

## HOW TO CALCULATE INFORMATION VALUE FOR EFFECTIVE SECURITY RISK ASSESSMENT

**Mario Sajko, Kornelije Rabuzin, Miroslav Bača**  
Faculty of organization and informatics, Varaždin, Croatia  
{mario.sajko, kornelije.rabuzin, miroslav.baca}@foi.hr

---

**Abstract:** *The actual problem of information security (infosec) risk assessment is determining the value of information property or asset. This is particularly manifested through the use of quantitative methodology in which it is necessary to state the information value in quantitative sizes. The aim of this paper is to describe the evaluation possibilities of business information values, and the criteria needed for determining importance of information. For this purpose, the dimensions of information values will be determined and the ways used to present the importance of information contents will be studied. There are two basic approaches that can be used in evaluation: qualitative and quantitative. Often they are combined to determine forms of information content. The proposed criterion is the three-dimension model, which combines the existing experiences (i.e. possible solutions for information value assessment) with our own criteria. An attempt for structuring information value in a business environment will be made as well.*

**Key words:** information value, security risk assessment, information evaluation.

---

### 1. INFORMATION VALUE AS A RISK FACTOR

As a part of the information system (IS) risk management process, risk assessment was first mentioned in 1974 when the *Federal Information Processing Standard (FIPS)* issued the publication *Automated Data Processing Physical Security and Risk Management*. According to many authors [6; 9; 10; 13; 15; 16; 21; etc.], risk assessment is a pre-condition and a key component of risk management, which is fundamental in choosing effective security measures. Authors also regard risk assessment as the first stage of the IS risk management process in which security measures are used to identify the effects on the determined risk. The determined risk size is an indicator of required security or indicator needed for cost protection management. The relationship between investments and risk when discussing security management is delineated in Figure 1 (higher investments result in lower risk).

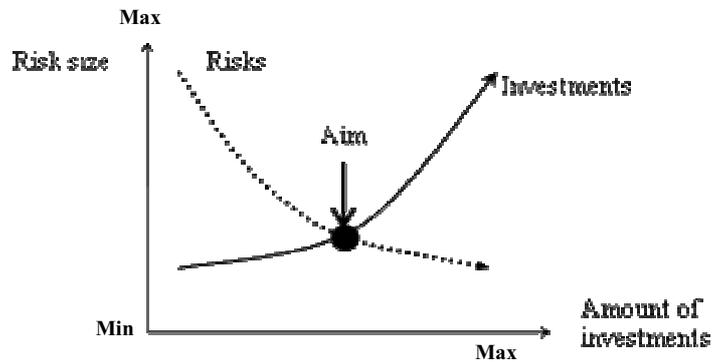


Figure 1: Diagram of risk and cost proportion

Despite the changes and new ideas in the field of risk assessment, even today risk assessment concepts are based on the *NIST* standard (*National Institute of Standards and Technology*) consisting of six factors [28; 29]:

$$\text{Risk} = f \{ \begin{array}{l} \text{Security threats,} \\ \text{Property value,} \\ \text{Threat influence probability,} \\ \text{Property exposure to threats,} \\ \text{Threat influence on property,} \\ \text{Existing security} \end{array} \}$$

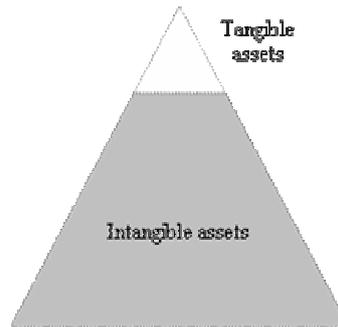
According to the *NIST* concept, security risk is calculated by combining these factors and their assessment of the influence on some of the *IS* features. Some other information risk assessment approaches can be found in [4; 5; 7; 10; 13; 14; 15; 16; 21; etc.], but there is still no general agreement about risk factors.

As a factor of risk function, values of *IS* asset are also present. Their value derives from the ability to create new values, new products and knowledge, and the ability to offer the services of a business, which is using them. *IS* property or assets can be divided into intangible property (knowledge, information, data etc.) and tangible property (equipment and other physical assets). According to *Guide to BS 7799 Risk Assessment and Risk management* [14], *IS* assets are:

- Tangible assets (Computer equipment, computer network, media, portable electric wires, etc.),
- Intangible assets (Databases, system documentation, user manuals, operative procedures, plans etc.),
- Paper documents (Contracts, instructions, business documentation, business results etc.),
- Software (application and systemic software, developmental tools and supporting tools),
- Image and company reputation,
- Services (Computer and communication services, other services for process support) and

- Knowledge.

