Risk Management

Information Security

Dr Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2011 – Week 5

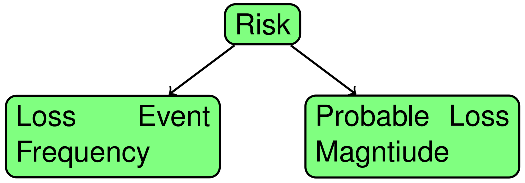
Learning Outcomes

After this week, students should be able to

- understand what risk is.
- know what one can do about risk.
- conduct a simple risk analysis using the FAIR framework.

Definition of Risk

Risk is potential event which, if occuring, will cause some impact.



Risk

Loss Event Frequency

Probable Loss Magntiude

Risk Treatment

Only four approaches to risk — TARA

Transfer	Let someone else take the risk.
Avoid	Drop the business.
Reduce	Implement effective controls to reduce the probability and/or impact.
Accept	Conclude that the benefit outweighs the risk and live with it.

Transfer

- Common example: insurance
  - pay someone to take the risk for you
  - insurers gather risks in large quantities
  - Law of Large Numbers in Statistics reduces total risk
- Contractual matters
  - transfer risk to your clients
  - key issue of any contract: who takes the risk?

Avoid

- Avoid means staying out of the business.

  Nothing ventured, nothing gained.
- One avoids the risk it outweighs the possible gain.
  - Choosing not to have WiFi
  - Choosing not to use BankID
  - Choosing not to have web pages
  - Choosing not to do business in South America

  There is NO *other way to avoid risk.*

Reduce

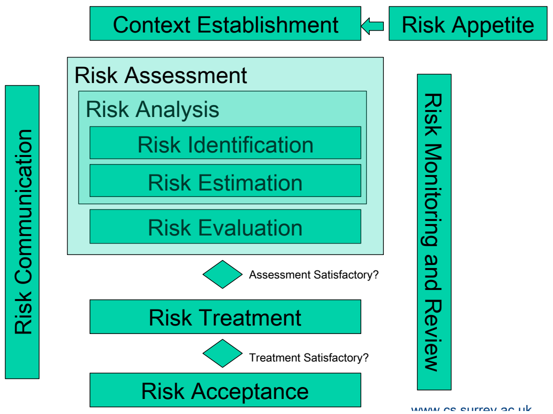
- Controls reduce risk
  - you can (almost?) never reduce risk to zero
  - expect some residual risk
- Access control may reduce the risk of having WiFi
- Malware filters may reduce the risk of using BankID
- Good secure coding practice may reduce the risk of web pages

Accept

Risk does not have to be bad

- We accept risk when ...
  - The possible gain outweighs the risk
  - The cost of reducing or transferring the risk outweighs the risk itself

Graphical View of ISO 27005



www.cs.surrey.ac.uk

ISO 31000 Risk Principles

Risk management should

- create value
- be an integral part of organisational processes
- be part of decision making
- be systematic and structured
- be based on the best available information
- be tailored
- be transparent and inclusive
- be dynamic iterative and responsive to change
- be capable of continual improvement and enhancement

Risk Appetite

Risk Tolerance

- The organisation must decide how it values risk
  - risk seeking or risk adverse?
- Risk appetite refers to the willingness to take risk
  - decides what risk levels to accept
  - risk does not have have to be negative
  - ... high risk may mean huge gain
- FAIR speaks of *risk tolerance*
  - how much risk will you tolerate?
  - indicates that risk is always negative

Assessing a methodology

- Risk analysis is never perfect.
  - depends on approximation and guesswork
- Structure available information
  - emphasise most important pieces of information
- Considering a methodology, FAIR asks:
  - Is it useful?
  - Is it logical?
  - Does it track with reality?

Possibilities and Probabilities

Possiblility is a binary quantity. Either we might lose, or we cannot.

Probability is a continuous measure. A negative outcome be more or less likely to happen, and we may or may not find the probability acceptable.

