Risk Assessment – a human psychology approach

Mazareanu, Valentin

Universitatea "Al.I.Cuza", Facultatea de Economie şi Administrarea Afacerilor

2007

Risk Assessment – a human psychology approach

Valentin Petru Măzăreanu, drd.
Universitatea "Al.I.Cuza", Facultatea de Economie şi Administrarea Afacerilor
Catedra de Informatică Economică
Carol I blvd, nr. 22 A, 700505, Iasi, Romania
E-mail: vali.mazareanu@feaa.uaic.ro

Abstract

As most of us already know, risk management means making steps in order to identify those risks with a highly probability of causing problems to a project, to analyze the probability of loss and the magnitude of loss for each risk and developing composed risks, to classify the risk points identified according to the composed risks they belong to. All these processes are important in a risk management plan, but one is definitely considered to be a "*landmark*" for the rest. And this is risk assessment. At this point a risk manager would probably choose a qualitative approach or a quantitative one?

This paper will make a short overview over the risk evaluation process but also proposing a new approach in this direction - a human psychology approach.

Key words: risk management, assessment, human factor, psychology

1 A short introduction in the methodology of assessing risks

As Hal Tipton and Micki Krause noted[1] in *Handbook of Information Security Management*, whether we choose the quantitative assessment, whether we try a qualitative assessment, the elements that need to be considered (if we recall the *„Divide et Impera"* adage) are:

- *tangible or intangible asset value* (the value of these assets is determined, usually, in terms of cost required for replacing them)
- *threat frequency* (the threat defines an event whose existence would lead to an unwanted impact.)
- *threat exposure factor* (this factor represents a measure of the magnitude of loss or the impact on the value of an asset.)
- *safeguard effectiveness* (this term represents the degree to which a safeguard manages to effectively minimize a vulnerability and to reduce the risks of associated loss.)
- *safeguard cost* (safeguards are often described as controls or countermeasures and we can talk here about the practice of the cost/benefit analysis.)
- *uncertainty* (this term characterizes the degree, expressed in percentages of trust in the value of any element of the risk assessment process)

As a (*pre*-)conclusion, if these elements are evaluated starting from a high-medium-low type criteria, the assessment will be qualitative. To the degree to which each of these elements is quantified into independent objective indexes such as the monetary value of replacing the value of the asset or the annual occurrence rate for the frequency of the threat, risk assessment becomes predominantly quantitative. If all these six elements are quantified through objective independent indexes, risk assessment is fully quantitative, undergoing a series of statistic analyses.

2 The project's predisposition to risk

The elements presented before do, in truth, perform a risk assessment, but more through risk *behavior* (the exterior event with devastating potential, the financial damages it causes etc.).

For this reason, we think that other elements can also be considered in risk assessment, such as:

- the professionalism of the assessment team / trust granted to the human factor;
- the time available to make the assessment;
- the moment of risk identification in the system's life cycle (analysis, project, implementing, testing, effective functioning etc.);
- the necessary cost for assessment and adopting the risk response plan – acceptance, avoidance or transfer. ("Is the assessment still worth if it generates a cost higher than the damage that would be generated in the case of a risk occurrence?");
- the STEEP factors (social, technological, economical, environmental, political).

We reveal on this opportunity another factor which should be considered in the assessment of risk generated by the human component - the psychological factor. And we don't necessarily mean by that abilities, skill (ability

[1] Tipton, H. & Krause, M., *Handbook of Information Security Management*, CRC Press LLC, 1998

consolidated through habit) or intelligence (analytical, synthetic, pragmatic, and theoretical). We consider personality, character, creativity (when required), and temperament to be important.

We admit that this is not the first time man is being analyzed. We mention the *risk centers* technique, the P^2I^2 *formula* (people – processes – infrastructure – implementation) or the *cause-effect diagram* (fishbone diagram or Ishikawa diagram) where the analysis of the human factor is one of the important elements. But this paper proposes a different approach: *the project's predisposition to risk starting from the human factor.* Let's remember that when the famous Golden Gate bridge was built in San Francisco, Joseph Strauss, the founder of this project, a symphony in steel as it is called by John Bernard McGloin, professor at the University of San Francisco, dismissed one of his best workers because he, so confident of himself, refused to follow the required work protection measures (e.g. wearing a protective helmet, ensuring himself with safety wires). Or more recently, talking about Google's human resources policy, Eric Schmidt (CEO Google) and Hal Varian (professor at Berkeley and consultant for Google) highlighted the fact that, in a project, it is almost fatal to have in a team an intelligent but inflexible person. Exactly for this reason the combination of recommendations „*he is the most clever person I have ever met*" and „*I would never want to work with this person again*" represents a bad solution for Google[2].

