CIRA –
Conflicting Incentives Risk Analysis

Gaute Wangen, PhD student at Gjøvik University College

COINS PhD Seminar in Tromsø, 13-15.10.14

Problem description

Current Risk Analysis methods are too focused on IT-security, and does not consider the humans in Information Security adequetly

Incentive based systems explained

- An incentive is something that motivates a person to commit an action or behave a certain way
- We can use incentive based systems to compell a certain behavior
- Such a system can be
  - Reward based – e.g. financial based, benefits for acting in a particular way
  - Moral based – e.g. the right or wrong thing to do, achieve fame or shorn from a community
  - Coersive – e.g. the threat of punishment for not acting in an certain way
  - Natural based – e.g. curiosity, mental or physical exercise

Examples of Incentive based systems

- Salaries – working more earns you more (most of the time…)
- Laws and juridical system – crime comes with punishment
- Rules in Soccer to ensure desired behavior

Incentive
/in-sen-tiv/
def: A reward or promise of payment that encourages a person to take a certain action, behave better or work harder.

http://www.entredonovan.com/media/wysiwyg/Incentive.jpg

Conflicting Incentives in Soccer?

© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com
DRAMA COACH
search ID: tpa0151

Conflicting Incentives

- According to CIRA *“we have risk if the stakeholder that is in the position to trigger the action and the risk taker would be in disagreement as to weather or not the action should be implemented“* - Snekkenes, 2012

- Is conflicting incentives a source of information security risk?

Information Security Risks explained in Conflicting Incentives

- Conflict 1: Nurses/Doctors in healthcare, patient as risk owner:
  - Incentive 1: Gossip to achieve social status
  - Incentive 2: Preserving Patient privacy

- Conflict 2: User efficiency vs security compliance, employer as (main) risk owner:
  - I1: Cutting corners for efficiency
  - I2: Complying with security policy

- Which is the stronger incentive?
- How do we risk manage these scenarios?

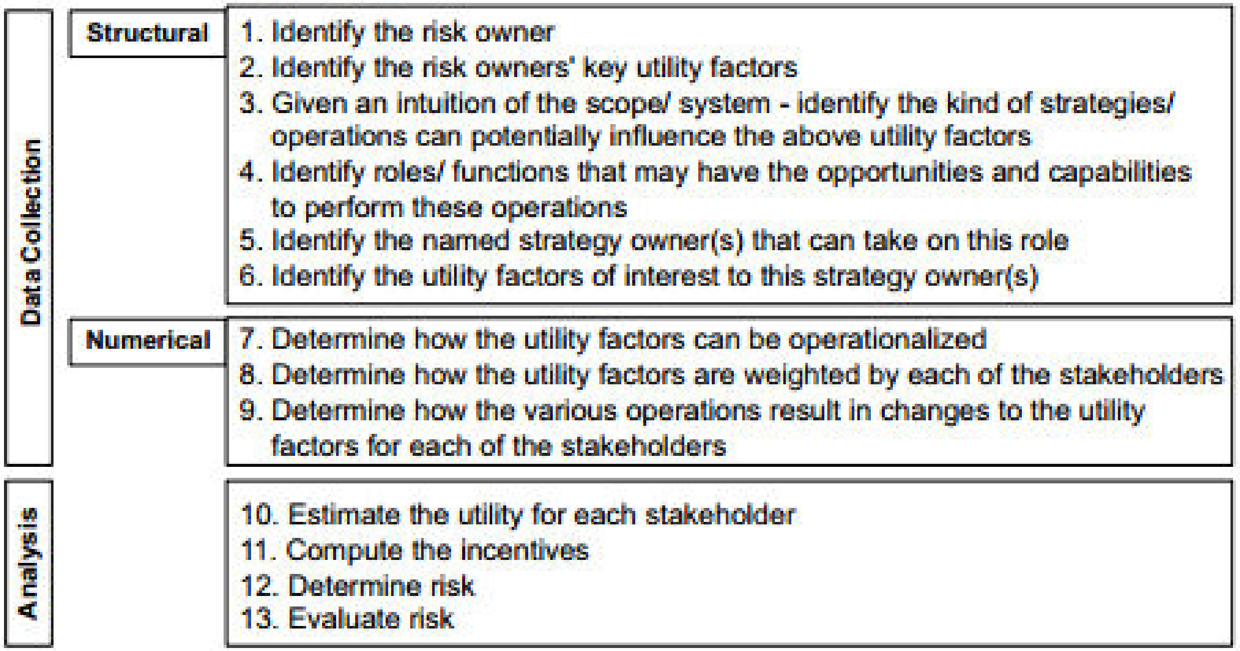
The Components of CIRA (1)