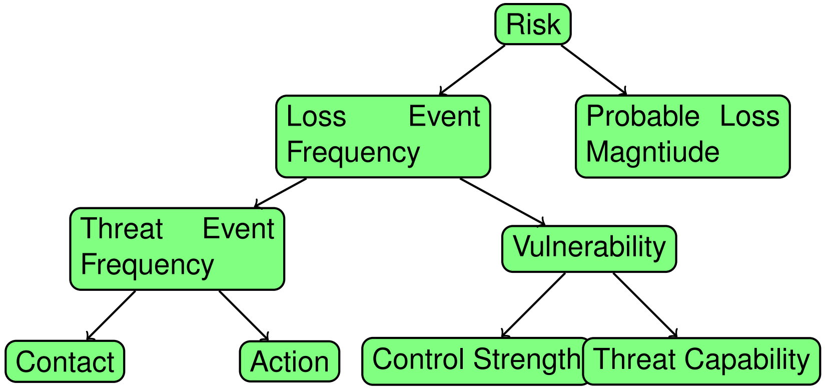
> *Prediction is very difficult, especially about the future.*
>
> *Nils Bohr*

- A security expert will always lose; either
  - waste resources on controls where there is no loss
  - lose when struck by a threat not controlled

Impact

1. Personal Impacts
   - Death, injury
2. Business Impacts
   - Bankruptcy
3. Societal Impact
   - Collapse of social order
4. Geo-Political Impact
   - War
5. Environmental Impacts
   - Global Warming

The FAIR framework



Risk

Loss Event Frequency

Probable Loss Magntiude

Threat Event Frequency

Vulnerability

Contact

Action

Control Strength

Threat Capability

Factor Analysis of Information Risk

- *Quantitative* approach
  - measure probabilities and magnitudes
  - loss measured in USD
  - probabilities or frequencies as incidents per year
- Differs from other, *qualitative* approaches
  - where the focus is *identification* of risks
  - with possible distinction between low, medium, and high
- The quantitative scale used by FAIR
  - assumes a certain size of organisation
  - may require tweaking when you apply it to a one-person business

Key elements

FAIR uses some of our basic terms in a slightly different way

Threat Let's call it a *threat agent*

Vulnerability FAIR considers vulnerabilities only relative to threats, rather than absolute properties of an asset or system. FAIR talks about potential vulnerability when the existence of a relevant threat is uncertain.

Asset objects (items and data objects) of value.

Risk Probable frequency and probable magnitude of future loss

Threat Analysis

Identifying and enumerating various threats and threat agents is a key step in any risk analysis methodology

Threats

Threat Population many threats, related and unrelated

Threat Agent Individual within the threat population

Threat Community Subset of the threat population

Threat Characteristics

FAIR asks the following questions about each threat (agent).

- How often does the threat agent come into contact with our organisation or assets?
- How probable is it that the threat agent will act against us?
- How probable is it that the threat action succeeds?
- What is the probable impact of a successful action?

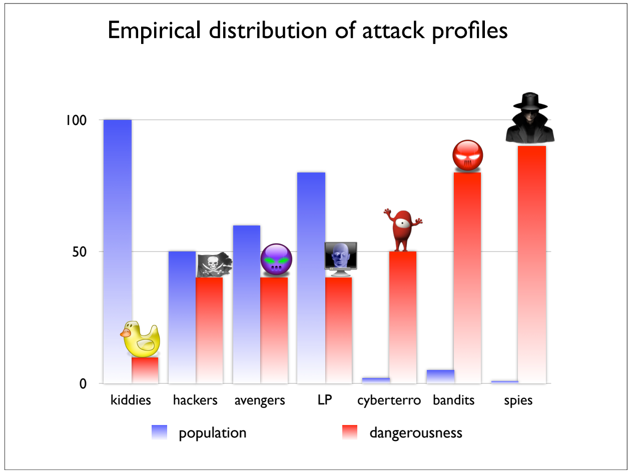
The Seven Cybercriminal Families

A viewpoint from Law Enforcement

- Dr. David Benichou at WIFS'09 in London
  - French *juge investigatoire*
  - Special advisor to the Minstry of Justice
  - PhD in Computer Sciences
- Model based on field experience
  - more than 1000 cases
  - Qualitative rather than quantitative
- Real-life, rather than academic view

The seven families of cybercrime

Seven classes of threat sources (graphics © David Bénichou)



The seven families of cybercrime

- Adolescent amateurs
  - script kiddies
  - hackers
- Amateurs with a goal
  - avengers
  - legal persons
- Resourceful professionals
  - Organised crime
  - Terrorists
  - Spies

The big majority

Script Kiddies
- Clueless amateurs
- Use scripts created by others
- Trying hacks for fun
- No understanding of the techniques used

Hackers
- Technically adept
- Obscure motivations
  - challenge, learning, experience

