# Risk Management of Human Behavior in IT Enterprises:
## A Survey of Current Approaches

Gao Lili
IDA, Linköping University
liga810@student.liu.se

Wu Jianqiu
IDA, Linköping University
jiawu735@student.liu.se

## ABSTRACT
Human issue is emerging as the one of the main difficulties in risk management of information security system. Especially for IT-related enterprises, this problem is hard to settle within traditional techniques. Traditional risk analysis often disregards the human behaviors in company business. As an investigation, this paper reflects on several risk analysis methods considering human factors, along with how they are being implemented. It presents several existing methods which are quantitative or qualitative based approaches designed for risk analysis of human factor in IT enterprises. There is a discussion about the survey following, it narrates the comparison among these methods with their application features. Finally it illuminates the limitation or incompletion of these methods and prospects the future in this field.

## Keywords
Risk analysis, Risk management, Human factor, Human behavior, Information security

## 1. INTRODUCTION
In recent years, our society has become more and more dependent on computers, which are used in everyday life, from business to banking, from entertainment to healthcare. Since most of their systems are interconnected through Internet, which inherently is open and vulnerable to cyber attacks, the importance of information security continues to be highlighted. Especially the IT-related enterprises, which business involved in computer and information, are looking for risk analysis techniques to help them select effective countermeasures to protect their information assets.

However, in early risk management, security problems related human behaviors are usually neglected by the IT-related company who is installing the security policy [1, 6]. These traditional policies commonly assume that people behave logically and as instructed. Whereas, since people are the main component of any information system and it is obviously that they are not totally logical, some human behavior can bring the same severe threats as computer vulnerability can do.

Nowadays, as people realize the importance of human factor in security [2], more and more researchers devote themselves into the study of the human factor in risk management. In the middle of 1980s, some scientists suggested that information security is not only a technology problem, but it also concerns people; in 1990s, they stated some cases of sabotages are committed by employees in industry [1].

The focus of this paper is on the particular technique of risk analysis of human behaviors. We elaborate several methods built upon current solutions. Our main goal is to reduce the occurrence of the human factors, and minimize the impact of human behaviors. At last, we will lay out some limitations of the proposed solution and point out the potential way of this topic.

## 2. PROBLEM
Generally, the human issues in information security include three aspects as follow [1]: (1) the objectives of personnel, which may conflict with those of company; (2) the cultures of the persons involved; (3) the attitudes of personnel which can be influenced by things happened positively or negatively. For example, an IT company as a telephone carrier, usually provides the telecommunication service which needs to be online 24 hours per day, and 7 days per week. Thus, the personnel who want spare time will not work overtime, and some employees who have religious beliefs will not work on Sundays. To solve this problem, some companies give the employees admission to carry out a considerable number of extra tasks when they are outside the offices, such as login from outside computers. It is feasible but dangerous. Some outsiders will hack into the network system easily.

Within a company daily routine, Withman [8] enumerates the following security problems caused by human behaviors.

· Act of human error or failure (accidents, employee mistakes)

· Compromises to intellectual property (piracy, copyright infringement, and so on)

· Deliberate acts of espionage or trespass (unauthorized access and/or data collection)

· Deliberate acts of information extortion (blackmail of information disclosure)

· Deliberate acts of sabotage (destruction of systems or information)

· Deliberate software attacks (viruses, worms, macros, denial of service)

· Deliberate acts of theft (illegal confiscation of equipment or information)

· Quality of service deviations from service providers (power and WAN service issues)

According to the human issues listed above, traditional Probabilistic Risk Assessment (PRA) schemes have been criticized on the grounds that the probabilistic framework may not be appropriate for modeling uncertainties in human operator behavior [9].

Some researchers also claim that another point unconsidered is the environment in which the system operates [1]. The environment includes for example, managers, employees, customers, competitors and legislation etc. All these affect information security of an IT company in many ways. Some competitors may pretend customers to fetch the information about the software mechanism or attack the network system deliberately with the lack of legislation.

Risk analysis is a complex task that entails the consideration of many parameters which are rather difficult to quantify. Generally speaking, all methods can be categorized into three types: qualitative, quantitative and semi-quantitative [10].

Qualitative risk analysis methods are used to set priority for various purposes including further analysis. They are useful when reliable data for more quantitative approaches is not available. The qualitative approach takes the point of view that many potential losses are intangible, as human factors presenting; therefore, risks cannot be easily specified monetarily. Risk results are portrayed in a linguistic manner (i.e., "no risk" to "very high risk"). Some qualitative approaches carry the risk result a step further, where risk is represented mathematically as a scalar value (i.e., a value from one to five, or one to ten, etc.) with descriptive terminology for each point on the scale. Still others provide graphic decision tree illustrations which provide a probability distribution highlighting common causes.