Currently, we are all witnesses of the growing interest for intangible *IS* assets. Nowadays there is increased growth in the structure of *IS* property, as well as more influence from it on businesses' success, especially in the field of the business information where its share of total assets "is threatening" to become a bigger share, as it is shown in Figure 2. It is rather difficult to determine their value under these circumstances, and usually it is determined subjectively, which is problematic.



**Figure 2:** The proportion of visible tangible and invisible (visible with more difficulty) intangible *IS* assets

Actual literature explicitly avoids answering the question of how to estimate information value. The value of intangible assets, although considered very important, is regularly neglected and is usually subjectively estimated, which is not a good base for decision-making. Even today, there are few papers written on the subject [1; 16; 18; 22], in which we cannot find appropriate kind of presentation of information values or even implementation example. Because of that, the aim of this paper is to determine the information value dimensions, to work out the problems of their assessments, and determine a new way of how to evaluate information value in the context of security risk assessment.

## **2. DISCUSSING DIMENSIONS OF INFORMATION VALUE AND ITS INFLUENCE ON A BUSINESS PROCESS**

Evaluation and determination of intangible assets value is an open problem in determining the size of security risk. The fact that some information is more important or interesting does not explain much to the manager who needs to invest in security. Because information value needs to be determined more precisely it is necessary to understand its appearance, manifestation, activity methods and structure of its value. The problem is stimulated because of a need for a unique and understandable method of evaluation that could also be suitable for the security risk assessment process.

The reason for difficulties in *IS* assets evaluation is that information, data and knowledge do not have exactly determined values and their effect on the business results is not completely understandable. Problems derive from the fact that information cannot be understood or determined by physical evidence or size [8]. It is immaterial and without any physical qualities, despite the fact that it exists as a physical transcription.

Despite the fact that the quantity of information content can be calculated by measuring the uncertainty that is eliminated in the system, during the evaluation of its business value the aim is not to determine physical quantity of transferred or saved content. The quantity does not operate with the quality and meaning of content, so that is the reason why we

cannot use Shannon and Weaver's mathematical theory of entropy. It neglects content and its meaning [24].

### *2.1. EFFECTS AND INFLUENCE OF INFORMATION ON THE BUSINESS*

Generally speaking, information appears when a line of arranged and recognisable signs with meaning, presenting a feature of a certain object or reality, is organised in a meaningful form, and it is something new for a receiver. In a business, the content, which is a function of the realisation of business aims, becomes business information. Business information mostly serves as a basis for making decisions, but it also is used for keeping and supporting business processes, facilitating communication between employees, etc. It can be particularly interesting if information has to be withheld, or if it presents an indirect financial value.

Different from other tangible *IS* assets, information as an asset can be recognized as product designs, technical data, management instructions, operative data, operative processes, technical data, employee knowledge, computer software [8], working instructions, business results and reports, data basis, systemic documentation, user manuals, operative procedures, plans, application and systemic software, developmental and supporting tools etc. Human potentials, such as intellectual property and know-how, are also included [25].

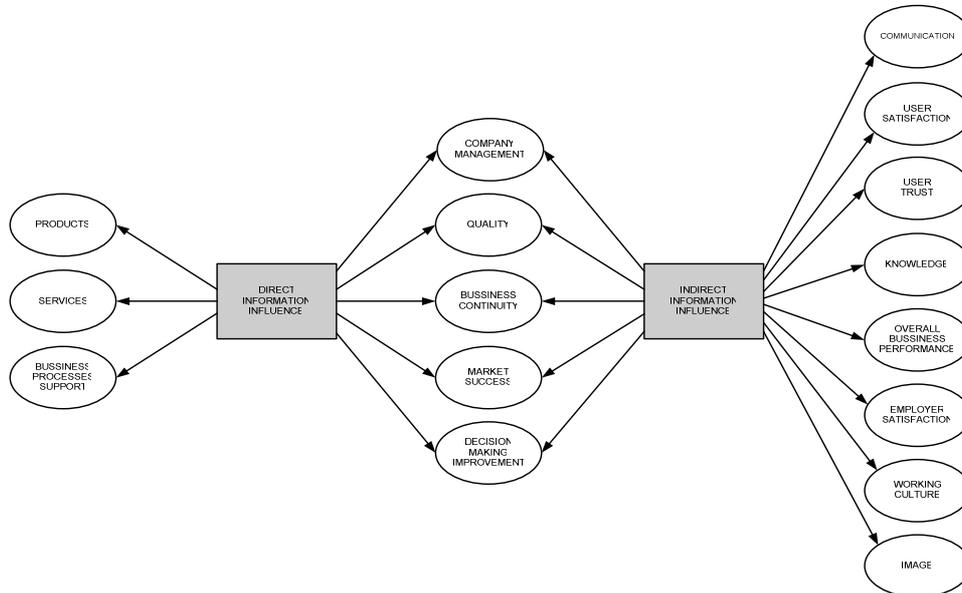
In business systems, information is a strategic resource [18], which is key to running a business. Information's are one of the biggest business values, the basic source of income earnings and motive power for creation of a new value [19]. For Moody [19], information is important in all businesses, and particularly in decision-making, improving system performance, and achieving market success and in supporting working processes. Lawlor [17] stresses the role of information and communications as well. In each case, information is accepted as an instrument of change, and an instrument of formalising and managing a business environment [11].

