UDC 501

RISK MANAGEMENT AND ASSESSMENT BY CARRYING OUT THE MULTI-UNIT REVIEW

Y. Tsyba[1, a], A. Arhypov[1]

[1] *National Technical University of Ukraine «Kiev Polytechnic Institute»*

Abstract

The technology behind information systems evolves at an exponential rate, while at the same time becoming more and more ubiquitous. This brings with it an implicit rise in the average complexity of systems as well as the number of external interactions. In order to allow a proper assessment of the security of such systems, a whole arsenal of methodologies, methods and tools have been developed in recent years. This thesis aims at uncovering the differences and limitations of the most common risk assessment models, tools that implement them and describe more complex case of miltiunit review.

Keywords: Risk assessment, information security, multi-unit review, risk analysis models, CVSS, CRAMM

Introduction

Information security is often conceptualized as being the protection or preservation of four key aspects of information: availability, integrity, authenticity, and confidentiality.

Availability: Accessibility of information for a purpose

Integrity: Completeness, wholeness, and readability of information, and the quality of being unchanged from a baseline state.

Authenticity: Validity, conformance, and genuineness of information.

Confidentiality: Limited observation and disclosure of knowledge to only authorized individuals.

The purpose of any risk analysis is providing decision-makers with the best possible information about the probability of loss [1].

Risk management is usually a continuously reiterating process, that typically consists of several activities. Such activities typically include identifying, analyzing and prioritizing risks and finding, evaluating and applying relevant countermeasures as well as monitoring the results. It shows at the figure 1. This process is either continuous or cyclical and focuses on achieving a coordinated and economical application of resources to minimize, monitor, and control the probability and/or the impact of unfortunate events [2].

1. Risk Assessment Methodologies and Tools

The main result of a risk assessment is usually a qualitative or quantitative evaluation of the possible risks that a given complex system is exposed to, taking into consideration its context and likely threats.

It should be noted that most risk assessments, as well as most risk management processes, do not aim at obtaining a fully secure system as this is often impossible.

Fig. 1. Continuous process of risk management

Instead, the end-goal is to reach what is perceived as an acceptable level of security at an acceptable cost.

As a risk analysis result, it is important that decision-makers accept the risk analysis method used, and that information resulting from the analysis should be in a useful form. There are several different approaches to risk analysis, but they can be broken down into two essential types: quantitative and qualitative.

Whether a method is considered quantitative or qualitative stems from its output (i.e. the way risk levels are measured). If the risk is expressed in numbers on a ratio or interval scale, where the difference between any two values is known, then the method can be considered quantitative. If however, risk is evaluated on an ordinal scale (e.g. high, medium, low), where only the ordering amongst values is known, then it is considered to be a qualitative method.

Qualitative risk assessments are descriptive rather than measurable. Purely quantitative methods usually rely on mathematical computations based on various metrics and thus usually require considerable amounts of data. Qualitative methods, on the other hand, could usually be performed within a shorter time, with fewer

[a] eugene.tsiba@gmail.com

resources, less relevant data and require less mathematical, financial and security expertise.

Not all risk assessments are equal. There are obvious variations in approach, scope or applicability; some methods are designed to be used (or usable) as standalone risk assessment methods while others are designed to work in conjunction with more general, enterprise-wide risk management processes [3].

Nevertheless, The common skeleton that most RA methodologies seem to use is the following:

1) Asset identification and valuation. The goal here is to identify and value assets.
2) Threat and vulnerability assessment. The goal here is to assess the CIA risks to assets.
3) Countermeasure selection and recommendation. The goal here is to identify the changes required to manage the CIA risks identified.

For example, CRAMM – is the wide spread Risk Assessment methodology [4] follows a rigid format:

1) Uses meetings, interviews, and questionnaires for data collection.
2) Identifies and categorizes IT assets into one of three categories: 1) data, 2) application/software 3) physical assets
3) Requires you to consider the Impact of the loss of Confidentiality, Integrity and Availability (CIA) of the asset.
4) Expresses Vulnerability (the likelihood that a threat may occur) as: very high, high, medium, low or very low.
5) Expresses Risk (the likelihood that a threat could exploit the Vulnerability) as: high, medium or low.