Quantitative Risk Analysis involves the calculation of probability and sometimes consequences, using numerical data where the numbers are not rank (1st, 2nd, 3rd) but rather real numbers [3]. Most commonly, quantification of risk involves generating a number that represents the probability of a selected outcome, such as a fatality [4].

The SQRA approach is something of a mixture of the qualitative analysis and quantitative analysis [10].

Traditional security research has tended to be technical oriented, such as designing cryptograph algorithms or users identifications. The current solutions about vague factors in risk assessment are functionally divided into two categories: quantitative and qualitative measures. We can see the main method that they used is to reduce the incertitude of vagueness, make the probability of the threat happening more specific and estimate the costs in risk analysis more clearly. There are two recent examples listed below: fuzzy logic based on quantitative measure [7] and RAMeX based on qualitative measure [5].

Fuzzy logic techniques have proven to be a very viable alternative to conventional solving methods for problems which have inherently been unstructured and intuitive. Thus, fuzzy logic presents a natural way of modeling the vagueness in risk assessment, while also ensuring that human creativity and intuition, which is an essential ingredient for successful risk analysis [7]. Fuzzy logic holds that everything is a matter of degree. It models the assets, vulnerabilities and the probabilities of hazard occurrence into some status on the same scale, so that they can be evaluated relative to each other. For example, the new personnel who is a junior with the operation system will belong 0.4 while the senior staff belongs 0.3 (on scale from 0 to 1) [7].

Even using fuzzy logic, the difficulty of predicting probabilities of loss before it occurs still confuses the risk analysts. That is the common bottleneck of all the quantitative measures. The qualitative method RAMeX solves the deficiency of quantitative method. The main steps of RAMeX follow the traditional risk analysis, and there is an additional step of risk management which is used while the risk analysis can not avoid the loss [5]. We just need to select a level (low/medium/high) for the impact severity and the loss occurs, and then make the final assessment by accounting the vulnerability, strength and impact severity levels.

## 3. PROPOSED SOLUTION

There are various models and methods for risk analysis on human factor being used today, they are variants of other risk analysis methods, such as human error analysis, fault tree analysis, event tree analysis, failure modes, effects and criticality analysis and so on.

The following presents an overview of risk analysis tools currently in use, each of them can be modified for risk analysis of human factor:

Informal Risk Assessment (RA): general identification hazards and risks in a task by applying a way of thinking, often with no documentation.

Human Error Analysis (HEA): general or detailed analysis of human factors or reliability issues.

Fault Tree Analysis (FTA): detailed analysis of contributors to major unwanted events, potentially using quantitative methods.

Event Tree Analysis (ETA): detailed analysis of the development of major unwanted events, potentially using quantitative methods.

There are also many other methods which can also be modified for risk analysis on human factor, such as Level of Protection Analysis, Consequence Analysis and so on.

Whilst traditional engineering safety assessment techniques such as FMEA and FMECA generally focus on engineering system, some researchers extend these techniques to look at human systems. When doing so, the operator evaluates each human factor that has been identified and the likelihood of it occurring. For example, how likely would a person fail to perform a task? What effects could this have, and how critical is this effect? Human errors (accidents, employee mistakes) as well as deliberate (rule violation) behavior in the analysis are included. There are a number of techniques that have been developed specifically to estimate the likelihood of human error occurring. These include:

- Human Error Assessment and Reduction Technique (HEART) [12]: This method combine both qualitative method and quantitative method. It uses task error analysis method to accomplish a task and the identification and analysis of possible errors and their probabilities.
- Techniques for Human Error Rate Prediction (THERP) [13]: It create a Human Factors Issues List to identify human factors, once human factors has been identified, using human failure probabilities to represent the probability of failures by people, an approach is used in which credits are assigned for each type of human factors result according to its hazard.
- Systematic Human Error Reduction and Prediction Approach (SHERPA) [14]: It uses a prepared checklist to identify possible human errors, after that using quantitative method to calculate the probability of each factor, and then using qualitative method to analyze the risk from each factor.
- Generic Error Modelling System(GEMS) [15]: After identifying human factor, using impact analyzer in the quantitative risk model that includes frequency and exposure distributions for threat-asset categories, next use statistical algorithms to this model and develops both risk curves and analyzed exposures for each threat.