Considering the mentioned information characteristics, information in a business will take affect (as is shown in Figure 3.):

1. INDIRECTLY- when information is tied to products/services and
2. DIRECTLY - when it supports secondary activities, human needs, technology, organisation and technical infrastructure.

In order to ensure that information affects the business, the necessary prerequisites need to be present, which are:

- Content and quality of information,
- Features of information,
- Form and holder,
- Knowledge and experience of a receiver and
- Conditions in which they are exchanged.



**Figure 3:** Direct and indirect information influence on business process

Reeker J. [24] suggests that the influence of information also depends on:

1. Which symbols and/or information forms are used and the way they are organised,
2. Meaning that is attributed to the symbols and
3. Application of the information in the system that appears as a result of understanding the transferred meaning

The influence that is produced by information, knowledge and data is usually identified with financial values, but it is only one of the forms of influence it has on the system. The forms of information that can be capitalised on the market (e.g. Patents, recipes, designs, secret contracts, plans etc.) can have a direct financial value. The value of these forms of information can be quantitatively expressed as a proportion of the possible capitalisation on the market. In proportion to this, the risk of their threat is calculated. Together with a quantitative value, information can have other values that cannot be expressed in financial terms. Such a value form is qualitative and it can be more outstanding than the quantitative one. In other words, many aspects, such as employees processing information and the conditions in which a business organisation works, determine the information value.

## 2.2. STRUCTURING AND EVALUATING THE INFORMATION VALUE

When considering different forms of information impacts on the business, the following information features have to be taken into account: (1.) information value is growing with use, (2.), the information value is not stable, (3.), the information value is growing with own accuracy, (4.) the information value is growing when it is combined with other information, (5.) quantity is not a value and (6.) information value does not drop with use [19]. According to [18], information value increases with the use of information, with its accuracy and relationship with other assets and information value decreases if it is outdated, inaccurate, inaccessible or overloaded.

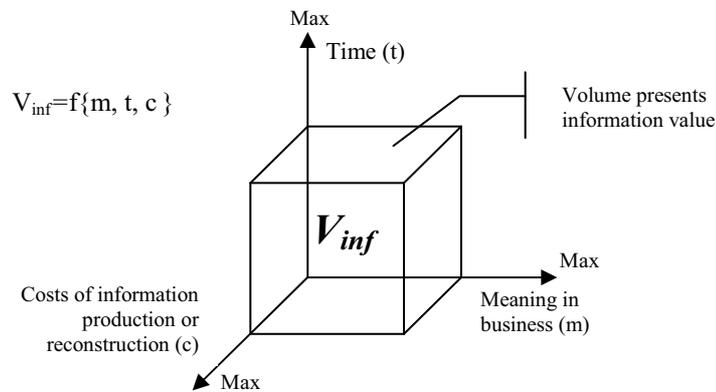
As a solution for determining multidimensional information value, Cramer [8] suggests that the evaluation criteria should be developmental, working, collective and incorporate

marketing efforts. A similar approach is proposed by Moody and Walsh [19]. In their opinion, information property values can be determined if the use and possibilities for selling information are considered. On the basis of this suggestions information value can be explained through three basic paradigms (1) Cost (*Cost or Historical Cost*), (2) Market value (*Market or Current Cash Equivalent*) and (3) Utility (*Utility or Present Value*). Poore [23] has similar ideas and considers six conditions to estimate the value of information for the purpose of risk management. Besides expenses which occur during the (re)construction of information, Poore stresses that for the estimation of the information value the exclusive possession (exclusively owned information or asset) is very important as well.

By comparing and interpreting those suggestions for the evaluation of information content values, it has been established that basic information is being valued via its:

1. Meaning to the business
  - Profits evaluation (For functions, processes and decisions in which information appears as a moving force) and
  - Utility (feature of information to produce required effects)
2. Cost defining - that appear in order to produce, buy, reconstruct, change or compensate for information)
3. Time - only the accurate information will have the potential to create changes

By including those dimension, we have a model that can be shown in a three-dimensional diagram (Figure 4.), and the function of information value is the same in this case.