Actually, when one expert is carrying out a risk assessment is the common and in trivial case. Let's consider the more complicated example when several experts are carrying out an assessment. The main question is how to analyse the output of each expert in the process compare to all output set and how to determine result one?

The answer to this question is describing in the next section.

2. Assessment Processing Results of Multi-Unit Review

Multiple element reviews – a kind of collective expertise, in which involved a group of N experts, each of which carries individual examination of one and the same group of objects. The peculiarity is sufficiently large volumes of objects for which the examination is performing.

In order to understand how to evaluate expert knowledge, it is necessary to get a way to make a numerical representation or calculation on this characteristic. So first of all the problem reduces to constructing of expert knowledge models that will drive process numerical calculations.

To achieve this simulation experiment is developing with the essence of is the artificial reproduction experts sample data. This data is composed of the well-known original values and superposition of noise (expert mistakes). The nature of these mistakes in each different case allows to model one or the other one type of behaviour in the expert examination process.

Large sequences of individual expert evaluations $Z_i, i = \overline{1,N}$ obtained by multi-unit review, among the other, contain specific information about individual capacity corresponding jth expert [5]. It includes a level of its competence, knowledge of which is important for effective treatment of examination results.

If we take into consideration that the obtained expert estimations of N objects can be represented with a matrix:

$$Z = [z_{ij}] = \begin{bmatrix} z_{11} & \cdots & z_{1n} \\ \cdots & \cdots & \cdots \\ z_{m1} & \cdots & z_{mn} \end{bmatrix} = [Z_1, Z_2, \ldots, Z_n]$$

and the value estimates obtained from the jth expert, as

$$Z_i = [z_{1j}, \ldots, z_{mj}]^T$$

we note that each component z_{ij} has a info component x_{ij} and random error e_{ij}.

By analyzing data we can build a model of expert competence in the form of dependence

$$C = a_0 + a_1 X_1 + \cdots + a_n X_1 X_2 * \cdots X_k + \cdots$$

using a value of competence, functionally related to the calculated results of cluster analysis of expert data M-dimensional space with Euclidean metric, where each object classification corresponds to a point with coordinates $z_{1j}, z_{2j}, \cdots, z_{Mj}$ called the image of the j-expert.

To do this, after the allocation of cluster with normal experts coordinates of its centre are determines $z_{10}, z_{20}, \ldots, z_{M0}$ as

$$z_{i0} = \frac{1}{N} \sum_{1}^{N} z_{ij}$$

and then estimates the distance between the centre and image for each of the N experts:

$$r_j = \left[\sum_{1}^{M} (z_{ij} - z_{i0})^2 \right]^{1/2}, j = \overline{1,N}$$

Select the structure of this model in two steps (fig. 2).

First, generate possible options for conversion $c^{(k)} = F_k(r)$ (I step). Second, build competence models by searching the possible variants of models for each c^k (II step).

There are such statistics and their combinations are used to calculate mathematical model of expert competence:

