ABOUT THE HUMAN FACTOR IN RISK MANAGEMENT – PRIMARY SOURCE OF UNCERTAINTY

Valentin Petru Măzăreanu[1]

Abstract

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, to classify the risk points identified according to the composed risks they belong to. An especially important role in any system is owned by the human factor, maybe the most incontrollable component of the surrounding world, a primary source for uncertainty, as John von Neuman and Oskar Morgenstern claim [*].

The main objective of this paper is to analyze the human component and to offer solutions from the risk management perspectives at least from two points of view, that is: human, as an attack source to the information system (e.g. outside attacks, inside attacks – ill intended persons, unprepared persons etc.) and the risk generated by the status of key position of a human resource within the system (e.g. the effects caused by disease, death, leaving the team etc.).

Keywords: risk management, human factor, uncertainty

1. Introduction

Normally, if a business man were asked which the most important component within the organization he manages is, he would answer: “the most important asset of my company comes down with that elevator each night and goes home”.

Obviously, it is not the only point of view which would put the human resource first. Let us not forget that in the opinion of Peter Drucker also the human resource holds a prime place within any system. It is true, Peter Drucker talks about the knowledge worker, those persons who works, manage knowledge.

But, speaking of the human resource in general, he states: “the purpose of an organization is to make the strong points of people productive and their weak points irrelevant”. Moreover, highlighting the importance of the human resource within the company, company managers should answer questions such as:

- Are we attracting people we trust the organization to rely on?
- Do we develop their abilities so as they are better than ourselves?
- Do we manage to maintain, motivate them, and recognize their merits? In other words, do we build our future based on the decisions of these people or are we content with the comfort of today?

1 The Faculty of Economics and Business Administration , “Alexandru Ioan Cuza” University of Iasi, Iasi, Romania, email: vali.mazareanu@feaa.uaic.ro

But at the same time, man is considered to be the primary source of uncertainty within any activity and thus identified as being a main source of risk within any organization. Thus, researchers talks about the reasons that cause the failure of projects and elaborates a list inspired from real mistakes met in projects. From his listing we extract: turning to a technical specialist who has never implemented a similar system or attributing the data migration to a beginner developer three months before the system is implemented. In the implementing projects of the distribution chains, difficult because they imply connecting tens or hundreds of suppliers, among the causes for failure we mention the hostility between departments (if it is not hostility, there is at least a passive resistance), poor management (because multiple departments are involved, the distribution chain projects need to be managed from a higher level in order for them to survive the pressures and problems that occur along the way) or sabotage from the employees (be that bad or well intended).

The reasons are many, but at least one is known since Cicero: *Errare humanum est*. To err is human, indeed. But this error could badly affect the good performance of the activity of an organization.

A person 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 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 we 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 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.

So here are some points of view (and we must admit that the list is not complete) that need to be taken into consideration when deciding the risk analysis through the prism of the human resource.

2. Man, Source And Means Of Attack Of The Information System Of The Organization

As can be seen in the "top ten risks" lists published by various authors, but also as shown by multiple studies regarding the attacks on the information systems (see the annual editions of the CSI/FBI survey) the human factor is on the first places as source of risk or attack against a system.

The Cybercrime is a growing problem having its origins in the external environment and internal environment of the organization. In Wespi's [1] opinion the security risks remain high because of four reasons:

- Vulnerabilities are growing, despite the efforts made by software manufacturers to secure their products;
- Badly designed software, with a greater emphasis on new features and performance, but with too little attention on the security;
- Methods of attack have increased and have become extremely sophisticated, while more and more attack tools are available on the Internet, which no longer requires specialized knowledge, thereby easing the work of such attackers like script kiddies (name given to those attackers using attack tools found on the Internet);
- Vulnerabilities discovered are often treated inappropriately highlighting the lack of knowledge or ignorance of their system administrators, taking into consideration that the information about a discovered vulnerability is rapidly speeding in the community of the attackers.