**Figure 4:** Dimensions of information value

But, there is still a question of how to express the size (amount) of multidimensional information value. In practical situations, an assessor combines possibilities of particular security risk analysis methods (like COBRA, BSI Guide, OCTAVE, CRAMM, NIST, FRAP, RuSecure, etc.) with historical data, and his/her knowledge and intuition. The methods being used depend on the methodology that is applied. Since the 1980s, there have been two basic methodologies (and their combinations) utilised in security risk assessment:

1. Qualitative (Based on descriptions or ranging),
2. Qualitative (Based on numeric calculation) and
3. Combinations of these basic principles are also possible.

### 3. BASIC APPROACHES FOR INFORMATION VALUE EVALUATION

In documented cases, these methodologies have been evaluated differently [10; 16; 20; 21; etc.], and results and the effectiveness of information value assessment depend on the choice of methodology. Although recently the interest for qualitative methodologies has become more outstanding because of the focus on the evaluation of *IS* intangible assets, it seems that the most suitable method of evaluation is somewhere between the two basic principles. After all, qualitative methodology itself possesses a quantitative component, which has resulted in the existing methods using the best features of both methodologies.

A particular form of assessment characterises the way in which information values are joined to qualitative/quantitative intensities or sizes in certain dimensions. These intensities are indicators of value in which the combination of total information value can be achieved. What have also been observed in the process of assessment are problems in determining the type of indicators sizes (like currency units or different forms of quantitative scales) to best represent the information.

Quantitative assessment is suitable in determining asset value, which has a direct financial value as licences, patents, designs, and knowledge bought on the market or made by the proper actors.

Their financial value is shown during purchasing or it can be determined by the production price. It is harder to determine the value of information not bought on the market or that appears during the business process (indirect information value). Qualitative assessment makes understanding the importance of information evaluation simpler. The overview of characteristics of two basic methodologies is given in Table 1.

Information value forms	Meaning	Assessment form	Assessment features	Value derives from
Directly measurable	Value can be expressed in financial terms. Information is bought or appears as a product of someone's intellectual work that can be financially evaluated. Very often information present a basis for producing new knowledge, product or services.	Quantitative	- complex calculations, often incomprehensible, long-lasting, demands software support, nonstandardized procedure; values are financially determined, better security management, good basis for costs analysis, results are comprehensible	Value can be determined in terms of appearance costs, replacement or reconstruction costs and possibilities for capitalisation of information on the market
Indirectly Measurable	Information value is mostly described as a qualitative and subjective size: It contributes to a more successful business and even if positive effect of information is clear, it is hard to be determined.	Qualitative	- simple, comprehensible, relatively short-term, subjective, does not deal with financial sizes, does not give any basis for cost/profit analysis and determining security measures, it is not possible to follow system performance	Value derives from importance for business processes and functions, importance for an individual and his work, importance for business objectives, needs for filling and documenting

**Table 1:** Forms and features of value assessment of information content

Possibilities for the use of different analytical procedures depend on the support for combining and calculating components of information values in sizes and intensities that present the basis for determining required security. Also, their utilities depend on the level of support for the assessor to abstract a larger amount of different information features

according to their character and turn them into a meaningful form. In other words, the assessment methods are suited differently depending on the use of qualitative and quantitative metrics that are used to express and demonstrate the components of information value. Two dominant forms of metrics that are often combined in practice are outstanding in this case and will be explained in following sections.

**Table 2:** Metrics of value assessment of information content

Metric	Meaning
Financial value	expresses the relation cost/profit in clear variables possible; it can be applied to all propriety and security measures, supports mathematical and statistical calculations, can make assessment more difficult
Weak, medium, strong; one, two three, (1, 2, 3)	metric is clear, the group of rules for categorisation or recognition of intensities levels should be arranged; it can be applied to all the elements of risk metrics, it does not require much time; notions are comprehensible; calculations are simple; rough intensities division makes it inflexible, cost/profit analyses are not supported
One, two, three, four , five (1, 2, 3, 4, 5); key, critical, important, reliable, informative etc.	supports five levels of importance; successfulness of this metrics depends on subjectivity of criteria definition that determines a particular level; it offers bigger flexibility, does not demand much time, calculations are rather simple, it is useful if financial value of assets is unimportant or unknown; it can be applied only to value assessment, result is subjective, does not support cost/profit analysis.

In the next part, what is proposed is the use of a few processes and techniques combining different dimension and forms of information value. For quantitative assessments determining information value through cost and the categorisation of value by numerical intensities are used. For qualitative assessment, value ranking by describing intensities and the subjective evaluation method will be used.