1) Average ratings deviation of jth expert

$$\overline{\delta_i} = \frac{1}{M} \sum_{1}^{M} \delta_{ij}$$

2) Second initial moment

$$\mu_i = \frac{1}{M} \sum_{1}^{M} \delta_{ij}^2$$

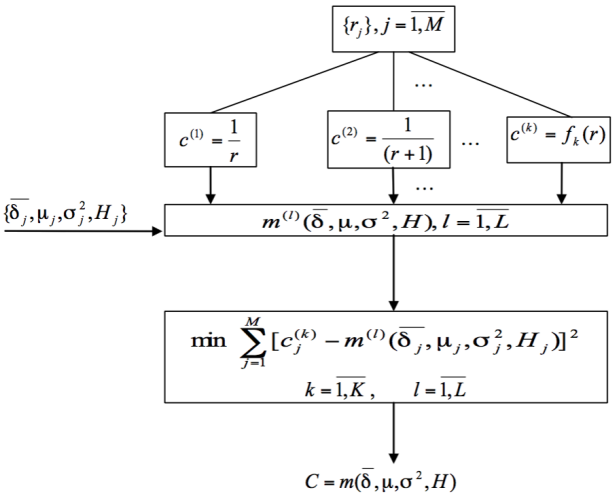

Fig. 2. Expert competence determination procedure

3) Dispersion

$$\sigma_j^2 = \frac{1}{M-1}\sum_{1}^{M}(\delta_{ij} - \overline{\delta_j})^2$$

4) Evaluation of entropy deviations jth expert

$$H = -\sum p_j \log p_j$$

In carrying out of modeling multi-unit expertise within noise blending on actual evaluation objects the values were superposed with errors with different mathematical distributions: normal, a uniform and Laplace. Thus, each had a set of expert estimations over all objects of examination, which consisted of in some real evaluation and estimation errors.

The stepwise regression method was used for identification structure models. As a result of calculations [6] the models are calculated with characteristics satisfying requirements of quality models:

1) The model for normal distribution of noise

$$C = a_0 + a_1\sigma^2\mu + a_2\mu + a_3\mu^2 + a_4\sigma^2\delta$$

, where $a_0 = 0.97, a_1 = 3.3 \cdot 10^{-4}, a_2 = -0.027, a_3 = -2.8 \cdot 10^{-4}, a_4 = -3.3 \cdot 10^{-4}$

2) The model for uniform distribution of noise

$$C = a_0 + a_1\sigma^2 + a_2\delta^2 + a_3\delta\sigma^2 + a_4\delta H$$

, where $a_0 = 0.985, a_1 = -0.02, a_2 = -0.025, a_3 = -6 \cdot 10^{-4}, a_4 = 1.5 \cdot 10^{-5}$

3) Laplace distribution model

$$C = a_0 + a_1\mu + a_2H^2 + a_3\sigma^2$$

, where $a_0 = 0.98, a_1 = -0.03, a_2 = 0.02, a_3 = -0.002$

3. Results Handling of Multi-unit Review Regarding Risk Assessment

As stated earlier there are two fundamental types of risk assessment. Quantitative risk analysis applies mathematical and statistical tools to represent risk. Qualitative risk analysis methods perform risk analysis with the help of adjectives, not mathematics.

The methodology can be adapted to either qualitative or quantitative risk assessment. The scenario of analysis and subsequent risk-measurement activity are specifically well-suited to qualitative assessment. In a quantitative risk assessment, both tasks could be automated calculations, based on asset values, frequency of vulnerability exploitation, and probability of successful attack.

The qualitative approach does not utilize any mathematical tools or statistics for the risk model, so therefore the outputs of the remote method depend on the ideas of those who undertake risk analysis. There can be a subjective decision about risk when the risk was analysed with a qualitative method

Let's back to the question when several experts are carrying out an assessment and how to analyse the output even with a set of qualitative values?

In this case, we are dealing with two subquestions. First, how to obtain clear measurements of multi-unit review. It means result set of scores has values without assessments of the expert in case expert has a some bias towards review objects. Second, output result should represent quantitative value to manage it.

Our helper in at least one question above is CVSS standard.

Common Vulnerability Scoring System (CVSS) - is a free standard (and tool) which attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. Scores range from 0 to 10, with 10 being the most severe.

CVSS is the last developed approach to measuring security vulnerabilities and also could be used as risk assessment methodology [7]. Moreover, it has correspondence table with qualitative or quantitative values.