Simplified Human Error Potentials (HEPs), based on generic situations, maybe used in QRA.

Example Human Error Potential Values

| Type of Behavior | Human Error Probability |
|---|---|
| Extraordinary errors: of the type difficult to conceive how they could occur | 10^-5 (1 in 100.000) |
| Error in regularly performed, commonplace, simple tasks with minimum stress | 10^-4 (1 in 10.000) |
| Errors on commission, such as typing wrong key or reading wrong display, | 10^-3(1 in 1.000) |
| Errors of omission where dependence is placed on situation cues and memory. | 10^-2 (1 in 100) |

After quantifying the threat probability and impact severity, using threat-resource matrix to get the risk level. Processes after it are in the same way as other risk analysis.

The traditional method mainly use quantitative analysis (R=P*C) quantifying the damage that can be caused by human factor, and the values of assets that exposed to the threat. A number of variants of such risk assessment methods have been developed that vary considerable in scope. These variants include those developed by Computer Resource Controls (Computer Science Corporation), Citibank, and the National Computer Center in the U.K. [11].

Another risk analysis method performed using probabilistic methods is very similar in concept and approach to the traditional method [16]. With the main difference being the methods used to incorporate variability and uncertainty of human factor into the risk estimate. A variety of modeling techniques can be used to characterize variability and uncertainty of human factor in risk, such as SHEL [19] model which considers human as

integrated and not separable component; complex model of risk evaluation whose principle consists in evaluation of each components. The main application area for this method is human risks. It integrates several basic components of human factor analysis.

Some organizations adopt such method which includes two steps [17].

First, implement qualitative analysis of human errors. This step identify human errors, classify them into broad groups, such as deliberate act and behavior error, then sub-categories them into small groups, such as skill-based, role-base, knowledge-based.

Second, choose one method for quantification of human failures. There are several methods can be performed in this step.

(i) Technique for human error prediction: This method provides mechanism for modeling as well as quantifying the human error. It starts off with a task analysis that describes the tasks to be performed by the crew, maintainer or operator. Together with the task descriptions, performance shaping factors (PSF) are collected to modify probabilities. The task analysis is then graphically represented in HRA event trees. The human error probabilities (HEPs) for the activities of the task or the branches are read and/or modified from a THERP table.

(ii) Success likelihood index method-multi-attribute utility decomposition (SLIM-MAUD): The SLIM-MAUD is based on the assumption that the failure probability associated with task performance is based on a combination of PSFs that include the characteristics of the individual, task etc. It further assumes that experts can estimates these failure rates or provide anchor values to estimate them.

(iii) Intent: This method use predefined resource such as file, system etc, and licensee event reports to identify a generic list of potential errors which may be manifested as erroneous acts. From expert judgement, the corresponding human error probabilities (HEPs) in lower and upper bounds were generated. Normalized importance weights were also computed for each of the performance shaping factors. The specific ratings for the PSFs together with these generic weights were then used to compute a composite PSF score, to which is mapped onto an HEP distribution. The HEP for the decision-based error in a specific situation is thus obtained. A point to note here is that the HEPs then obtained are based on expert judgement and not empirical based. These values should be used judiciously and replaced when operation data are available.

Some methods for human error analysis are using quantification methods which use a structured performance shaping factor (PSF) approach [18]. With this method it is possible to determine the contributions of individual PSFs to human error goals. There is a method that is embedded within the systematic Human Error Reduction and Prediction Approach. This human error analysis method consists of a computerized question—answer routine which identifies likely errors for each step in the risk analysis.

The character of Smith-Lim approach is using more sophisticated data structures in risk modeling. It uses matrixes and trees. One matrix formed a model that mapped generic human behavior threats onto generic targets. Using linguistic variables, each threat-target pair is evaluated using a hierarchy of event trees. Risk is assessed by plotting the evaluated system vulnerability and impact on another type of matrix, a linguistic algebra matrix map.

A different method uses interviews to collect information and then develops scenarios of possible undesired and damaging events. In developing scenarios, considerations include disclosure of information to unauthorized individuals and organizations, loss of information, and inability to access company information due to computer malfunction or loss of communications. Once the scenarios are complete, using qualitative method to rank them according to how severe the effects of their damage or loss would be, then ranking the probability of scenarios (frequent, probable, occasional, remote, improbable). After severity and probability levels are determined for each scenario, compare them to a predetermined set of categories that define risk levels and required actions. This method mainly uses qualitative analysis.

