Quantitative method of information security risk assessment by multicomponent threats

Raikhan Muratkhan and Dina Zhagiparovna Satybaldina

L. Gumilyov Eurasian National University, Munaitpasov str., 5, Astana, 010000, Kazakhstan

Abstract. Traditionally, information security risk is defined as a combination of the probability of adverse events and their possible consequences. But the risk of the security disturbance of the modern organization is a multidimensional complex concept that also includes a set of interrelated variables. The paper proposes a combined approach to assess the risk of occurrence of information security events based on an ontological description of the subject area and a quantitative method of risk assessment of implementation of multicomponent threats using more than a single vulnerability. The example of assessment of risk of information security is considered in accordance with international standards and preferences of the owner of information resources.

[Muratkhan R., Zhagiparovna S.D. **Quantitative method of information security risk assessment by multicomponent threats.** *Life Sci J* 2014;11(11):372-375] (ISSN:1097-8135). http://www.lifesciencesite.com. 61

Keywords: Risk, information security, method of risk assessment

Introduction

Organizations which business depends largely on the information sector, to achieve business goals should maintain at the required level information security management system (ISMS) [1]. Today many companies are coming to the fact that the ISMS should be built on the basis of generally accepted norms and accumulated international practices, including international standards [2-4]. In the dome of rules on management of information security [2] to form a comprehensive requirements to the information security three main indicators are marked out:

- Assessment of the risks which are faced by the organization (through the definition of threats to assets, vulnerabilities of assets and the probability of threats and possible damages);
- Compliance with legal, regulatory and contractual requirements that must be implemented by the organization, its business partners, contractors and service providers;
- The formation of a set of principles, objectives and requirements to the processing of information, designed by the organization to support its activities.

Standards [3,4] define the system of information risk management as a key element of the ISMS and using process model, describe an iterative approach to the risk assessment. However, the standards do not contain recommendations on the selection of a unit of risk assessment, as well as the synthesis of the measures, security tools and services that are used to minimize the risk that reduces the usefulness of standards as technical documents. In connection with this works become relevant for the development of risk - oriented security model of business processes, methods and algorithms of the qualitative and quantitative risk assessment of information security and the development on the basis of them software tools.

Mathematical apparatus of risk assessment is based on the information security methods of probability theory, which is due to the probabilistic nature of the uncertainty of the risk factors forming. The formula for calculating risk is most often a product of three parameters:

$$R = V \cdot P(T) \cdot AV \quad (1)$$

where *V*-measure the vulnerability of the asset to the threat;

AV-value of the asset;

P(T) - the probability of the threat.

The disadvantage of this approach is that it does not take into account a situation where one has several active threats or a threat uses several vulnerabilities. In this paper, we propose a method for quantitative risk assessment of threats implementation by the confidentiality, integrity and availability of the assets based on the calculation of several levels of threats that exploit some specific vulnerabilities. The paper also uses ontology of subject area of risk management information security systems, which helps to identify vulnerable assets, security objectives, assess risks and identify security measures to mitigate these risks.

2. Ontology of subject area of risk management

Ontology defines a common vocabulary for researchers who need to share information in a subject area; it includes machine-interpretable formulation of the basic concepts in the subject area and the relationships between them [5]. Concept could be a description of the problem, function, action, strategy, etc. The relationship between the classes and subclasses of the concepts is organized as a directed graph which vertices correspond to the concepts of the subject area and the arcs (edges) define the relationship between them. Classes and subclasses have properties (attributes).

In this paper we use the ontology of security risk management information systems ISSRM (Risk Management Information Systems Security), proposed by the authors [6].

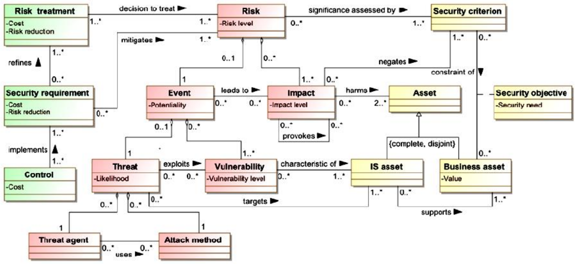


Figure 1. Model ISSRM [Mayer and Dubois et al.]

