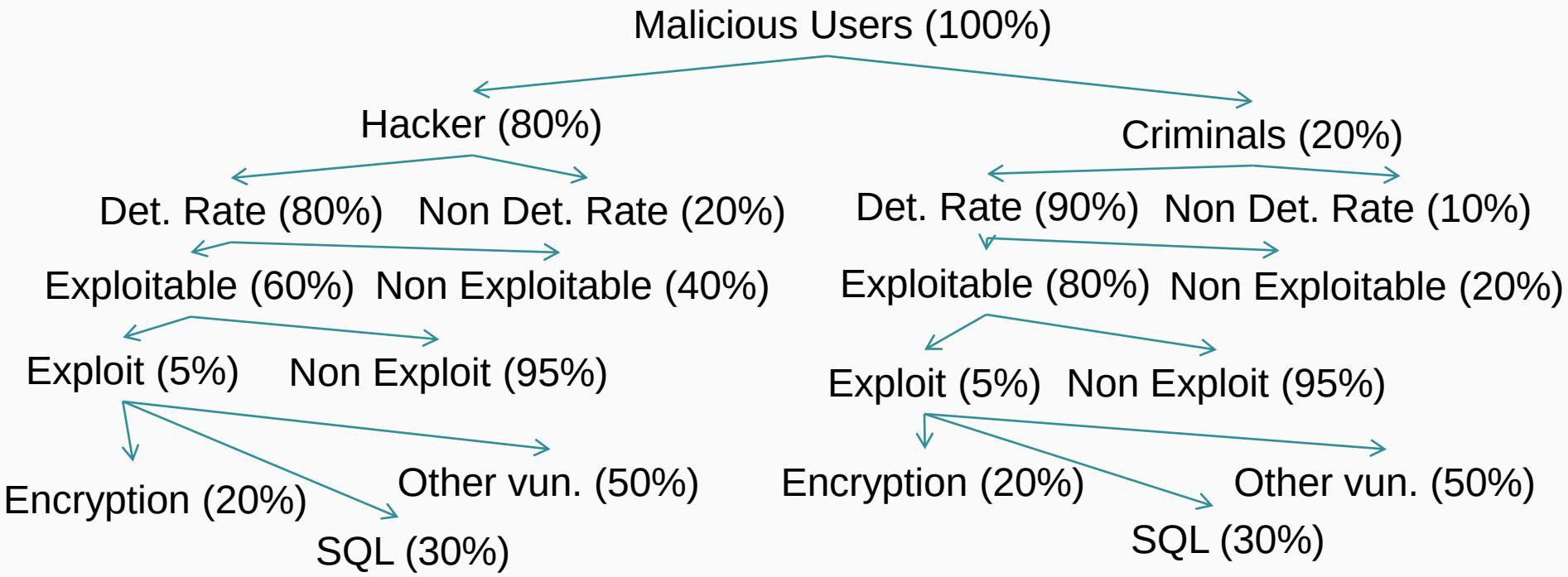
Problems in the different phases of a risk assessment

Assessment

- The consequences and the existence of **misestimating** are not considered as well as aggregation of probabilities misrepresents the occurrence of an event.
- **Psychological phenomena** may contribute to uncertainty, the assessors of probabilities and impacts are influenced by factors such as experience, social groups and negative media
- **Co-occurrence of risks**, uncertainty between event relations and different assessment scales are not considered.
- **Usage of decomposed model elements** simplify the organization and are not interconnected
- **Side effects** (multiple impacts or dependencies) are not modelled and results are **time dependent (**assessment at a specific time)

Assessment methods should consider dependencies, the business operation as well as reduce subjectivity. The result should be time independent and indicate the presence/absence of risk.

Example - Probability tree of a malicous action



Determine likelihood of an action - Problem: *Are parameters objectively determinable?*

Example - Probability calculation problems

Dependencies: There is a **direct dependency** of the result to single parameters e.g. a reduction/increase of one parameter from 5 to 10 (100 percent change) leads to a reduction/increase of the result in the same percentage. We recognized that the percentage of misestimating is relevant not the absolute amount.

Baseline: The **total population** has to be specified because a, for example, 12% or medium probability has no significance.

Probability: In a chain of parameters the total **probability inclines** against 0 or 100 percent as it is below or above the minimum or maximum values. These high or low values blur the total probability exceptionally.

Tree diagram: Generally, it is difficult to determine the dependencies of parameters, the **correct tree diagram** and to verify the diagram as there is no data available.

