Experiences from Using Indicators to Validate Expert Judgments in Security Risk Analysis

Olav S. Ligaarden[1,2], Atle Refsdal[1], Ketil Stølen[1,2]

[1]SINTEF ICT, Norway

[2]University of Oslo, Norway

MetriSec 2011

September 21, 2011 – Banff, Alberta, Canada

Problem statement

- Expert judgments are often used to estimate likelihood values in a security risk analysis
- The judgments are subjective and their correctness rely on the experts making them
  - Important that the likelihood values are as correct as possible, since they are used together with consequence values to calculate risk values
- Validate likelihood estimates based on expert judgments by the use of indicators based on historical data

Security risk analysis case

- Commercial security risk analysis from 2010
  - Indicators based on historical data were used to validate likelihood estimates obtained from expert judgments
  - The client required full confidentiality
  - Analysis team spent 400 hours on the whole analysis (not including writing the final report)
    - The estimation and validation of likelihood values was conducted as a process of six steps
- Experiences build on
  - Data collected during the analysis
  - Semi-structured interviews with the client experts

Estimation and validation process

Step 1: Expert judgments

Cell phone with sensitive company information is lost/stolen: [[1,4] : 1 year]

Step 2: Identification of indicators / Step 3: Indicator revision

I1: "the number of cell phones reported lost/stolen during the past year"	**30**
I2: "percentage of cell phones synchronizing e-mail"	**0.5**
I3: "percentage of cell phone owners with access to sensitive information"	**0.4**

Step 5: Obtaining indicator values

Step 4: Identification of validation criteria

I1 **x** I2 **x** I3 **in** [[1,4] : 1 year]

Step 6: Revision of expert judgments

30 **x** 0.5 **x** 0.4 = [6 : 1 year] **not in** [[1,4] : 1 year]

Change [[1,4] : 1 year] to [[4,8] : 1 year]

Results from case

Step 1: Expert judgments

Number of likelihood estimates based on expert judgments **28**

Step 2: Identification of indicators

Number of likelihood estimates with at least one indicator **28**

Total number of indicators after Step 2 **68**

Step 3: Indicator revision

Number of likelihood estimates with at least one indicator **25**

Total number of indicators after Step 3 **57**

Challenging to identify indicators for which it is feasible to obtain values within the available time and resources for the analysis

Results from case cont.

Step 3: Indicator revision

Number of likelihood estimates with at least one indicator	**25**
Total number of indicators after Step 3	**57**

Step 4: Identification of validation criteria

Number of likelihood estimates with with a validation criterion	**15**
Total number of indicators used to formulate validation criteria	**19**

Challenging to formulate validation criteria for likelihood estimates in terms of their indicators

Results from case cont.

Step 4: Identification of validation criteria

Number of likelihood estimates with with a validation criterion	15
Total number of indicators used to formulate validation criteria	19

Step 5: Obtaining indicator values

Number of likelihood estimates for which validation criteria could be evaluated	10
Total number of indicators used to formulate validation criteria for which the client experts obtained values	13

Results from case cont.

Step 5: Obtaining indicator values

Number of likelihood estimates for which validation criteria could be evaluated — **10**

Step 6: Revision of expert judgments

Number of likelihood estimates with a fulfilled validation criterion — **4**

Number of likelihood estimates with a validation criterion where it was undecided whether the criterion was fulfilled or not — **2**

Number of likelihood estimates with a not fulfilled validation criterion — **4**

Number of likelihood estimates with a not fulfilled validation criterion for which the likelihood estimates were adjusted — **2**

Indicators can bring forward new information useful for detecting flaws in expert judgments

Conclusion

- 2 out of 28 likelihood estimates were adjusted based on new information brought forward by the indicators

- Main challenges
  - Identifying indicators for which it is feasible to obtain values within the available time and resources for the analysis
  - Formulating validation criteria based on indirect indicators