Referring to the human attacks on the information systems, Eugene Spafford [2], a professor and security expert, claims: "the public perception on the persons who fraudulently access an information system is, unfortunately, one through which they are considered either geniuses, or misguided children who show off. But this fact is far from the truth. These persons are simply criminals". When it is talked about computer crime, it is also remembered the fact that this "information highway", as the internet was called, has its share of wrongdoers. And even if by computer crime it is referred most often to actions without serious negative effects of some young hackers (attacks performed out of the desire to show off or to affirm oneself), in reality the virtual space is full of illegal activities, from computer crimes to prostitution, from child pornography to industrial espionage.

But not always is the attack of an information system performed through the virtual space. We mention in this sense the case of the famous hacker Kevin Mitnick (known under the alias of „the Condor"), an authority in the field, author of some attacks on companies such as Sun Microsystems, Motorola, Nokia, Nec, Fujitsu and Novell, a source of inspiration even for some movie directors (Takedown, directed by Joe Chappelle). A short history of Mitnick's crime activity would comprise the following facts: he started his career in the early '80s as a *phone-phreak*[**], then approaching the hacking techniques by breaking into the computer system of the Monroe high school; he was charged in 1981 for breaking into the information system of the Pacific Bell and Microport System companies and sentenced in the late '80s for hacking into the system of the MCI phone company (and remote

accessing of the codes), as well as for the damages of millions of dollars caused to the Digital Equipment Corporation company (for which he served only one year in prison); caught and incriminated in 15 February 1995, by the FBI helped at the time by another great hacker of the times, Tsutomu Shimomura.

But what is interesting and touches on the subject of the current section is the fact that Mitnick performed almost all these criminal acts by taking advantage of the naivety and poor training of the personnel of the above mentioned companies, to which he would present himself as a completely different person, regularly as a technician from the maintenance of technical equipment or even as a man of law, thus obtaining various access codes to the network or confidential phone numbers [***].

The literature talks about this type of attack as being one of typical social engineering, that type of attack in which persuasion, fraud, deceit or industrial espionage is used in order to obtain access data to an information system with the purpose of compromising its security. The social engineer-type attackers come into the possession of access data in two ways [3]: physical means (access to the system documentation or to passwords written on inappropriate support) or psychological means (persuasion or presenting themselves as someone else).

Studies [3] have shown the fact that four out of five people employed in a company would disclose their own access password into the system if "they were asked in the right way" (if the one requesting the information would claim to be the network manager or a person on the technical team). A similar conclusion was also reached by Burțescu [4], in a case study performed in a company: claiming to be sent by the manager to repair the computers, the author came into the possession of the passwords from 20 workstations.

If we refer to the human factor seeing him as a volunteer attacker of a system, it is worth discussing the classification made by Carayon, Kraemer şi Bier [5] in the attempt to model the behavior of the attacker:

- opportunistic attackers: the ones in search of easy preys, not being attracted by a certain target or a certain type of target (e.g. there are used denial of services type attacks);
- determined attackers: the ones who target attacking a certain target (e.g. the military or medical system, the information system of the competition) with a precise purpose (e.g. the stealing of data, the destruction of the reputation of an organization).

We also shouldn't ignore the fact that the human can also involuntarily become an attacker of the information system. We are talking here about human error, defined by Reason [6] as being a generic term through which there are highlighted those occasions when a planed sequence of mental or physical activities fail to reach their purpose, and this failure cannot be attributed to the intervention of a factor.

There can be included into this type of attack the loss of confidential data. One of the most discussed cases is the one of the loss of personal data of 25 million individuals from HMRC (an institution responsible for collecting the incomes from the payment of fees

and allowances) from Great Britain. But it is not a singular case, the press covering a long time about the Choice Point case, a data collecting agency in the USA, which sent 145.000 notices notifying their recipients that they have wrongfully provided towards inappropriate persons, their personal data, including their social security number. Another case is that of Bank of America, which announced on February 25 2008, that they have lost the records containing information with a personal character on 1 million government employees, including on some senators.