Qualitative value	Quantitative value
None	0
Low	0.1—3.9
Medium	4.0—6.9
High	7.0—8.9
Critical	9.0—10.0

Table 1. Correspondence between qualitative or quantitative values

Next point we should handle result processing to avoid irregular experts scores. Irregular experts are experts with own competence less than the average in the review. To do it we can use discovered approach in section 2 and calculate competence for every expert. Then just reject ones with unreliable competence.

Representation on the processing flow shows at the figure 3.

Summary

There was reviewing several methodologies of risk assessment and management.

Variations often arise from different interpretations of these methods. Differences can also occur in the

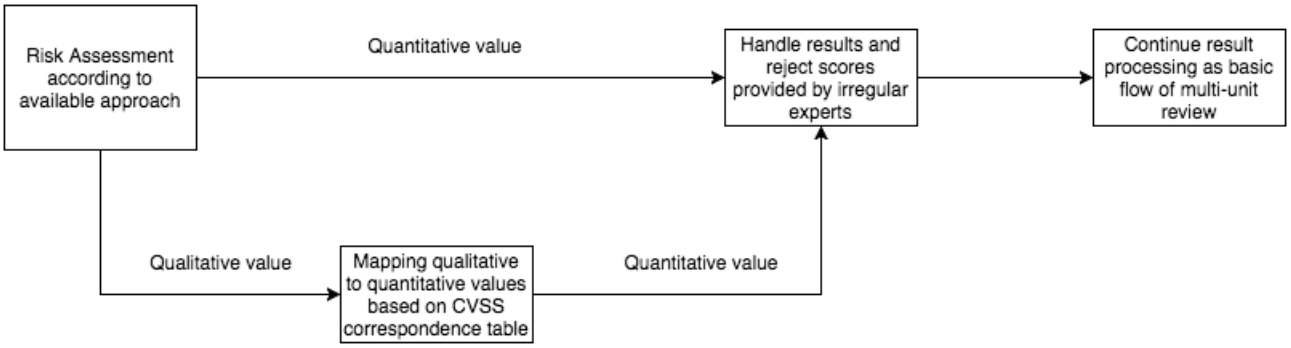

Fig. 3. Representation of risk assessment processing flow of multi-unit review

number, meaning and relationships of the factors driving risk, as well as how they could be operationalized, measured and computed in order to quantify risk in a meaningful way.

Processing and result handling of the risk assessment was touched. Also, it includes more complicated case – a multi-unit review.

As a result of the analysis and data processing of expert interviews, the model of expert competence was introduced. It can significantly simplify the procedure for evaluating competence. Particularly, it enables a direct calculation required a score of a set of expert data.

Considered the possibility of expert estimation of the data quality obtained in the examination process.

There are few models are developed for evaluation of expert competency.

It is obvious that the use only one model of expert competence is not a silver bullet to solve the problem of abnormal experts presence.

A more prudent approach to its solution based on the use of several model forms and designed for their estimations experts competence.

References

1. Shukla Neeta, Kumar Sachin. A Comparative Study on Information Security Risk Analysis Practices // Special Issue of International Journal of Computer Applications. — 2012. — no. 0975-8887.
2. Hampton J.J. Fudamentals of Enterprise Risk Management, Second Edition: How Top Companies Assess Risk, Manage Exposure, and Seize Opportunity. — 2014.
3. Ionita Dan. Current Established Risk Assessment Methodologies and Tools. — 2013. — P. 123.
4. Marquis H. 10 Steps to Do It Yourself CRAMM // Do-it-yourself Guides. — 2008. — no. 4.50.
5. Arhypov A., Arhypova S. Expert assessment quality by data carrying out on multi-unit examination // Information security. — 2011. — № 4(53).
6. Tsyba E., Arhypov A. Identification of expert competence model based on multi-unit review data with different types of noise distributions // Theoretical and applied problems of physics, mathematics and information science. — 2015. — № 15. — С. 213–216.
7. FIRST. Common Vulnerability Scoring System v3.0: Specification Document. — 2015. — URL: `https://www.first.org/cvss/specification-document`.