Perception: The **perception of the results** is dependent on the probability question and the result value.

Probabilities are difficult to determine and to verify. Interpretation and estimates necessary.

Overview of problems in IT risk assessments - Summary

- Methods: Data needs to be available and correct as well as results be interpreted.
- Guidance and identification: The concept used for identification of threats, vulnerabilities or correlations is “you know one when you see one”
- Dependencies: Assessment concentrates on single assets or threat scenarios.
- Probabilities: Correctness and completeness of estimates.
- Assessment: Specific to a point of time and contains intransparent uncertainties.
- Risk results: Perception, consideration of cost objectives and prioritization of measures occurs.
- Environment: Events, parameters, probabilities, the basic population as well as correlations are not known (Changing environment).

IT risk assessment methods have multiple weaknesses.

New Direction

We believe the question should not be ‘What are the threats/events, potential vulnerabilities and impacts” because there are to much uncertainties in the risk identification process. Instead the question should be “Is the company operation sufficiently protected and operate controls correctly.”

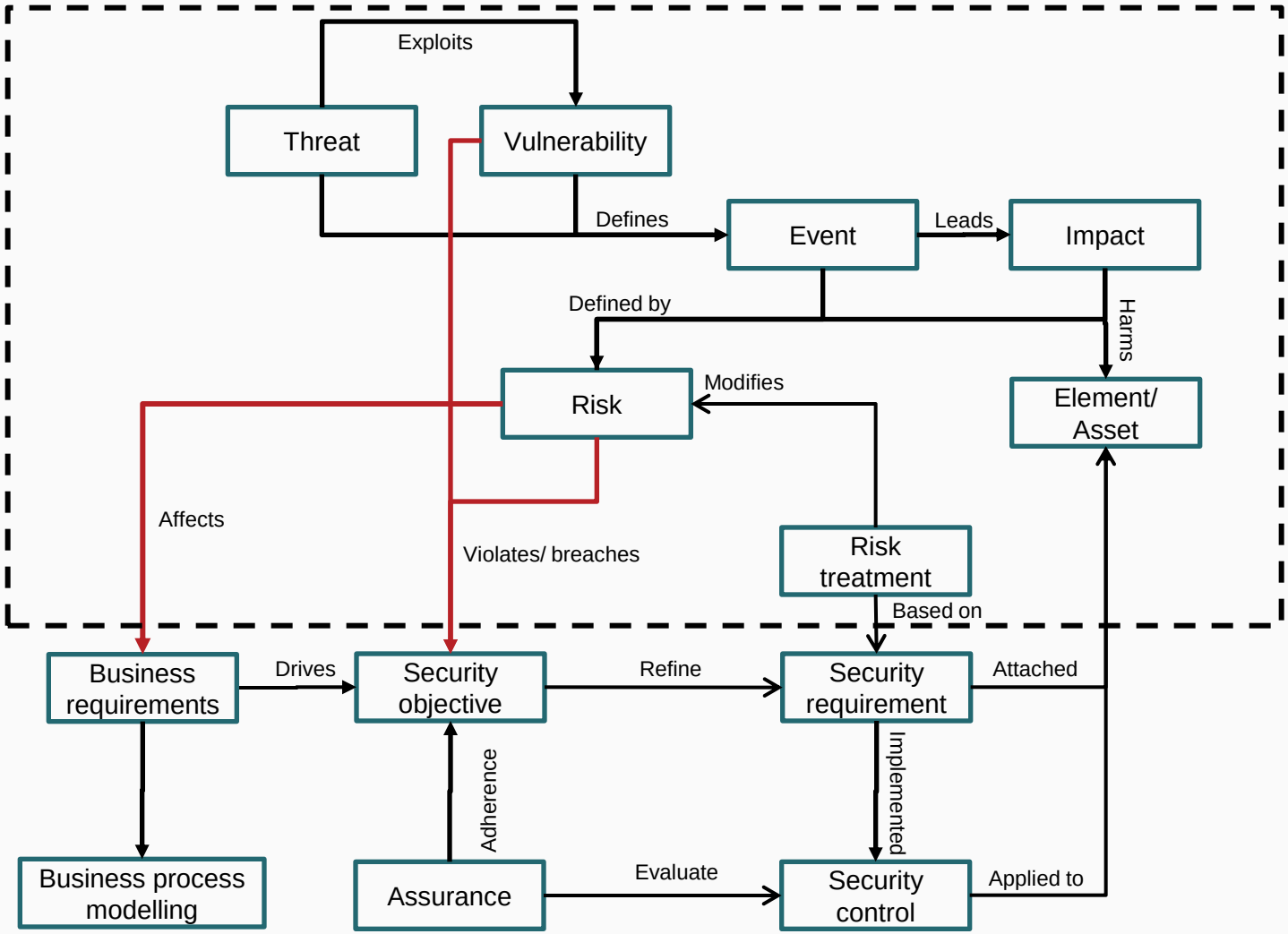
Different assessment process that focus on e.g. security requirements and security design and control implementation within the business context. Linkage of security needs, perils, controls and control implementation in an assessment method.