### 3.1. QUANTITATIVE ASSESSMENT

The most direct procedure of quantitative assessment relates to the utility of information evaluation through their financial values (purchase, reconstruction or capitalisation on the market). There are two forms of assessment. The first, which is financial assessment, can be used only for information assets characterised by mainly direct importance. For such an assessment each piece of information whose value is directly proportional to its financial value (licences, patents, original designs, projects, and prescriptions) is suitable. It can be written as follows:

$$V_{\text{direct}} \approx F_{\text{value}} \quad (\text{value} \approx \text{financial value})$$

If the importance cannot be directly expressed as a financial value, assessment is more complex. In that case, indirect values can be expressed as a loss/cost that appears when we do not have complete information. More indicators such as the possibility of discontinuing the process or service, profits for other subjects (concurrence, market value of information, costs of reconstruction) and delays, which appear because of non-existent information should be considered.

$$V_{\text{indirect}} = \{ \begin{array}{l} \text{Value for a business organisation,} \\ \text{Value for other business organisations,} \\ \text{Cost of reconstruction of assets,} \\ \text{Time dimension (property duration)} \end{array} \}$$

Each of the listed components is then described by financial sizes or they can be decomposed as sub-elements as follows:

1. The value for a business *{The absence of information reflected on business, the obligation to keep information. The consequences for an organisation if it losses it}*,
2. The value for other businesses *{what happens if the rival has this information}*,
3. Cost of the reconstruction of assets *{How much will it cost to replace or reproduce that information?}* and
4. Time dimension (property duration) *{How long should the information be kept? Does its value decrease over time?}*.

In the process of assessment, the defined level of subjectivity can be eliminated via group methods or repeated decision-making. The result of such an assessment is a financial value that determines the limit of investment in information security.

Another way for quantitative assessment is the categorisation of the importance by numerical intensities (Table 3.). The procedure of assessment is simpler in this case, as the scale of importance used to describe information importance consists of only three, five or seven degrees. Instead of using financial values, value is determined by joining information to the determined value group according to determined features of the group. Each value group is joined to descriptive and numerical intensity points or values. (E.g. on a scale from 1 to 5, where the value “1” is the lowest and “5” is the highest). In Table 3, numerical equivalents are used to mark a particular group defined by a relative information value.

**Table 3:** Example of descriptive expression of similarity intensity

<b>Intensity</b>	<b>Meaning</b>
1	Information is without any economic value and value for the process, so it can be replaced with minimal costs
2	Information is interesting and in this matter costs appear. Their loss has a small influence on business
3	This information is important but replaceable, but costs are higher. Loss of information has medium-serious consequences on business
4	Information is particularly important for business and its destruction can have serious consequences on a business organisation
5	The most valuable information whose information value is even bigger that their market value. The loss of information has multiple influences on a business organisation.

If it is necessary to have a completely different range of values for determining security cost, the intensity scale can be changed. Such assessment is suitable for information with

direct financial and indirect values. But the assessment results themselves are more imprecise. The obtained values do not determine required investment in security. Due to this, it is recommended to determine security measures consistent with intensity values.

Although it is a less precise method, it is much easier and faster to carry it out, and it can satisfy less demanding systems. On the other hand, the most dangerous threat to this assessment is subjectivity.

### 3.2. QUALITATIVE ASSESSMENT

In qualitative assessment, a larger number of participants can be included to achieve a more objective assessment. In an assessment process, we can use different forms of graphic scales in which qualitative (descriptive) value intensities (important, medium important, unimportant) are pointed out. The intensities of evaluation are scarce and graded, and evaluation itself is mostly based on the experience of the assessor. The biggest imperfection of this approach is neglecting the financial value, which is hard to express with a determined qualitative intensities or levels of similarities as well as expressing high subjectivity in assessment.

As the basic possibilities for qualitative assessment, we should point out unavoidable techniques for group decision-making (brain writing, brainstorming and Delphi) that can be combined with previously described approaches for quantitative assessment. Here we illustrate structural techniques for determining scenarios (what-if methods) that are based on individual or group brainstorming. As table 4 shows, *What-if* analysis is an analytical process structured to direct the assessor to think about the information results (and consequences) on business. Logical thinking about information influence is set up in this way, leads the assessor, and the result itself describes the importance of the information and potential size of the loss that is then turned into qualitative intensities.