- CIRA uses aspects from many theoretical fields:
  - Risk Management and Analysis
  - Game Theory – Games and Strategies
  - Economics – Utilities
  - Psychology – Human incentives
  - Decision Theory – MAUT, MCDA

The Components of CIRA (2)

- CIRA identifies:
  - Scenario
  - Risk Owner
  - Stakeholders
  - Utility Factors
  - Actions/Capabilities
  - Perceived expected consequences that characterizes the risk situation
  - Controls

The Components of CIRA (3)



Data Collection

Structural

1. Identify the risk owner
2. Identify the risk owners' key utility factors
3. Given an intuition of the scope/ system - identify the kind of strategies/ operations can potentially influence the above utility factors
4. Identify roles/ functions that may have the opportunities and capabilities to perform these operations
5. Identify the named strategy owner(s) that can take on this role
6. Identify the utility factors of interest to this strategy owner(s)

Numerical

7. Determine how the utility factors can be operationalized
8. Determine how the utility factors are weighted by each of the stakeholders
9. Determine how the various operations result in changes to the utility factors for each of the stakeholders

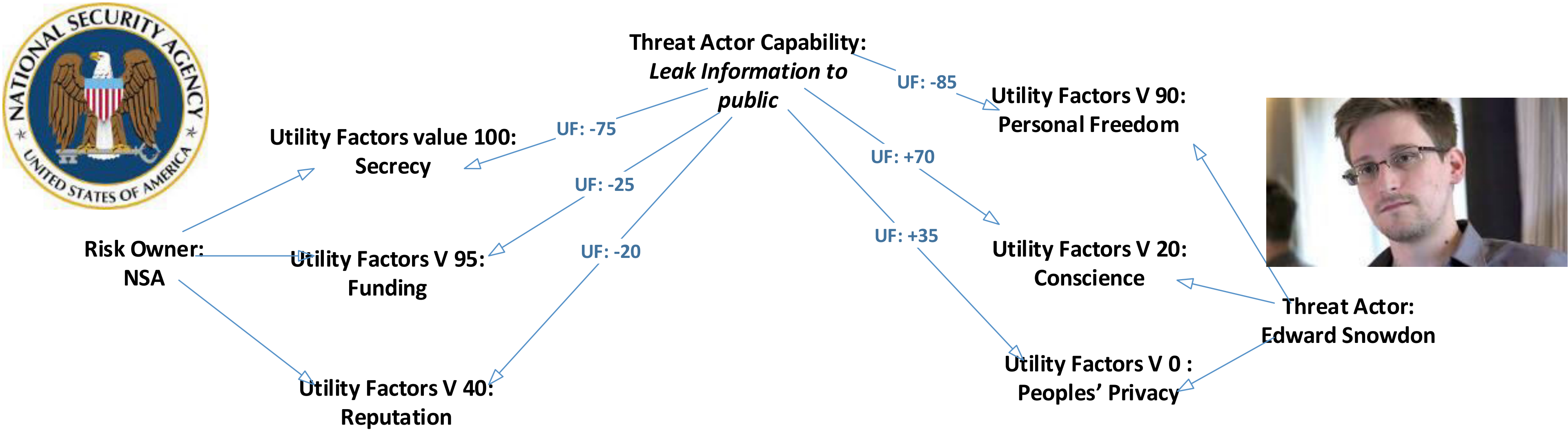
Analysis

10. Estimate the utility for each stakeholder
11. Compute the incentives
12. Determine risk
13. Evaluate risk

Figure 11.1: Procedure in CIRA

Rajbhandari & Snekkenes (2013)

Simple CIRA in practice, example scenario Snowden leaks



Threat Actor Capability:
Leak Information to public

Risk Owner:
NSA

Utility Factors value 100:
Secrecy

Utility Factors V 95:
Funding

Utility Factors V 40:
Reputation

UF: -75

UF: -25

UF: -20

UF: -85

UF: +70

UF: +35

Utility Factors V 90:
Personal Freedom

Utility Factors V 20:
Conscience

Utility Factors V 0 :
Peoples' Privacy

Threat Actor:
Edward Snowdon

Future Work

- Case Studies
  - The theoretical work of CIRA is well under way, and needs to validated
  - Further development of CIRA
  - CIRA in Business Processes Security Re-engineering