Ontological model ISSRM (see Figure 1), describes three different conceptual categories.

Concepts related to the asset, describe the organization's assets are divided into current assets and business information systems (IS) assets. They also determine the criteria for security restrictions as business assets, expressed as integrity, confidentiality and availability.

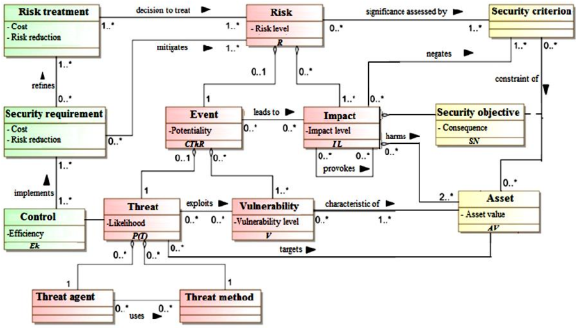


Figure 2. Modified model ISSRM

The concepts of risk, determine the potential harm to the business. They include the threats that contain one or more vulnerabilities in the case of their successful implementation; they damage the system assets, a negative impact on assets, defined as an influence. The event is the union of a threat and vulnerability, where vulnerability is a weakness in the system that can be used by a source of threat. The threat is a way of applying the attack. Source of threat - it is attacker who initiates a threat of harm to IS assets. Method of attack is the means through which the source of the threat carries a threat.

Concepts associated with the processing of risk, determine a treatment decision risks to avoid, reduce, retain or transfer potential risks. They specified security requirements. Controls implement security requirements.

In the modified model ISSRM in each frame the title of concepts are written on the first line, and on the second – measure and on the third line - marking of the calculation formulas.

3. Proposed risk assessment method

The method is based on a model of the threats used in the software product "GRIF 2006" of Digital Security [11].

Compliance with the ontology of the subject area (see Figure 2) the vulnerability of the asset is estimated by the measure of vulnerability to the threat, and the threat – by the probability that a threat through this vulnerability. Asset value of the measure of vulnerability to the threat and the probability of the threat through the vulnerability expert estimates and indicates in levels from 0 to 1.

At the first stage calculate threat vulnerability based on criticality and probability of threats through vulnerability. The calculation is performed using the formula:

$$Th = V \cdot P(T), \qquad (2)$$

where *Th* - the level of threat vulnerability.

Meaning the level of threat vulnerability obtain in the range from 0 to 1.

In order to accommodate the controls, modify the formula (2) and the probability of threat will count as follows:

$$Pk(T) = \frac{P(T)}{C \cdot Ek}, \qquad (3)$$

where *Ek* - the level of efficiency of introduced countermeasures. The level of the effectiveness of introduced countermeasures expert estimates and indicates in the range from 0 to 1. Coefficient $C = 10$ is needed in order to get the value of the level of threat vulnerability in the range from 0 to 1.

To calculate the level of threat to all vulnerabilities, which can be realized through the threat of an asset, sum received threats' levels via specific vulnerabilities according to the formula:

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th). \qquad (4)$$

Values of the level of threat to all vulnerabilities get in the range from 0 to 1. Similarly, considering all the threats acting on the asset, we expect the overall level of threat on an asset or event acting on the asset:

$$CThR = 1 - \prod_{i=1}^{n} (1 - CTh). \qquad (5)$$

The value of the level of threats to assets is in the range from 0 to 1.

In accordance with the subject area to calculate the level of risk of the asset using the possibility of the event and the level of exposure (Fig. 2):

$$R = CThR \cdot AV, \qquad (6)$$

where IV - exposure value is determined as follows:

$$IV = AV \cdot SN, \qquad (7)$$

where AV - the value of the asset (see Figure 2),

SN - a consequence of the vulnerability of the asset.