**Table 4:** Example of “What-if” analysis

What-if	Condition of evidence	Consequences	Security measures	Potential loss	Character of loss	Size of losses
Because of an error on the magnetic disc some accounting data disappear.	Tech. error; Sabotage; Bad maintenance; Lack of knowledge.	Impossibilities for selling and supplying in a period of one day Demand for employees engagement on data reconstruction jobs	Data reconstruction from the spared magnetic disk; data reconstruction form analogous data carriers.	2 men/day; credibility at buyers and suppliers; increase of uncertainty in its own powers; bad working climate.	Direct (financial); Indirect.  Potential medium sizes.	small <10.000 US\$
What if an employee illicitly discredit some data about salaries	Employee is not satisfied with conditions. Employee wants to receive profit for himself or for the others	Revealing of business secret; Dissatisfaction of other employees; Unauthorised change of salaries; Theft of financial assets.	Cryptography; Physical protection to the approach; Passwords.	loss of credibility; bad working climate; loss on the image; fluctuation of employees.	Indirect.  Potentially medium sizes.	big > 50.000 US\$

Some potential events (ex. loss of information) as well as some consequences deriving from it can be determined by applying this method. Structuring the problem graphically and determining cause-and-effects makes producing scenarios and discovering possible dangers easier. In this method, it is easier for the assessors to determine information values, but the problem of assessment subjectivity is substantial. Conditionally, such an assessment can be used as an analytical method during the quantitative assessment of indirect values if the presumed size of loss is expressed in financial terms.

The second way of qualitative assessment is the “value matrix”. It classifies business information based on its importance (strategic, tactical, operational and personal information). It is also classified based on age of information (is it old, medium-old or new information?). The assessment process includes association of the information with two assessment dimensions. The obtained result is a descriptive (qualitative) intensity of information importance. The marks, which are used in the value matrix, (Figure 5) are:

- V - very valuable information,
- M - medium valuable information and
- L - less valuable information.

Losses are the third dimension, but by increasing the number of assessment dimensions, the time of assessment is increased too. Inserting the third dimension achieves all three components of information value stated in Figure 4. Also, it is possible to include a higher number of assessment intensities, but more than seven is not recommended. The use of the value matrix can be combined with the techniques of group decision-making. So, as can be seen in Figure 5, strategic information, which is new, is very valuable; on the other side, older information is almost meaningless to the business.

strategic	L	V	V
tactical	L	M	V
operative	L	M	M
personal	L	L	L
	old	medium old	new

**Figure 5:** Information content value matrix

#### **4. OUR EXPERIENCES IN EXPRESSING INFORMATION VALUE**

Concerning the our experience in implementation of a particular type of metric and expression of information value during risk assessment in business practice, a few problems have been found. The two of them are particularly highlighted.

The first one concerns the limitations of a particular metric contained in actual risk assessment methods. In other words the authors of this method foresee the unified metric for all risk factors, so for further coordination and calculations of assessment results it is not possible to use different metrics. In that, what is mostly used is qualitative metric and value

ranks with (3 or 5 similarity levels) or already mentioned matrix values. Quantitative assessment is rarely possible and it is valid mostly for licences, contracts or patents.

The second problem concerns the tendencies so called *stakeholders* (person who places a particular value on assets or, who use its value[25]) to a particular assessment form. The *stakeholders* which are usually assessors have different tendency toward qualitative, descriptive, quantitative and graphic forms of expressing risk size. That is the reason why it seems useful to carry out experimental assessment the aim of which is to examine tendencies of the assessor before the beginning of “real” assessment.

In such assessment, it is necessary to highlight a few typical intangible assets of clear value and at least one value which is more difficult to assess. The preliminary assessment is carried out individually and on this occasion the assessors use all the offered metrics for risk assessment from the sample.

Such procedure has been carried out on the sample of 4 companies. As a metric for expressing value were used:

- Descriptive scale (free language)
- Qualitative scale (rank of 3 or 5 intensities in whole numbers)
- Graphic (one -dimensional value scale or two-dimensional matrix)
- Relative importance according to some referential value
- Financially expressed value

Except these possibilities for assessment, an new metric based on the questionnaire of 5×5 questions (Table 5.) considering different dimensions of information value was formed.

