Risk Analysis supported by Information Security Metrics

Jakub Breier, Peter Hofbauer, Ladislav Hudec

Abstract: *This work presents motivation for using metrics as an instrument for the risk analysis. There are information security standards, like ISO 27000 family, which serve as a reference for risk analysis and assessment, however there is a lack of formal methods and some discrete-scale evaluation. The main goal of this work is to propose the metric - control objective mappings, so the chosen metrics will help the management decide whether the control objectives are fulfilled or not. We present a mathematical model of evaluation based on metrics, which should lead to more automatized risk analysis.*

Key words: *Risk Analysis, Computer Security, Security Standards, Security Metrics, Security Model*

INTRODUCTION

The importance of assuring the security of information assets is becoming more critical every year. The discussion about information security issues is necessary for business enterprise and companies are becoming aware of it. However the key areas of information security risk management and risk metrics still do not receive enough attention. Despite lots of documents describing the managed approach to risk, they do not clearly define a proper risk analysis and assessment. There exists ISO standards which explain the theoretical risk analysis approach and provide generic guidance on choosing security objectives, like the ISO 27000 standards family, however they do not describe the practical aspects and they fall short when evaluating the sufficiency of security mechanisms in a formal way. The situation of knowledge base has improved in a past few years; however there is still need of standardization in a whole risk assessment process.

In this paper we propose a formal model for the quantitative risk assessment with the usage of measures and metrics, which minimizes the subjective factors of the security evaluation. This model is designed to make the risk analysis process more automatized, so it could be easily repeated and the results should be consistent and comparable.

SECURITY METRICS

At first we have to define the term *security metric*. Information security is a process of providing confidentiality, integrity, availability, authenticity and non-repudiation to some entity according to some policy. It protects information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction [1].

A metric is an abstract subjective attribute derived from measurement. Metrics measure the attributes of entities [2]. With proper metrics we can improve decision making, performance and accountability in organization. We can differentiate between two attribute types: internal and external. Internal attributes characterize the entity itself, external attributes are the actions performed by the entity operating in some given environment [6]. From the top-level point of view we can evaluate whether the chosen metric is relevant by measuring the return on security investment (ROSI), which is based on implemented security mechanism. Those mechanisms are directly or indirectly dependent on used metrics and their results. According to [5] good metrics should be consistently measured without subjective criteria, cheap to gather, preferably in an automated way, expressed as

a cardinal number or percentage, expressed with at least one unit of measure and finally contextually specific and relevant to decision-makers.

SECURITY CONTROLS

There are several security frameworks, which can be used to quantify the effectiveness of security controls in an organization. These frameworks usually tell us how to implement reporting and accountability controls to get the demanded information about security processes. Four most popular frameworks are following [5]:

- *Control Objectives for Information Technology (COBIT)[7]:* COBIT provides a set of best practices which are useful for organizations implementing IT governance and control. COBIT 4.1 defines thirty-four high-level processes, covering over three hundred control objectives, categorized in four domains. The 4.1 revision of COBIT was published in 2007.
- *ISO/IEC 17799 (ISO/IEC 27002)[8]:* This standard is entitled Code of practice for information security management. It provides best practice recommendations on information security management in order to initiation, implementation and maintaining Information Security Management Systems (ISMS). Eleven security control clauses containing a thirty-nine security categories and one clause introducing risk assessment and treatment are introduced in this standard. Information security controls and objectives are described in each section and for each security control is provided implementation guidance. The latest revision was released in 2005, expecting the next version in 2011.
- *Information Technology Infrastructure Library (ITIL):* This framework contains a set of practices for the Information Technology Service Management. It is much more general than previous frameworks; it does not focus only on security topics. There are nine topic sets in this standard. ITIL Security Management describes fitting of information security in the management of the organization and it is based on the ISO/IEC 27002. The latest revision, ITIL v2, was released in 2009.
- *US NIST SP 800 Series:* The United States National Institute of Standards and Technology presents a set of documents about information security under the Special Publication 800 Series. SP 800-18 and SP 800-80 specify seventeen high-level security control families. SP 800-30 introduces risk management guidelines for information technology systems.