Asset value and consequence for the asset is estimated and indicated by an expert in the range of 0 to 1.

The result is the risk value of the asset in the range from 0 to 1.

4. Return of the investment invested in the information security

Information security risk management is coming to reduce the quantities of high and medium risk to low risk specific to the point where perhaps their adoption. To do this, you want to apply countermeasures. The stronger security countermeasures are difficult for malicious activity, the more successful we can assume their choice. As a formalism that supports this approach, it is advisable to use attack graphs whose vertices are labeled possible countermeasures and their quantitative economic evaluation in terms of defending and attacking. [8]

A one-time damage to the resource will be determined by the formula:

$$SLE = AV \cdot V, \qquad (8)$$

where AV - value of the resource, which includes all kinds of its costs (installation, maintenance, etc.) and V - a measure of the vulnerability of the asset to the threat.

Since not all threats are equally, we introduce the probability of the threat (*P(T)*). Then the expected annual damage from this threat will be calculated by the formula:

$$ALE = SLE \cdot P(T). \qquad (9)$$

Assessing the significance of *P(T)* can be based on statistical analysis of information security disturbances.

The economic effect of the countermeasures (i.e., spending on information security) can be estimated by the formula:

$$ROSI = (ALE \cdot Ek - CSI) / CSI, \qquad (10)$$

where *Ek* – coefficient of the reduction rate risk as a result of the implementation of countermeasures (lies in the range from 0 to 1) and *CSI* - the cost of implementing countermeasures. With a positive security regulator ROSI implementation of the security regulator is economically justified; otherwise, it makes no sense. ROSI is a tool for the economic evaluation of the effectiveness of the (defensive) organization in the field of information security. The aim is to maximize the value of ROSI.

ROSI criterion allows to evaluate the effectiveness of both single and multiple events and helps to reduce information security risks, and to assess the degree of risk reduction for classes of threats.

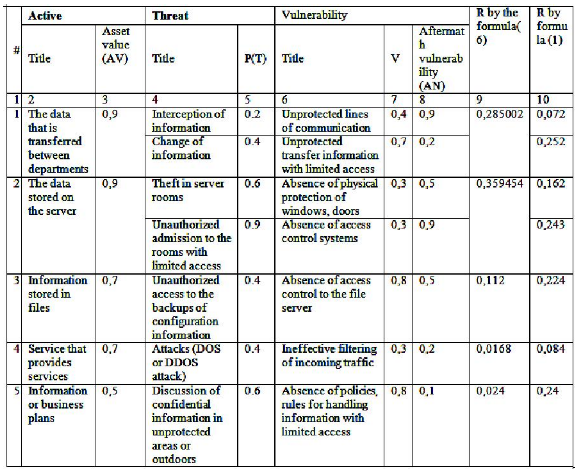
5. Results and discussion

Based on the information entered by the owner of the data, you can build a model of threats and vulnerabilities relevant to the company's information system. On the basis of the model, the expert assesses the probability of the threat, a measure of vulnerability to the threat and the value of the asset, based on this, information security risks will be calculated (Table 1).

To reduce the level of the risk it is proposed to apply countermeasures. When applying countermeasures the probability of threats through vulnerability decreases.

After the introduction of countermeasures expert evaluates the effectiveness of countermeasures introduced (Table 2, column 7) and formula (3) evaluates the probability of a threat after the introduction of countermeasures. After that, according to the formula (6) and (1) again will calculate the level of information security risk.