**Table 5:** Questionnaire for assessment of information value

Dimensions	Questions	Scores
Lost	What happens if we do not have this information any more	
	Nothing special	0
	Some processes are late, but not essentially	1
	Its imperfection is noticeable, but replaceable	2
	New unnecessary costs appear without information	3
Bigger halt and wrong decisions are threatening – new urgent production is necessary	4	
(Re)building	Cost of replacing information or production of the new one	
	Negligibly small	0
	Cost exists but it is low	1
	Higher costs appear	2
	Cost is hardly tolerable	3
Intolerably high costs	4	
Market value	What happens if the competitor has the same information	
	nothing	0
	competitor has all unimportant information about our company available	1
competitor has insight in our important business processes	2	

	competitor can reach the company	3
	competitor gets competitive advantage	4
<b>Legislative</b>	Is there any obligation for keeping information and consequences for organisation if it losses it	
	It does not exist	0
	It is necessary to keep information for a brief period	1
	Organisation should keep information but without consequences	2
	Keeping information is obligatory and the company can meet sanctions	3
	Keeping information is obligatory and sanctions are strict	4
<b>Time</b>	Does the information value falls in the course of time	
	Very quickly	0
	Quickly	1
	After 1 year	2
	After a few years	3
	Does not fall at all	4

Following individual assessment, the result analysis is carried out in a group with all team participants. After interviewing all the participants of the assessment, we try to determine tendencies and suitability of a particular assessment form of the assessors themselves and also in the relation with prevailing categories of information resource that are the object of assessment in a specific environment. The table below (Table 6.) is showing the list of the most common answers how the respondents assessed the assessment metrics.

**Table 6:** Experiences about different type of information value assessment

Summary of all the answers	
Qualitatively	does not tell us much does not give basis for decision making
Descriptively	we find difficult to express ourselves without formal way of expression it is even more difficult to make decision on the basis of such information determined sizes are subjective and they depend on the features of the assessor
Numerically	there is a lack of value scale that would represent values that I feel it is impossible to connect qualitative value in this way
Relatively	good controlling manner of assessment consistencies
Financially	it is rarely possible to apply dependent on the mistakes if ALE is used
New questionnaire	the most suitable of all the offered forms contains all value dimensions on the basis of which information is supposed to be valuable

These answers trigger the conclusion that the offered questionnaire and 20 questions among the offered assessment form are the most suitable ones (in our cases). The question which is imposed on is what to do with the given value. Considering this fact it can realise max 4 point (for one question), what makes value range form 0 to 20. The given numerical

amount is a level according to which we should take the responding security measures or investments. The Table 7. is recommended as a way to deal with such estimated amounts.

We should also highlight that such judgement was obtained on a small sample of the respondents. What makes it more difficult in such researches is business sensitivity as well as motivation of the assessors. The use of the offered model would be more credible also in further time period.

**Table 7:** Security recommendations based upon estimated information importance

Range of value	Significance
0- 6	For the internal use – value that information has for an individual and also does not present a real picture of the value for the process itself, protection measures should be established but the employees themselves are responsible for that, insecurity and activities of threats do not have important consequences.
7-13	Business private information – information that the process depends on, but not to such a degree that the basic business processes could not take place. The size of protection should be such that it can eliminate major threats as technical and program ones
14-20	Business sensitive information- information that are very important so a business organisation can not be without them nor even a single day, establish the protection and all measures that can be invalidated by any form of threats that can create loss or corruption in the period longer than one day, and if there is a business secret to establish protection form revealing it.

## 5. CONCLUSION

This paper puts emphasis on the problem of determining information value and the criteria used for information evaluation. Information value assessment is solved by re-examining the role of information on a business. For more qualitative evaluation, it is crucial to define criteria that realistically describe processes in a company in which information that is being assessed is counted. The concept of information assessment is determined by two components:

1. Dimensions of information value or criteria that describe information value and
2. Intensities of importance of these criteria on the global structure of information value.

During the information evaluation process, we should determine the amount of influence the information will have on business results. This mostly depends on an individual receiver or his abilities, so information is usually subjectively examined and evaluated. To achieve objectivity in evaluation, the process of assessment should be carried out in the following steps:

1. Structuring the problem of information value using three basic dimensions of value,
2. Determining the importance (intensity) of particular dimensions of information value and
3. Acts of assessment that include the determined technique for bringing opinions and metrics of assessment.

There are two dominant forms of assessment and associated metrics that stand out, quantitative and qualitative. The assessment itself is determined by the chosen methodology of assessment, and it depends on the characteristics of the information that is being assessed (direct value and/or indirect value). In each case, the chosen methodology and range of intensities value should be directed towards choosing the most effective security. Presented analysis of information value dimensions, new ideas and experiences represent the contribution to further efforts promoting information systems security of which their intangible component is particularly important. We can conclude that future efforts will be directed to formalising assessment procedures for information content.