CONTROL OBJECTIVES SUPPORTED WITH METRICS

In the ISO 27000 series we can find a set of control objectives which can be chosen for the organization. These objectives usually include the assurance of confidentiality, integrity and availability of organization's assets.

When selecting which metrics to use within an organization, the metric should contribute in some form to the security objectives, which we have to fulfil. The ability to apply a security metric is dependent on organization's individual capabilities [3]. The security capabilities can represent the connection between security objectives and metrics. In order to determine the most adequate metric for the given objective we need to evaluate the possible metrics candidates with respect to given capabilities.

When assessing risks, we can view on this model from another perspective. We can choose a control objective, from ISO/IEC 27002 for example, and select security metrics, which can be used to evaluate, if the control objective is fulfilled. This perspective is illustrated in figure 1. We have to choose a proper subset of metrics, which will support the control objective and assign a weight to each metric in the subset, so it can be decided, which metrics are most important for the chosen objective. One metric can support more control objectives with different weights for each of them. If one or more metrics from the

subset is not available or difficult to obtain, we can omit it and reassign the weights in the subset.

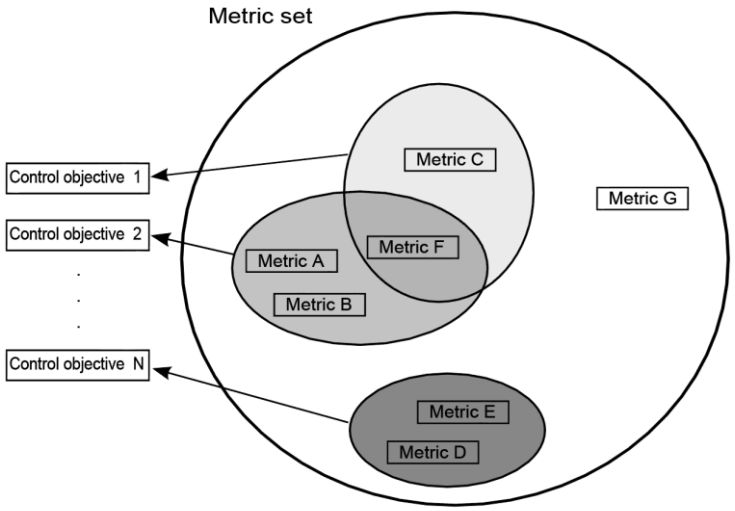

Figure 1: Control objectives and metrics.

In tables 1 and 2 there are proposals for the metric-control objective mappings for the Information security policy category within the Security policy clause and for the Responsibility for assets category within the Asset management clause from the ISO/IEC 27002.

Table 1: Information security policy category with proposed metrics.

Control Objective	Metric	ID	Weight
Information security policy document	Percentage of employees with the awareness of the security policy document	ISPD 1	40%
	Number of security briefings per annum	ISPD 2	40%
	Percentage of employee job descriptions specifying responsibility for following the corporate security policy	ISPD 3	20%
Review of the information security policy	Security policy violations per annum	RISP 1	50%
	Number of reviews per annum	RISP 2	50%

Table 2: Responsibility for assets category with proposed metrics.

Control Objective	Metric	ID	Weight
Inventory of assets	Percentage of assets in inventory	IA 1	30%
	Percentage of assets with classification	IA 2	30%
	Percentage of IT security budget in comparison to the assets value	IA 3	40%
Ownership of assets	Percentage of assets with responsible owners	OA 1	100%
Acceptable use of assets	Number of reviews of the rules defining the acceptable use of assets per annum	AUA 1	60%
	Number of shortcomings identified in the rules per annum	AUA 2	40%

FORMAL MODEL

To obtain the desired results which will give us the evaluation of the security clauses listed in standard we have to make the formal model. We can think of each of the security clauses as a sub model with the state and a quality function. The goal is to determine

whole eleven states of sub models, which will tell us the security state of the company from the view of ISO/IEC 27002 standard supported with metrics.

First of all we have to determine the metric parameters, which will be persistent through the whole evaluation process and the variables, which will be dynamic:

- Parameters:
  O_i = Optimal value of the metric *i*
  W_i = Worst value of the metric *i*
- Variables:
  M_i = Value obtained by measurement of the metric *i*
  E_i = Weight of the metric *i* according to the selected control objective

The optimal value means that we will obtain the best results if the measurement value reaches this point, so even if the result is better than the optimal value for the metric, it will no further affect the result. This is illustrated in figure 2, where the optimal value is 20%, so the resulting value raises until it gets to it and then it stays constant.