Masked Avengers

- Grown up individuals
  - with a score to settle
- Obvious motivation
  - relatively easy to unmask
- e.g. a disgruntled employee with a desire to punish the company
- e.g. Mr/Mrs average dragging an ex-lover down in the mud

Legal Persons

- Financial motives
  - unfair competition
  - trade secrets
- Highly skilled
- Easy to identify — the motive is a give-away

The big and resourceful

Spies, organised crime, and terrorists

- Different motivations
  - political (spies)
  - financial (organised crime)
  - ideological (terrorists)
- All are resourceful, with solid backing
  - few have resources on this scale
  - the resources make serious impact possible

The rare and serious agents

- Terrorists
- Spies
- Organised Crime

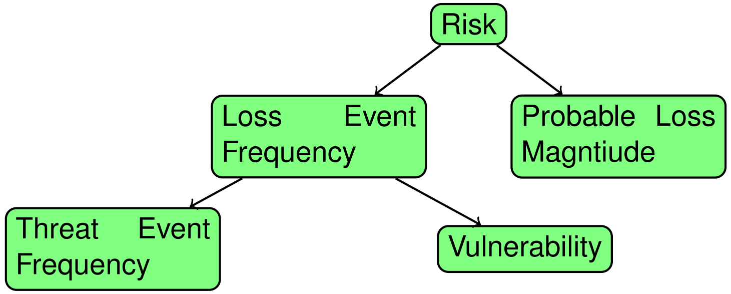
- Backed with considerable resources
  - money, manpower, information, backup
- Different objectives
  - Ideology — Terrorists
  - Politics — Spies
  - Money — Organised Crime
- Similar dedication
  - professionalism and clear objectives

Risk Analysis

How does each family affect your risk analysis?

- Script Kiddies
- Hackers
- Avengers
- Legal Persons
- Terrorists
- Spies
- Organised Crime

Loss Frequency and Loss Magnitude



Risk

Loss Event Frequency

Probable Loss Magntiude

Threat Event Frequency

Vulnerability

Consider Loss Magnitude (Impact) next week.

Loss Event Frequency (LEF)

LEF is the probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset.

LEF decomposed

Loss Event Frequency (TEF) the probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset.

Threat Event Frequency (TEF) the probable frequency, within a given timeframe, that a threat agent will act against an asset.

Vulnerability the probability that an asset will be unable to resist the actions of a threat agent.

Threat Event Frequency (TEF)

Threat Event Frequency is two components

Contact When does the threat agent have an opportunity?

- Random – threat agent stumbles upon the asset
- Regular – the threat agent has access at regular intervals
- Intentional – the threat agent has to seek out the asset

Action When does the threat agent use the opportunity?

- Asset value
- Leevel of effort
- Risk to the threat agent

Vulnerability

- Vulnerability is decided by comparing
  1. Threat Capability — what force can the threat agent muster?
  2. Control Strength — how powerful is our control?

Threat Event Frequency (TEF)

Very High	> 100 times per year
High	10–100 times per year
Moderate	1–10 times per year
Low	1–10 years between incidents
Very Low	less than an incident per decade

Threat Capability (Tcap)

Very High	Top 2% when compared to overall threat population
High	Top 16% when compared to overall threat population
Moderate	Average skills and resources
Low	Top 16% when compared to overall threat population
Very Low	Bottom 2% when compared to overall threat population

Control Strength

Very High	Protects against all but top 2% of threats
High	Protects against all but top 16% of threats
Moderate	Protects against the average threat agent
Low	Only protects against bottom 16% of threats
Very Low	Only protects against bottom 2% of threats

Deriving Vulnerability

		Control Strength				
		VL	L	M	H	VH
Tcap	VH	VH	VH	VH	H	M
	H	VH	VH	H	M	L
	M	VH	H	M	L	VL
	L	H	M	L	VL	VL
	VL	M	L	VL	VL	VL

Deriving Loss Event Frequency (LEF)

		Vulnerability				
		VL	L	M	H	VH
TEF	VH	M	H	VH	VH	VH
	H	L	M	H	H	H
	M	VL	L	M	M	M
	L	VL	VL	L	L	L
	VL	VL	VL	VL	VL	VL

Summary

- The FAIR framework is a fairly readable document
  - proposing a concrete strategy for analysing risk.
- Many different methodologies
  - some qualitative
  - FAIR is quantitative