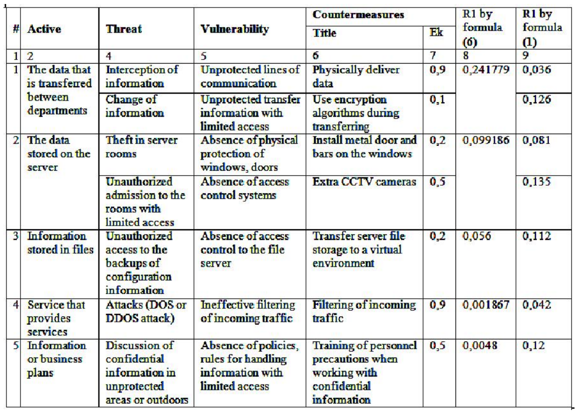
Table 1. Entered data experts and the resulting of risk level IS



#	Active		Threat		Vulnerability			R by the formula(6)	R by formu la (1)
	Title	Asset value (AV)	Title	P(T)	Title	V	Aftermath vulnerability (AN)		
1	2	3	4	5	6	7	8	9	10
1	The data that is transferred between departments	0,9	Interception of information	0.2	Unprotected lines of communication	0,4	0,9	0,285002	0,072
			Change of information	0.4	Unprotected transfer information with limited access	0,7	0,2		0,252
2	The data stored on the server	0,9	Theft in server rooms	0.6	Absence of physical protection of windows, doors	0,3	0,5	0,359454	0,162
			Unauthorized admission to the rooms with limited access	0.9	Absence of access control systems	0,3	0,9		0,243
3	Information stored in files	0,7	Unauthorized access to the backups of configuration information	0.4	Absence of access control to the file server	0,8	0,5	0,112	0,224
4	Service that provides services	0,7	Attacks (DOS or DDOS attack)	0.4	Ineffective filtering of incoming traffic	0,3	0,2	0,0168	0,084
5	Information or business plans	0,5	Discussion of confidential information in unprotected areas or outdoors	0.6	Absence of policies, rules for handling information with limited access	0,8	0,1	0,024	0,24

As can be seen from Table 1, if one asset is influenced by several threats and one threat uses several vulnerabilities, then get a real risk of an asset by the formula (1) is difficult (see the intersection of line 1.2 column 9 of Table 1). That’s why; by the classical method we obtain two risks on the one asset. As one asset is influenced by two threats, that by the proposed method we obtain a risk for one asset (see the intersection of line 1.2 column 8 of Table 1). If one asset is influence by only one threat, and it uses only one vulnerability, whereas our method corresponds to the classical method of risk assessment (see the intersection of line 8.9 3,4,5 columns of Table 1).

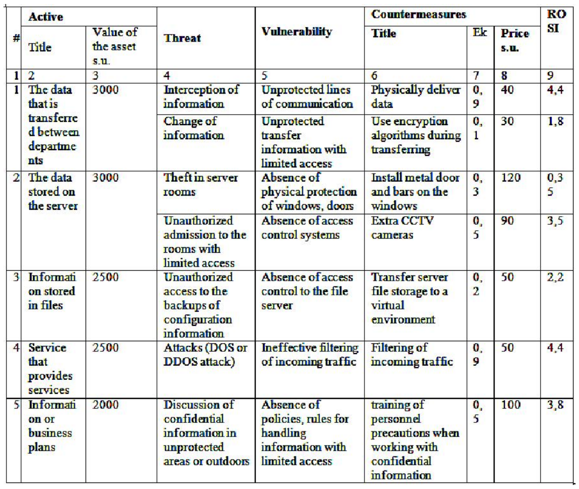
Table 2. Risk level after the introduction of countermeasures



#	Active	Threat	Vulnerability	Countermeasures		R1 by formula (6)	R1 by formula (1)
				Title	Ek		
1	2	4	5	6	7	8	9
1	The data that is transfered between departments	Interception of information	Unprotected lines of communication	Physically deliver data	0,9	0,241779	0,036
		Change of information	Unprotected transfer information with limited access	Use encryption algorithms during transferring	0,1		0,126
2	The data stored on the server	Theft in server rooms	Absence of physical protection of windows, doors	Install metal door and bars on the windows	0,2	0,099186	0,081
		Unauthorized admission to the rooms with limited access	Absence of access control systems	Extra CCTV cameras	0,5		0,135
3	Information stored in files	Unauthorized access to the backups of configuration information	Absence of access control to the file server	Transfer server file storage to a virtual environment	0,2	0,056	0,112
4	Service that provides services	Attacks (DOS or DDOS attack)	Ineffective filtering of incoming traffic	Filtering of incoming traffic	0,9	0,001867	0,042
5	Information or business plans	Discussion of confidential information in unprotected areas or outdoors	Absence of policies, rules for handling information with limited access	Training of personnel precautions when working with confidential information	0,5	0,0048	0,12

