

Security Risk Assessment – Scales

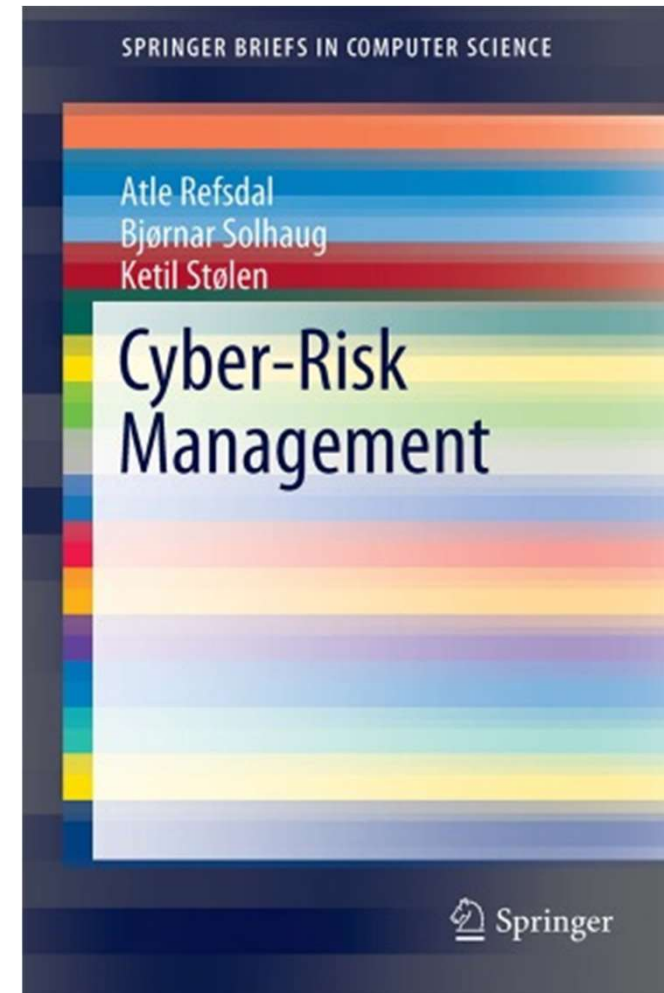
Ketil Stølen

Motivation

- Measurements and estimates are important to priorities risks
- This requires well-designed and carefully thought through scales

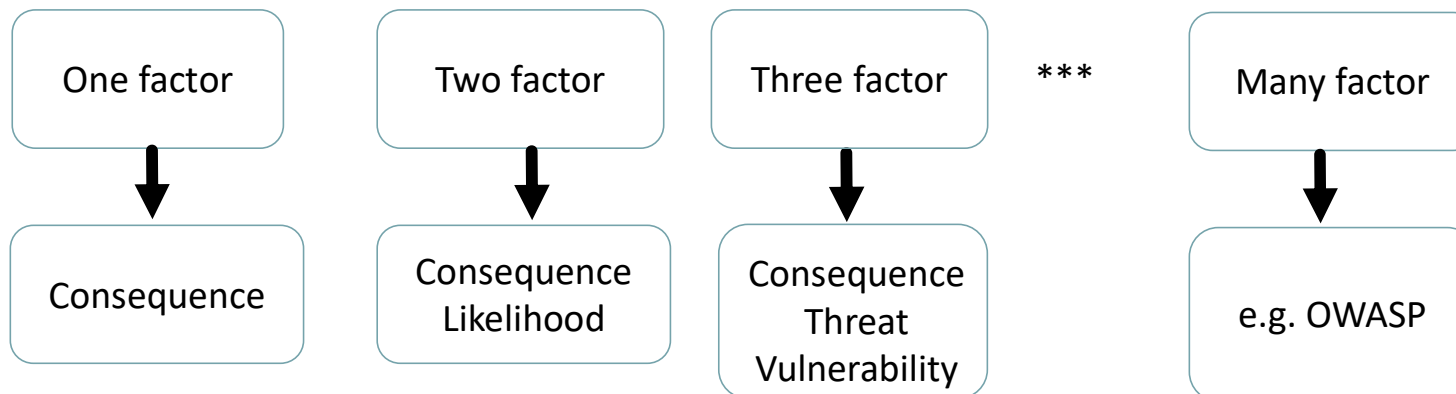
BUT

- What does it mean that a scale is good or well-suited?
- How to select and/or define scales?



See Chapters 11 and 12

Security risk level is a measurement of the seriousness of a negative or harmful potential incident



Independent of the number of factors:

Good and well-suited scales is a prerequisite for a satisfactory result

Is this a good scale?

Likelihood
Guaranteed
Likely
Possible
Unlikely
Rare

With
respect to
what
interval?