## REFERENCES

- [1] Andress Amanda, *Surviving Security: how to integrate people, process and technology* - 2nd ed., CRC press LLC, Boca Raton, 2004.
- [2] Barker Jeffrey: *The Value of a Good Idea: Developing and Protecting Intellectual Property in an Information Age*, Silver Lake, Los Angeles, 2002.
- [3] BS 7799, *Preparing for BS 7799 Certification*, BSI, 1999.
- [4] BS ISO/IEC 17799:2000, *Information technology - Code of practice for information security management*, BSI, 2000.
- [5] Ciechanowicz Z.: Risk analysis: requirements conflicts and problems, *Computers & Security*, Vol. 16, No. 3, <<http://www.sciencedirect.com>>, (20.10.2002.)
- [6] Cohen Fred: *Managing Network Security – Part 5: Risk Management or Risk Analysis*, *Network Security*, 1997., <<http://www.sciencedirect.com>>, (20.10.2002.)
- [7] Craft Rick, Wyss Greg, *An Open Framework for Risk Management*, <<http://csrc.nist.gov/nissc/1998/proceedings/paperE6.pdf>>, (12.12.2002.)
- [8] Cramer L. M.: *Measuring The Value Of Information*, DAMA Australia, 1997., <<http://www.dama.org.au/>>, (20.10.2002.)
- [9] Ekenberg L., Danielson M.: *Handling Imprecise Information in Risk Management*, <<http://www.dsv.su.se/~mad/what.html>>, (16.01.2003.)
- [10] Gerber M., Solms v Rossouw: *From Risk Analysis to Security Requirements*, *Computer & Security*, No. 20, <<http://www.sciencedirect.com>>, (25.11.2002.)
- [11] Gordon J. R., Gordon R. S.: *Information Systems - A Management Approach* second edition, The Dryden Press, 1999.
- [12] Graef J.: *Measuring intellectual assets*, The Montague Institute, 1997., <<http://www.montague.com/>>, (15.010.2002.)
- [13] Habtamu Abie: *Risk Analysis, Assessment, Management*, <<http://www.nr.no/~abie/RiskAnalysis.htm>>, (25.02.2003.)
- [14] Humphreys E. J., *Guide to BS 7799 Risk Assessment and Risk Management*, British Standards Institution, London, 1998.
- [15] Ingwersen Peter, *Information and information Science, Encyclopaedie of Library and Information Science*, Vol. 56, p.137-174, New York, 1995.
- [16] Krause Micki, Harold F. Tipton: *Information Security Management Handbook*, CRC press, Boca Raton, 2005.
- [17] Lawlor C. S.: *Computer Information Systems*, The Dryden Press, Harcourt Brace & Company, 1994.
- [18] McCumber John, *Assessing and Managing Security Risk in IT Systems*, CRC Press LLC, 2005.
- [19] Moody D., Walsh P.: *Measuring The Value of Information : An Asset Valuation Approach*, *European Conference on Information Systems*, <<http://www.dama.org.au/melbourne/ValueOfInformation.pdf>>, (10.09.2002)
- [20] Nosworthy, J.: *A Practical Risk Analysis Approach: Managing BCM Risk*,

- Computers & Security, Vol. 19, <<http://www.sciencedirect.com>> (20.08.2002.)
- [21] Peltier R. Thomas: Information Security Risk Analysis, CRC Press LLC, Boca Raton, Florida, 2000.
- [22] Petrocelli Tom, Data Protection and Information Lifecycle Management, Pearson Education inc., New York, 2006
- [23] Poore R. Spencer: Valuing Information Assets for Security Risk Management, , Information Systems Security, Auerbach Publications. Vol. 9. No.4., 2000.
- [24] Reeker Jones: Measuring the Impact of Information on Complex Systems, <[http://www.isd.mel.nist.gov/research\\_areas/research\\_engineering/Performance\\_Metrics/PerMIS\\_2001\\_Proceedings/Reeker\\_Jones.pdf](http://www.isd.mel.nist.gov/research_areas/research_engineering/Performance_Metrics/PerMIS_2001_Proceedings/Reeker_Jones.pdf)>, (25.11.2002.)
- [25] Schumacher Markus: Security Engineering with Patterns, Springer-Verlag, Berlin, 2003.
- [26] Solms Von B.: Information Security – A Multidimensional Discipline, Computers & Security, Vol. 20, <<http://www.sciencedirect.com>>, (17.09.2002.)
- [27] Stair M. Ralph, Reynolds W. George: Principles of Information Systems, Course Technology, fifth edition, 2001.
- [28] Stoneburner G., Goguen A., Feringa A. : Special Publication 800-30, Risk Management Guide, NIST, 2001., <<http://www.nist.gov/>>, (15.10.2002.)
- [29] Swanson Marianne, Guttman Barbara: Generally Accepted Principles and Practices for Securing Information Technology Systems NIST SP 800-14, 1996., <<http://www.nist.gov/>>, (30.02.2003.)