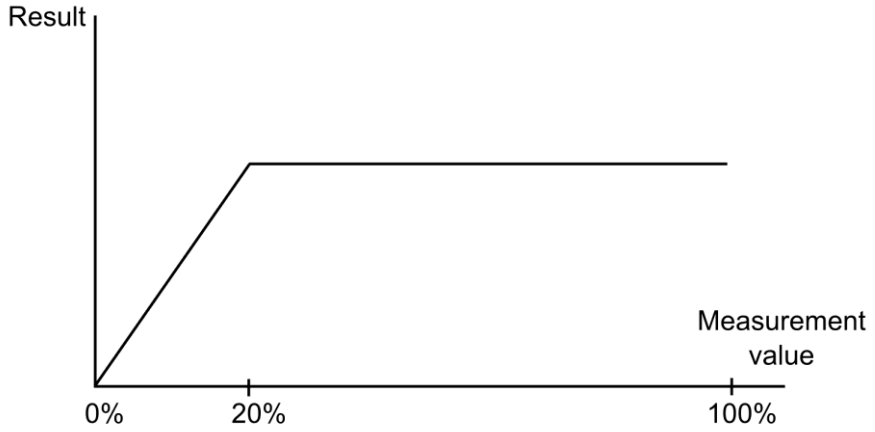

Figure 2: Effect of the optimal value. X-axis holds the measurement value, y-axis holds the resulting metric value in percentage.

Next points we need to include to our model are the company parameters. Some metrics may take those parameters as arguments or they can be involved when computing the optimal or the worst value which can the metric gain.

- Company parameters:
  C_E = Company size (number of employees)
  C_B = Annual budget for information technologies

Now we can define the quality functions for each control objective, which will involve the metric parameters and variables. There are thirty-nine control objectives in the latest revision of the standard and it would be space-consuming to list all of them, so we will define just the first of them for the better understanding of this approach. The metric identifiers are listed in table 1.

- Information security policy document:
  - Specifications (listed in table 3):

Table 3: ISPD control objective metric characteristics.

Metric ID	Optimal value (O_i)	Worst value (W_i)	Weight (E_i)
ISPD 1	100%	0%	40%
ISPD 2	3	0	40%
ISPD 3	20%	0%	20%

- Quality function:

$$Q_{ISPD} = \frac{M_1}{O_1} \times E_1 + \frac{M_2}{O_2} \times E_2 + \frac{M_3}{O_3} \times E_3 \quad \textbf{(I)}$$

The quality function (equation I) simply divides each measured value by the optimal value and multiply it by the metric's weight.

- Review of the information security policy:
  - Specifications (listed in table 4):

Table 4: RISP control objective metric characteristics.

Metric ID	Optimal value (O_i)	Worst value (W_i)	Weight (E_i)
RISP 1	0	C_E / 10	50%
RISP 2	2	0	50%

  - Quality function:

$$Q_{RISP} = \left(1 - \frac{M_2}{W_2}\right) \times E_2 + \frac{M_1}{O_1} \times E_1 \quad \textbf{(II)}$$

The quality function of this control objective (equation II) is slightly different in this case, because the optimal value of metric RISP 1 is zero so we use the worst value in the expression.

To show how the partial metrics affect the final evaluation of the control objective, we can observe one variable, which changes its values and other variables consider as constants and vice versa. In figure 3 we can see the impact of metrics RISP 1 and RISP 2 on the Review of the information security policy control objective. In the first graph the RISP 1 metric acquire values from interval [0,20], C_E = 200 and the other metric has a constant value of fifty, in the second graph the RISP 2 metric has values 0,1,2 and the other metric has again a constant value of fifty.