Advantages

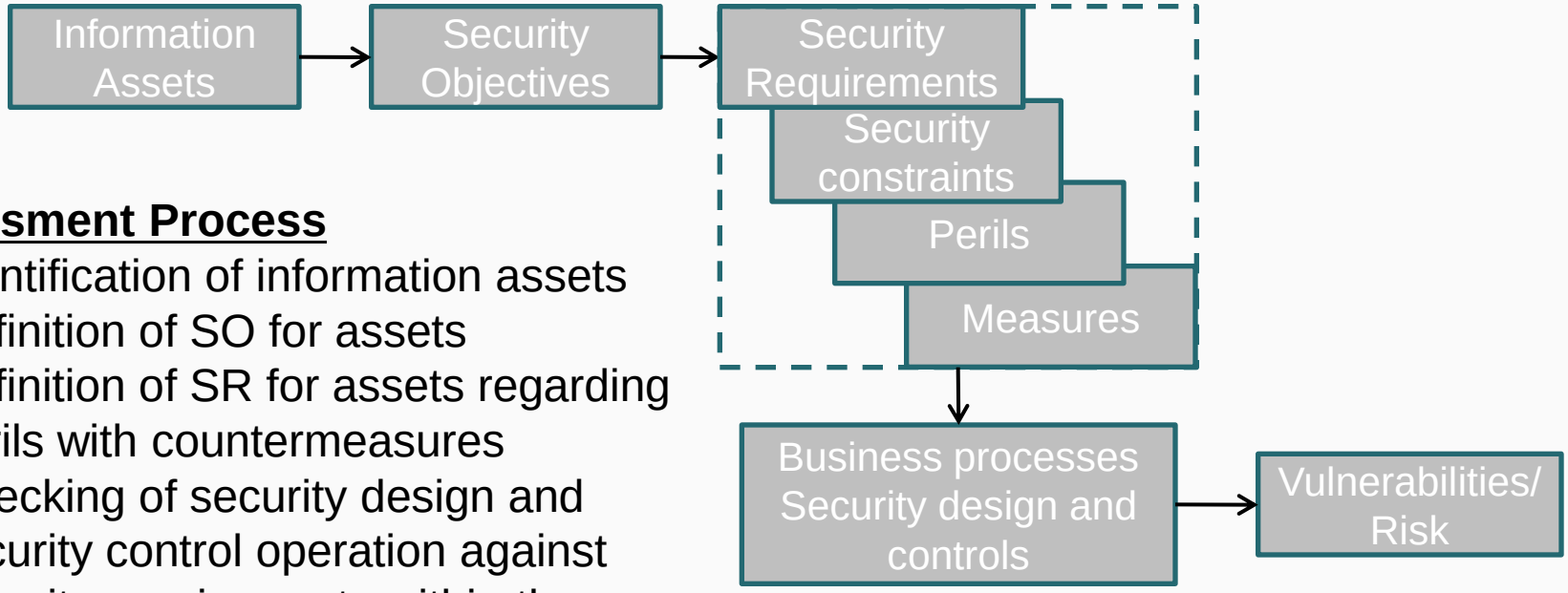
- Indication of the presence and absence of risk
- Evaluation of current security controls in the business context
- Statement about the security capability of a company
- More time independent risk results

Risk assessment will be still subjective however, focused on security needs, control operation and event protection.

An Information Security Risk Model



New Direction – Assessment process



Assessment Process

1. Identification of information assets
2. Definition of SO for assets
3. Definition of SR for assets regarding perils with countermeasures
4. Checking of security design and security control operation against security requirements within the business operation

Risk is defined as "non-adherence of security requirements thereby cause harm to the organization".

MANY THANKS FOR YOUR ATTENTION!

Stefan Taubenberger