The law system introduces the concept of *the benefit of the doubt or innocent until proven guilty* according to which every person is considered not guilty until proof of his/her guilt is brought through a final decision. If we were to start from the well-known saying by Cicero *errare humanum est* (to err is human) or from what Paul Williams said in one of his articles from the series *Thought for the day*[3], that is, „even the best-worded policies and the most technically advanced counter-measures will not compensate for human stupidity", we could safely say that at least as far as informational security is concerned seen through the human factor, there should be in risk management the concept of *guilty until proven innocent*. But by taking this concept form the desire of making it easier to be accepted we come to the *predisposition to risk*. See fig. 1

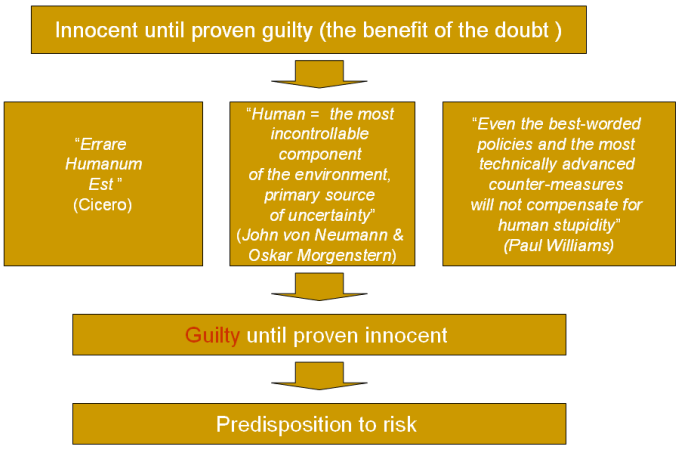

Figure 1 ***A new approach to risk management***

This concept can be applied to the human factor – the man is subject to mistake, blackmail, is corruptible etc. – as well as to any other element – the informational system is fragile, can be affected by viruses, by a sudden shortage of power or by a natural disaster, etc.; a building's frame is affected by the lapse of time etc.).

We thus bring forward the human nature – primary factor of uncertainty in a project. Let us not forget that arrogance, ignorance and fear are considered to be primary risk elements within any project. Let us take for example temperament. Without going into such an analysis for the moment, we mention that temperament is a form of manifestation of personality under the aspect of energy, quickness, regularity and intensity of the psychic processes. It is the dynamic side of personality with influence on the character.

The classical classification assigns four types of temperament:

- *Sanguine* – quickness, liveliness, calm, intensity of emotions and shallowness of feelings, instability of interests and inclinations, easy distribution and commutation of focus, maximum adaptability, endurance, maintenance of endurance and psychic balance.
- *Phlegmatic* – calm, slow affective response, durability of feelings, natural patience, inclination towards routine, refuse towards changes.
- *Melancholic* – reduced work capacity in conditions of overstress, low neuropsychological endurance, acute sensitivity.
- *Choleric* – no self control, impulsiveness, agitation, tumultuousness, impatience, emotional explosiveness, oscillations between impetuous activism and depression, inclination towards alarm states and anguish.

The temperament is influenced by aspects of genetics, experience, chemical substances in the body at a certain point. Closely connected with temperament is the attitude towards risk. Each person has a natural preference towards

[2] Schmidt, E. & Varian, H., *Google-Ten Golden Rules*. Newsweek, December 2005, pp.48-50
[3] Williams, P., *Thought for the day: The IT danger of coffee,* Retrieved 14.05.2006 from http://www.computerweekly.com/

risk, preference which depends on one's own temperament. By knowing a person's preference towards risk, we can anticipate which choices they are going to make. The attitude towards risk can be of three types:

- *Risk averse*: It shows a conservatory attitude towards risk, with preference for safe results.
- *Risk seeking*: it shows a liberal attitude towards risk, with preference for speculative results.
- *Risk neutral*: It shows an impartial attitude towards risk, with preference for future results.