In such cases, the lesson is obvious: *no security policy will ever compensate human stupidity* [7].

Obviously the loss of data can also result following some attacks, and this danger is increasingly greater also as a result of the various criminal tools such as NeoSploit, MPack or AdPack.

The human inventiveness is difficult to anticipate, so each passing day we will watch the development of new attack methods against the information system.

Recently a group of researchers has proved that, using the Google search engine, they have come into the possession of some data, such as email account access passwords, social security numbers (similar to the CNP), user names and access passwords to databases of some companies. Why is this happening? Because following some interrogations, Google returned information based on the log files available on the servers they found unprotected (from various reasons) [8].

An article on a similar subject, signed by Johnny Long [9], explains the way in which Google search engine can be used for developing a list of web domains that are to be attacked. The way in which the Google search engine can also be used as a hacking tool is explained by Long, a specialist in penetrations testing, who also has on his site a “Google hacking database”.

Aside from the various search keys, which used can provide sensitive information (including system access data), Google also offers a series of own instruments that can be used for criminal purposes: Google Earth, Google Patent Search or Google Blog Search. These seem to the instruments increasingly used by hackers with the purpose of finding out information (more or less confidential) about a company [10].

The subject is and will remain open for a long time, all the information presented above being only a few examples meaning to show the fact that the risk the information system of an organization is exposed to must not necessarily come via virtual way, but also via other ways, but in all cases benefiting from the weak link in the system, man.

3. The Key Position Of A Person As A Risk Factor

The subject refers to personnel dependency. And this problem can be treated from two points of view, the migration of the work force and the unavailability of an important person in the system.

One of the approach directions that deal with a sensitive issue, the migration of the work force, but an aspect that has been mentioned by most of the companies [*****] and as measure they are now extremely oriented towards making employees loyal, offering them the most diverse stimulants (training, team building sessions, free medical coverage etc.).

Another direction that can refer to the risks any human is exposed to, psychological or medical problems, domestic problems, even death, aspects that are somewhat overlooked by some managers, under the cover that the problems of the employees should not be the object of the concerns of the company.

In reality, these problems are not to be neglected by the management of a company, as long as the death or reduction of the work ability of a key employee of the company or of the project can lead to the reduction of productivity, to various legal consequences, maybe even to the failure of implementing a project or the impossibility to continue an activity. Aspects such a death, sickness, leaving the work place or the project team in critical situations, along with involuntary unemployment, aging, retirement are problems that must be granted an appropriate attention from the organizations. We refer to all employers, not only to the companies in the insurance field that perform estimations of the probable frequency of deaths and other such statistical data (e.g. data concerning the average number of days of work inability, data regarding the frequency of work accidents, data concerning the frequency of turning to medical services etc.).

Even if a company has not yet reached the level at which to perform these studies on its own, such statistical data are periodically published by the authorities in the field. For example, the statistical data about accidents can be used in various purposes [11]:

- to monitor the level of risk and security of work;
- to provide information to the risk analysis process;
- to identify hazardous situations;
- to analyze the causes of an accident;
- to evaluate the effect of the risk reduction measures;
- to compare alternative situations.

But we mustn't neglect the fact that, both in the case of death and in the case of health problems, it is about dealing with some complex and totally unpredictable risks. For this reason it is necessary to keep a concordance between the complexity of the administered system and the number of specialists allocated to the system components. Thus, if it is about a complex and difficult to manage system, the dependency on specialists is also great. We can also introduce a new unknown in the equation, system documentation. Here we will depend on the ability of employees in other areas to understand and learn based on the system documentation. In this case, if it is about a single specialist that manages the system then it is obvious that the risk is very high. The higher the number of the persons with managing knowledge of that system, the lower the associated risk. Similarly, if it is about a complex system that does not have an adequate documentation, the risk is high. By combining these types of risks we will obtain a matrix of the risk associated to the dependency on specialists, presented in the table below.