Proposed formula for calculating the probability of the threat through vulnerability takes into account the effectiveness of the introduced countermeasures. In the case of the risk reduction the effectiveness of implementation of countermeasures plays an important role. Because, with the introduction of countermeasures it is necessary to consider not only the reduction of the risks and return on the investment embedded in the IS (see Table 3), which will get a economic basis of the use of protective measures that will eventually lead to budget savings for organizations and businesses.

Table 3. Example of calculating return on investment embedded in IS



#	Active		Threat	Vulnerability	Countermeasures			ROSI
	Title	Value of the asset s.u.			Title	Ek	Price s.u.	
1	2	3	4	5	6	7	8	9
1	The data that is transferred between departments	3000	Interception of information	Unprotected lines of communication	Physically deliver data	0,9	40	4,4
			Change of information	Unprotected transfer information with limited access	Use encryption algorithms during transferring	0,1	30	1,8
2	The data stored on the server	3000	Theft in server rooms	Absence of physical protection of windows, doors	Install metal door and bars on the windows	0,3	120	0,35
			Unauthorized admission to the rooms with limited access	Absence of access control systems	Extra CCTV cameras	0,5	90	3,5
3	Information stored in files	2500	Unauthorized access to the backups of configuration information	Absence of access control to the file server	Transfer server file storage to a virtual environment	0,2	50	2,2
4	Service that provides services	2500	Attacks (DOS or DDOS attack)	Ineffective filtering of incoming traffic	Filtering of incoming traffic	0,9	50	4,4
5	Information or business plans	2000	Discussion of confidential information in unprotected areas or outdoors	Absence of policies, rules for handling information with limited access	training of personnel precautions when working with confidential information	0,5	100	3,8

The results can be extended in the next stages of research by analyzing a large number of business models and security events. Future research is related to the development of special software tools of risk assessment. Expert assessments will be processed by methods of statistical processing of fuzzy data [9,10].

Corresponding Author:
Dr.Muratkhan Raikhan
L. Gumilyov Eurasian National University
Munaitpasov str., 5, Astana, 010000, Kazakhstan

References

1. Koller G. and R. Koller, 2007 Modern Corporate Risk Management: Blueprint for Positive Change and Effectiveness. New York: J. Ross Publishing, pp: 272.
2. ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls.
3. ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements.
4. ISO/IEC 27005:2008. Information technology. Security techniques. Information security risk management.
5. Gruber, T. R. Toward principles for the design of ontologies used for knowledge sharing. International. J. of Human-Computer Studies, 43(5-6): 907–928.
6. Mayer N., 2009. Model-based Management of Information System Security Risk. PhD thesis. University of Namur.
7. Kukanova N. Methods rate risk GRIF 2006 from Makeup Digital Security Office www.dsec.ru/ipm_research_center/article/risk_assessment-_method_vulture_2006_from_the_composition_of_the_digital_security_office/?sphrase_id=406
8. Kashchenko A.G., 2007. Evaluating the effectiveness of measures to reduce the risk of information security. Informatsia i Bezopasnost', 3:511-513.
9. Bojadziev G. and M. Bojadziev, 1997. Fuzzy Logic for Business, Finance, and Management, World Scientific, Singapore.
10. Ngai E.W.T. and F.K.T. Wat, 2005, Fuzzy decision support system for risk analysis in e-commerce development, Decision Support Systems 40, pp: 235–255.

7/1/2014