With the risk of sounding familiar for some projects run nowadays by different organizations, we exemplify this approach through a few attitudes:

- *„Why should I bother to run a risk assessment program?"*
- *„I already know what the risks are!"*
- *„I already have enough problems to deal with!"*
- *„It has not happened ..."*

We are thus talking again about arrogance, ignorance, fear.

It is known that management often manifests ignorance when informational security policies, risk assessment processes, the real nature of risks and the benefits of risk assessment are concerned, especially when everything comes down to equipment acquisition costs which increase the security (safety) degree or specialized software acquisition which speeds the risk assessment / quantification process. And because by mentioning costs we have come into the financial-accountancy area, the arrogance manifested in this area regarding informational security is often encountered, and thus regarding risk assessment. Management often goes through difficulties in realizing how a healthy informational security can affect in a positive manner the financial-accountancy evolution.

Closely related to the ignorance manifested at a certain time in considering risks at their just injuriousness, is fear: the fear of being accountable for an assessment inadequately carried out, the fear of discovering risks which were not known before, the fear of having to address these new risks, as well as the fear of proving ignorance or arrogance in the activity.

Maybe considering these aspects we will think twice when we put together the team for a project which has to deal with, for example, activities which require a lot of concentration and extremely detailed work, and activities a choleric temperament could not deal with, in which case the project would be *predisposed to a risk* from the start.

Starting from the things stated above we present a model of analysis of the project's predisposition to risk starting from the analysis of the human component.

3 Model of risk assessment of a project[4]

3.1 Approach directions

When attempting to shape the risk profile for implementing a project, aspects related to the plan of the project, the resources of the project, the opportunities and attribution of the personnel within the project, the justification of the costs and benefits of the project, the expertise of the project's personnel, members of the consortium as well as of the beneficiaries, the clarity of the project's requirements, management techniques adequate for the project are considered. Obviously, not exclusively. When considering the human factor the analysis is usually done through the prism of the following aspects: health and safety at the work place, position held within the project (the risk of dependency on the key personnel), as well as aspects related to the human resources policies. In the model we will be presenting below we try to introduce a new approach, namely the psychological one, for the moment only on the level of the temperamental pattern and personality (Obviously this approach could also analyze aspects related to the person's abilities, character etc. And for abilities psychology provides us with what is called *the test battery for the profession of computer scientist,* a complex test structured on five levels – verbal comprehension, reasoning, logical operators, numerical ability and diagrams – meant to reveal the ability level of the individual).

But why would we try assessing personality? The reason to act this way is the attempt of behavioral prediction. More precisely, the purpose is to identify future probable behaviors of a person without relying on the information obtained through systematic observation of them. This can be done nowadays with the help of numerous instruments as we will see below.

3.2 Defining criteria

The first step a project manager (alongside with the human resource department) has to realize when deciding to form a team to make a project is to establish the performance criteria for the position advertised. These performance criteria can be *expected results* from the occupant of the respective position (what they must do) or *behaviors* which they have to realize in order to obtain the desired results (how to act). A criteria is a standard or a measure through which we can assess the professional performance, abilities etc., is a variable which allows the assessment of a phenomenon, the identification of criteria or of acceptable or unacceptable performance standards representing an essential preoccupation in building an assessment instrument.

---

[4] Havârneanu, C., *Cunoaşterea psihologică a persoanei. Posibilităţi de utilizare a computerului în psihologia aplicată*, Ed. Polirom, Iaşi, 2000

We must not ignore the fact that finding a good criteria based on which a project manager can decide to implicate or not a person in the project starts from the analysis of work, which brings us to a series of errors which can appear in the assessment of performance (e.g. the halo effect, indulgence / severity of evaluators, social influence, etc.).

Although these performance criteria are aspects related to the individuality of each project, companies such as Microsoft or Project Management Institute have revealed a few general characteristics which a person involved in a project should fulfill. Thus, Project Management Institute proposes "Project Manager Competency Development (PMCD) Framework", paper which presents the performance criteria and the knowledge required for each of the 9 components of project management[5]: (*Project Integration Management*), (*Project Scope Management*), (*Project Time Management*), (*Project Cost Management*), (*Project Quality Management*), (*Project Human Resource Management*), (*Project Communications Management*), (*Project Risk Management*), (*Project Procurement Management*). For each component a new decomposition is made, on the stages of project management: (*Initiating*), (*Planning*), (*Executing*), (*Controlling*) and (*Closing*).