Tabel 1 Risk Matrix

Source: Munteanu, A. Auditul sistemelor informaţionale contabile, Polirom, Iaşi, 2001, p.56

Dependence on Professionals	**Documentation Level**		
	High	**Medium**	**Low**
High	High	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Also to the dependency on specialists is connected to the evaluation of technological risk. This risk is identified based on the control matrix that combines the dependency on specialists with the technology itself.

Tabel 2 Technological risk

Source: Munteanu, A. Auditul sistemelor informaţionale contabile, Polirom, Iaşi, 2001, p.57

Technological Risk	**Dependence on Professionals**		
	High	**Medium**	**Low**
High	High	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Similarly there can be developed dependency relations between the dependency on specialists and the satisfaction level of the employees (which can lead to the decision to leave the work place or the project team).

4. Solutions

The migration of the work force is a phenomenon that occurs in all fields, but in a very visible way in the IT&C field. Studies show that the average of changing the work place is of 23%, the IT industry taking first place with a percentage of 31%. There were found several reasons representing the cause of dissatisfaction related to the position occupied among which weak leadership within the organization, the lack of clear objectives of the companies or the lack of general communication and management knowledge of the managers who went to technical schools (most managers of the technical departments, IT&C, data security fall into the previous profile). All these can lead to conflicts between management and staff, these conflicts ending with the severing of the contractual relationship between company and employee.

The solution is in the creation of an employee oriented management, applying various strategies to maintain the key staff within the company. There are human resources management aspects, as well as of quality management, aspects from which we mention:

- salary policies depending on the level of responsibility of the work place, work performance of the individual, external work market;
- policies for harmonization of the salary conditions;
- training, learning and knowledge policies;
- policies for reorganization of the way of performing activities (from the classic model to the project work model);
- equalization policies between staff and management;
- open management style, free upwards to downwards communication, but also downwards to upwards, introducing brainstorming and group studies to identify the problems and the needs of each team member.

Under the conditions where we noticed that the human factor represent a source of risk on a system, it is self-implied the fact that the management practice of human resources can provide a control instrument of the staff. And the most important practices and procedures of staff management that must be taken into discussion through the prism or risk and of its control, are in the opinion of Grundy, Collier and Spaul [12]:

- employment procedures (description of the job, using application forms for the work place, selecting the appropriate person for the appropriate position, interviewing, checking through references, testing of intelligence, of abilities, attitude etc., existence of a trial period);
- policies for not non using / non disclosure of confidential information;
- policies for rotation of the work place and for declaring a vacant work place;
- separating the work tasks;
- implementing means for addressing complaints;
- staff reevaluation procedures;
- policies for ceasing the work relation (firing).

We are at the intersection with another area and, although we will not fully approach it, we only wish to highlight the fact that the human resources management system represents an essential set of managerial tasks. They must be efficiently performed in order to encourage and motivate permanent employees, the ones hired temporarily in the project teams or volunteers.

The problem of dependency on a certain category of personnel can also be extended to the aspects related to the reticence towards new or resistance to change.

From various “top 10 risks” type lists there can be noticed that an important position is taken by the risk related to the behavior of managers and of staff in the face of the changes brought by a new information system. This category of risks emerges because, through his nature, the man is reticent to change and a new information system modifies the way they perform their tasks. The reticence to change also comes from the fear of new, fear of the unknown. But not exclusively: with the implementation of a new information system, the responsibilities of the employees increase and the fine

development of the activities can suffer because of some managers or employees who poorly manage the system, out of lack of knowledge, ignorance or ill-intent.