What is the real
difference
between
Guaranteed and
Likely?

What is the real
difference
between Unlikely
and Rare?

What about this?

Consequence
Catastrophic
Large
Moderate
Small
Insignificant

Maximal,
minimal,
average?

With respect
to what?

For whom?

And this?

Value	Probability interval
5	0.9-1.0
4	0.7-0.9
3	0.3-0.6
2	0.1-0.2
1	0.0-0.1

Probability with
respect to what?

Is 0.9 equal
to 4 or 5?

What about
2.5?

What kinds of scales are there?

Two main kinds of scales

Qualitative: Values defined or exemplified in natural language

Quantitative: Values defined in such a way that conventional rules calculation are well-defined

To variants of qualitative scales

Nominal scale:

Values correspond to different categories

Ordinal scale:

Values correspond to different categories and these values are ordered

Nominal scale

Activa category	Description
Information	Digital information; in storage as well as under transportation
Software	Source code, binary code, documentation
Hardware	Computer equipment, but also other equipment of relevance
Services	External as well as internal
People	Customers, employees
Immaterial values	Reputation, external trust

Ordinal scale

Consequence	Description
Catastrophic	Leakage of information that can be exploited by terrorists
Large	Leakage of information of legal relevance
Moderate	Leakage of information that may easily be exploited by competitors
Small	Leakage of anonymous information about employees
Insignificant	Leakage of information that to a large extent is public

Things to remember when defining qualitative scales

- Fully exploit the natural language so that the values are easy to understand and differentiate
- Make sure that definitions and formulations make use of words suited for the users of the scale
- Examples are often helpful
- If the scale is ordered this should be reflected in the definitions of the values
- The values should cover the full sample space

To variants of quantitative scales

Difference scale:

Subtraction (and addition) is well-defined

Ratio scale:

Division (and multiplication) is also well-defined

This is a quantitative difference scale – measures the frequency per year

Occurrences	Interval
Real non-negative number	Year

$$5 - 3 = 3 - 1 = 2$$

frequency of 5 - frequency of 3 =
frequency of 3 - frequency of 1 =
frequency of 2

Subtraction is well-defined

The very same frequency scale is also a ratio scale

Occurrences	Interval
Real non-negative number	Year

$$6 / 3 = 2 / 1 = 2$$

frequency of 6 / frequency of 3 =
frequency of 2 / frequency of 1 =
twice as much in frequency

This is also a ratio scale

Value	Description
Non-negative real number	Number of journals leaked

$$6 / 3 = 2 / 1 = 2$$

6 journals leaked / 3 journals leaked =
2 journals leaked / 1 journal leaked =
twice as many journals leaked

A difference scale that is not a ratio scale has a zero value selected "arbitrarily"

Consider three days in a row with maximum temperature 250, 275 and 277.75 degrees Kelvin:

- The increase in temperature from day 1 to day 2 is: $((275-250)*100)/250=10\%$
- The increase in temperature from day 2 to day 3 is: $((277.75-275)*100)/275=1\%$

Consider three days in a row with maximum temperature -23, 2 and 4.75 degrees Celsius. If we do the same calculations we get:

- The increase in temperature from day 1 to day 2 is: $((2-(-23))*100)/-23=-108.695\ldots$
- The increase in temperature from day 2 to day 3 is: $((4.75-2)*100)/2=137.5\%$

Kelvin is a ratio scale, while Celsius is only a difference scale.

BUT can't we just calculate with the numbers we have?

If the arithmetic operations are not well-defined then the utility of the calculation may have to be checked empirically

Example of calculation that requires empirical underpinning

The first step is to select one of the options associated with each factor and enter the associated number in the table. Then simply take the average of the scores to calculate the overall likelihood. For example:

Threat agent factors				Vulnerability factors			
Skill level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1	3	6	9	2
Overall likelihood=4.375 (MEDIUM)							

Next, the tester needs to figure out the overall impact. The process is similar here. In many cases the answer will be obvious, but the tester can make an estimate based on the factors, or they can average the scores for each of the factors. Again, less than 3 is low, 3 to less than 6 is medium, and 6 to 9 is high. For example:

Technical Impact				Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability	Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8	1	2	1	5
Overall technical impact=7.25 (HIGH)				Overall business impact=2.25 (LOW)			

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Things to remember when defining quantitative scales

- Make sure there are no intervals between values
- Avoid overlapping values
- Cover the full sample domain
- Be explicit with definitions and assumptions
- Make sure you are aware of which arithmetic operations are well-defined
- Be aware of that many utility functions require empirical underpinning

Summary

- To measure risk-level we need suitable scales
- Crap-in gives crap-out
- Quantitative is not better than qualitative – what is best suited depends on the case
- Independent of kind of scale, try to be precise