For the purpose of getting nearer to informational technologies, we will also refer to Microsoft. The specialists of this company propose Microsoft Operations Framework (MOF)[6], a guide which allows organizations to realize an assessment of the maturity of the management of IT services. One of the MOF components is MOF Team Model for Operations which represents a guide about the structuring way of teams in the information technologies operations field with the purpose of obtaining an increased efficiency. This model is based on the concept that any team has to reach a number of key qualitative elements in order to be considered a success team. Teams, in the view of this guide, are grouped on the following roles: infrastructure, operations, partner, security, launch (on the market), services, and assistance. Even if the model proposed by Microsoft relies more on the presentation of technical abilities and knowledge, in the present model we can rely on the specifications presented by the Management Institute, to which the particular requirements of each project will be added.

3.3 Establishing the prediction instruments

For each of these criteria the best *predictor*, has to be identified, that is the test, the evidence or the selection element which can predict with the greatest probability the ulterior performance at the work place. Examples of predictors are: personality tests, ability tests, performance tests and „work evidence", interest questionnaires, values and preferences, structured interviews, clinical evaluations, team/quality assessment, professional knowledge tests, integrity tests, the level of education, the quality of the school, the main study field, extracurricular activity, training and experience, certifications and accreditations, ponderate candidature forms, biographical data, recommendation letters, verification of recommendations, testing the background, CVs and letters of intent, initial interview.

In regard to the analysis of the temperamental pattern we will use a questionnaire model proposed by *Gaston Berger* and for the establishment of the personality traits we will use the 16 P.F. test (16 personality factors), model proposed by *dr. Raymond Cattell*, model which tries to identify the primary personality components with the help of the factor analysis. (A similar test is also the BIG Five Test, a test which approaches personality through the prism of five factors). Through the 16PF, we can obtain in a relatively short period of time an image of the personality traits which characterize one subject or another. As it was built, 16 PF does not discover isolated traits, but real differential systematic aspects, such as they were relevated by the studies of factor analysis which are the basis for the questionnaire.

The 16 personality dimensions or scales are relatively independent.

Any item of the questionnaire contributes to the score obtained on a single scale, which represents a certain factor. More so, the inter correlations between the 16 scales of the questionnaire are relatively independent, so each scale preserves its own individuality.

3.4 The phases of the application of the model

If for the criteria we can rely on the Project Management Institute model and on others identified at each particular project, the problem surfaces only when we try to identify the measure-criteria characteristics. Here is an example to explain this concept: *success at university represents a criteria, while the cumulated average is a measure-criteria.*

Thus it remains the task of the project manager to establish for each process / department such measure-criteria. We produce a few examples below:

- Number of errors per time unit,
- Number of risks identified by time unit,
- Number of preventive actions identified by time unit,
- Number of accidents per time unit (month, year etc.),
- Speed degree in the use / development of different risk management instruments (e.g. the preliminary matrix of risk assessment),

---

[5] Project Management Institute, *Project Manager Competency Development (PMCD) Framework*, Project Management Institute Inc., Newtown Square, Pennsylvania USA, 2002

[6] Microsoft, *Team Model for Operations version 3.0*, at http://www.microsoft.com/mof, accessed on 01.07.2006

- Aptitude tests (e.g. number of correct answers obtained to the questions in the battery of tests for the job of computer scientist),
- Number of data (delivered by third parties) verified from the point of view of accuracy by time unit,
- Etc.

Once the performance criteria and the measure of criteria are identified we proceed to determining the validity coefficient, useful in the determining of the predictive validity. In other words we try to determine the correlation between the scores obtained at the predictor test and the scores obtained at the measure-criteria.