5. Conclusions

It is truly "fashionable" in companies to implement new solutions, in the name of solving the fundamental problems of economic processes in a more rapid and efficient manner. Otherwise we would not have assisted to the explosion of offers for enterprise resource management systems, supply chain management, business intelligence, corporate performance management, business process management etc. Where there is a request it is normal that there will be an abundance of offers.

What do the managers of these companies forget is to ask: do I really need this new system?; do I have the necessary financial resources for implementing this new system?; are my men prepared to handle the new system?. We are speaking then of the analysis of profitableness of investment and of planning the implementing process. Both have to have as key point the education of staff in the spirit of the new information system, because, if the financial side and utility are controllable, in case the staff does not accept the new system, however good the offered solution might be, it is possible that the company will suffer because of the replacing of an old information system, they were all familiar with, with a new one, that no one knows how to use efficiently.

Notes

[*] John von Neuman (1903 - 1957) and Oskar Morgenstern (1902 - 1977), wrote the first paper dedicated to the game theory, „Theory of Games and Economic Behavior" (1944)
[**] Method of attack on the phone services by cracking the access codes
[***] Mitnick is not the only such attacker. There are others, among which Kevin Poulsen (also called „Dark Dante"), also an inspiration for movie directors („War Games", 1983), who because of his talent was employed in the defense industry as consultant for security problems (this after he managed to crack the security systems of some military and government institutions); but if in the daytime he was a loyal consultant to the workplace, in the nighttime he was acting against the system, stealing various classified military information or revealing various FBI classified information. We also mention: Gene Edward Howland („Poo Bear") and Daniel Glynn Van Deusen („Wild One") or Justin Tanner Peterson („Agent Steal").
[****] A fact also deducted from the behavior o many managers towards employees, information that we access almost daily in the press in the field.

References

1. Wespi, A., Securing your e-business by managing the inherent IT security risks in Abderrahim, L. (editor), *Handbook of integrated risk management for e-business: measuring, modelling and managing risk*, Ed. Ross Publishing, Boca Raton, 2003, pp.116-118
2. ***, *A Crime By Any Other Name*, at http://www.theta.com, accessed on 10.05.2006
3. Tulloch M., *Microsoft Encyclopedia of Security*, Ed. Microsoft Press, Redmond, 2003p.244

4. Burțescu, E., *Securitatea datelor firmei*, Ed. Independența Economică, Pitești, 2005, p.113
5. Carayon,. P., Kraemer, S., Bier, V., Human factors issues in computer and e-business security, in Abderrahim, L. (editor), *Handbook of integrated risk management for e-business: measuring, modelling and managing risk*, Ed. Ross Publishing, Boca Raton, 2003, p.67
6. Reason, J., *Human error*, Cambridge University Press, Cambridge, 1990
7. Williams, P., *Thought for the day-the IT dangers of coffee*, at http://www.computerweekly.com, accessed on 11.11.2004
8. Măzăreanu, P.V, *Google - instrument de hacking: din nou in atentia specialistilor*, published on http://www.managementul-riscurilor.ro, in 03.06.2008
9. Long, J., DNS name prediction with Google, *The Security Journal*, spring 2005, at http://www.securityhorizon.com, accessed on 27.04.2008
10. Măzăreanu, P.V, *Google ... sursa de informatii pentru hackers*, published on http://www.managementul-riscurilor.ro, in 20.03.2007
11. Aven, T., *Foundation of Risk Analysis: A Knowledge and Decision-Oriented Perspective*, Ed. John Wiley & Sons, West Sussex, 2003, p.8
12. Grundy, E., Collier, P., Spaul, B., Auditing Personnel: A Human Resource Approach to Information Systems Control, *Managerial Auditing Journal*, Vo.9, No.6, MCB University Press, Sept. 1994, p.10

Acknowledgements

The results presents in this paper were obtained in the framework of the postdoctoral school programme financed by the *"Developing the Innovation Capacity and Improving the Impact of Research through Post-doctoral Program POSDRU/89/1.5/S/49944"* project