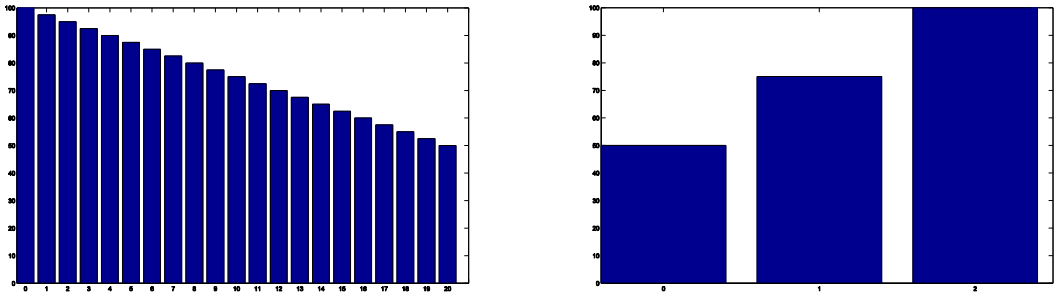

Figure 3: Observation of RISP 1 and 2 impact on evaluation. X-axis holds the metric values, y-axis shows results of control objective quality function

When we have the results of the partial quality functions, we can evaluate the whole security clause by using the weighted sum model. The resulting quality function is the arithmetic mean of weighted partial quality functions. To illustrate this approach we will use the Security policy clause quality function (equation III).

$$Q_{SC} = \frac{1}{n} \sum_1^n Q_n \times CE_n \quad \textbf{(III)}$$

Where Q_n is the security category quality function and CE_n is the weight of this function in the model space.

CONCLUSIONS AND FUTURE WORK

In the previous sections were described information security metrics, their usefulness and effectiveness in evaluating the organization's security. We introduced a formal model with mathematical background, which brings more objectivity to the risk assessment process and should minimize the subjective impact brought by security analysts. We hope that this approach will make the risk analysis easier to perform and the results will be clearer with the formal background.

The most difficult part is to choose the metrics from these collections, couple them with the control objectives from ISO/IEC 27002 and assign them adequate weights. The mappings examples proposed in this paper have to be done to all of the eleven security clauses from the standard. The weights of the particular metrics have to be further discussed so they could reflect the real significances of the measured objects in accordance to control objective properties.

In the future work we would like to determine all the metrics, which could be used for the risk analysis based on ISO 27000 family standards. This determination has to emanate from real experiences with the usage of metrics. There are few metrics databases on the internet and recently were published books [4], [5] which discuss the security metrics and lists the most useful and meaningful metrics to use within organizations. There should also be a model validation and comparison with the actual risk analysis methods after a complete design of the metric mappings.

REFERENCES

[1] 44 Code of Laws of the United States of America, § 3542.

[2] N. Fenton and S. Pfleeger. Software Metrics: A Rigorous and Practical Approach. International Thomson Computer Press, 1997.

[3] Christian Fruehwirth, Stefan Biffl, Mohamed Tabatabai, and Edgar Weippl. Addressing misalignment between information security metrics and business-driven security objectives. In Proceedings of the 6th International Workshop on Security Measurements and Metrics, MetriSec '10, pages 61–67, New York, NY, USA, 2010. ACM.

[4] Lance Hayden. IT Security Metrics. McGraw-Hill Osborne Media, 2010.

[5] Andrew Jaquith. Security Metrics: Replacing Fear, Uncertainty, and Doubt. Addison-Wesley Professional, 2007.

[6] Nwokedi C. Idika. Characterizing and Aggregating Attack Graph-based Security Metrics. PhD thesis, College of Science, Purdue University, 8 2010.

[7] IT Governance Institute. Cobit 4.1. ISA, 2007.

[8] ISO. ISO/IEC Std. ISO 17799:2005, Information Technology - Security Techniques - Code of Practice for Information Security Management. ISO, 2005.

ABOUT THE AUTHORS

Mgr. Jakub Breier, Institute of Applied Informatics, Faculty of Informatics and Information Technologies STU in Bratislava, Phone: +421 948 752 069, E-mail: breier@fiit.stuba.sk

Dr. phil. Ing. Peter Hofbauer, SIMEA Corporation, London, +43 680 236 9066, E-mail: peter.hofbauer@simeac.com

Assoc.Prof. Ladislav Hudec, PhD, Institute of Applied Informatics, Faculty of Informatics and Information Technologies STU in Bratislava, Phone: +421 (2) 60 291 243, E-mail: lhudec@fiit.stuba.sk