This calculation presupposes the passage through five different stages:

1. choosing a group of subjects;
    a. e.g. the persons (the members of the project teams) involved in other projects (preferably more than one project) whose results were successful
2. applying the predictor test to these subjects;
    a. e.g. the Gaston Berger temperamental pattern test or that of the personality factors Cattell 16 PF
3. developing some specific processing if required;
4. collecting the data from the criteria;
    a. e.g. number of errors per time unit
5. calculating the correlation between the scores obtained at the predictor and at the criteria;
    a. e.g. calculating the correlation coefficient between X (score obtained at the general knowledge test) and Y (score obtained at the attitude scale)
6. the correlation coefficient obtained helps to determine the validity coefficient;
    a. Obs. Different statistic instruments are used
7. applying the predictive test to the persons who wish to be involved in the present project and the interpretation of results
    a. Obs. There is the possibility to predict a criteria score for a subject based on the scores obtained at the predictive test; the problem of estimating a future result (y) based on the present information (x) about a person rises.
    b. e.g. the prediction of errors starting from the validity coefficient
    c. e.g. the prediction of the possibility that the subject is perceived as a leader starting from the high score obtained at a test measuring dominance

In this way a manager can determine if a person who is about to be hired in a project on an existing position is able or not able to perform a specific task. Starting this the risk manager can determine the effects of hiring a person on a specific position and the dimension of the predisposition to risk of a project.

4 Conclusions

Barry Boehm, a true pioneer in risk management had developed a risk management methodology. Shortly, this methodology is presented in the exhibit below:

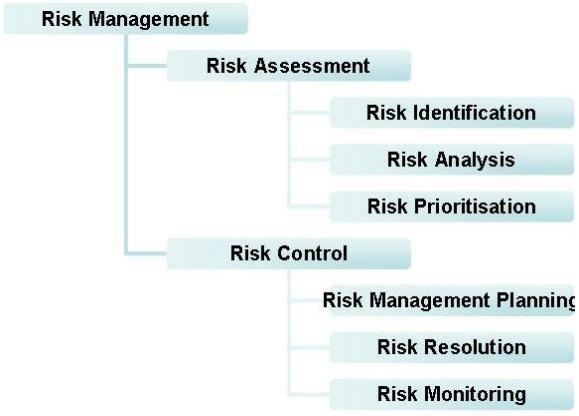

Figure 2 ***The Barry Boehm model (simplified)***

Accentuating this new psychological approach and remembering that the process of risk assessment is a dynamic process, run over time, we consider opportune to adjust the Barry Boehm model and to introduce a new subprocess, exemplified in the figure below.

Figure 3 ***The Barry Boehm model (adapted)***

The new model presupposes the elimination from the project of the element which would generate predisposition to risk and its replacement with another, much more viable. In an example corresponding to psychological evaluation, if in a project a person is considered to have a *melancholic* temperament following an eventual profile test, that person would be eliminated from a team which would have to deal with activities which require a lot of attention and which consume lots of energy in a short period of time. The difference consists of the fact that we no longer quantify this risk and we dispose it in a hierarchy following to be controlled and monitored subsequently. We could say that this new approach is a "*Just in Time Risk Management*" one.

References and Further Readings:

1. Boehm, B., W., *Software Risk Management: Principles and Practices*, Defense Advance Research Project Agency, la http://www.ece.ubc.ca/~elec443/priv/ReadingMaterial/Boehm-risk.pdf
2. Duncan, W., R., *A Guide to the Project Management Body of Knowledge,* Project Risk Management, Upper Darby: Project Risk Management, 1996
3. Haimes, Y., Y., *Risk Modeling, Assessment and Management*, New York: John Wiley & Sons, Inc., 1998
4. Havârneanu, C., *Cunoaşterea psihologică a persoanei. Posibilităţi de utilizare a computerului în psihologia aplicată*, Ed. Polirom, Iaşi, 2000
5. Havârneanu, C., *Resurse umane şi strategii de consultanţă*, Ed. Erota, Iaşi, 2002
6. Microsoft, *Team Model for Operations version 3.0*, Retrieved 01.07.2006 from http://www.microsoft.com/mof
7. Project Management Institute, *Project Manager Competency Development (PMCD) Framework*, Project Management Institute Inc., Newtown Square, Pennsylvania USA, 2002
8. Schmidt, E. & Varian, H., *Google-Ten Golden Rules*. Newsweek, December 2005, pp.48-50.
9. Tipton, Hal & Krause, Micki, *Handbook of Information Security Management*, CRC Press LLC, 1998
10. Williams, P., *Thought for the day: The IT danger of coffee,* Retrieved 14.05.2006 from http://www.computerweekly.com/

Aparut in Mazareanu P.V., *Risk Assessment – A Human Psychology Approach*, în Economic Theory and Practice in Knowledge Society, SedCom Libris, Iasi, 2007, ISBN 978-973-670-241-9