Some companies consider themselves to be risk averse and are particularly concerned with lost of customer confidence, as well as monetary and productivity losses. As such, they use the following method to analyze risk of human behavior. The process of risk analysis is:

Evaluate threats→rank impact of damage→assign risk level to each area of vulnerability. The first step is to evaluate possible threats to information security caused by human factor, consider the likelihood and consequences of the threat occurring. Elements considered in ranking risk includes: unauthorized disclosure, modification, or

destruction f information etc. the potential consequences includes: monetary loss, productivity loss, loss of customer confidence. After that, risk level is assigned high, medium, or low for each of vulnerability to show the possible effect of damage if the threat were to occur. Then use matrix to assist in its analysis of risk as shown in the following table:

| Areas of vulnerability and possible effects of damage | Risk of monetary loss | | | Risk of productivity loss | | | Risk of loss of customer confidence | | |
|---|---|---|---|---|---|---|---|---|---|
| | H | M | L | H | M | L | H | M | L |
| Unauthorized disclosure, modification, or destruction of information | | | | | | | | | |
| Destruction of hardware,system , software | | | | | | | | | |
| Inadvertent modification or destruction of f information | | | | | | | | | |

After completing the matrix, assign a composite risk level to each of vulnerability on the matrix. This is done by considering the potential types of damage identified under each area of vulnerability and judgmentally assigning a risk level of high, medium, or low to each area.

## 4. DISCUSSION

From analyzing the types of risk management for human behaviors, it is apparent that qualitative measure is the main component of most method, and the quantitative measure often aids it with leveling some resource into a certain number scale.

In an IT enterprise, insiders and outsiders will bring the same significant peril to information security. A security manager should construct a safety policy considering the human issues during implementation. For the large-size company, the simple quantitative or qualitative measure may not have the capability to accomplish the risk analysis. Thus, as a whole view, we prefer the method which combines the two methods together. First, use qualitative measure to classify the human behavior sources as small groups, then, follow the three steps in quantitative measure to obtain the specifications.

Other methods with quantitative measure can be performed in some given situations. For example, a manager who wants to introduce a countermeasure which has been assessed in advance will execute the approach with quantitative measure so as to get the true cost of loss. The “low/medium/high” expression is void for him.

For those small or middle size companies, which have no requirements in quantification of the cost of risks, the qualitative methods are more efficient and useful. The human factors in these companies are less complex than in those large-sized ones, so sometimes there is no need to estimate the resources costs and the probabilities of their loss. Using qualitative method also can achieve the results as from quantitative risk analysis.

## 5. CONCLUSION

Some of these mentioned methods can reduce the problem caused by human factor in IT enterprise, but they still have some disadvantages and incompleteness, such as the vagueness of prediction or the redundancy of the method steps. The main limitations are inherited from quantitative and qualitative measures. As the sub-approach of quantitative measurement, methods may cause plenty of work load on estimating the probability and cost of the occurring loss. On the other hand, qualitative measure leads its branches into a situation which it only develops risk analysis and management procedures for small to medium-sized organizations. In large-size IT enterprises, there are more people involved in the security policy. Too many managers and employees make the human factors more complex. In this case, to clear the vague human factors means more plentiful workload.

Also, there are still a lot of unfinished blanks in this field, it is anticipated by those researchers that feedback from users will result in modifications and improvements to their methodologies. For instance, some scientists focus on the inter-domain research in behavioral science to master the quality- and safety- critical risk analysis processes. They have already tried their research in industry [20].

## 6. REFERENCES

1. Jean Hitchings. “Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology” Computer & Security, Vol. 14, Issue. 5, 1995, pp. 377-383

2. Sacha Brostoff, M. Angela Sasse. “Safe and Sound: A Safety-Critical Approach to Security” NSPW 2001 Conference Report, Cloudcroft, New Mexico, USA, September 10-13, 2001

3. Gautam Biswas, Kenneth Debelak, Kazuhiko Kawamura. “Applications of qualitative modeling to knowledge-based risk assessment studies” Tullahoma, Tennessee, United States, ISBN:0-89791-320-5 Year of Publication: 1989 pp. 92 - 101

4. Keshnee Padayachee “Information security and risk management: An interpretive study of software risk management perspectives” Port Elizabeth, South Africa, ISBN:1-58113-596-3, 2002, pp. 118-127

5. Muninder P. Kailay, Peter Jarratt “RAMeX: a prototype expert system for computer security risk analysis and management”, Computer & Security, 14 1995, pp. 449-P463

6. Zbigniew Ciechanowicz “Risk analysis: requirements, conflicts and problems”, Computers & Security, Vol. 16, Issue 3. Elsevier Science B.V. 1997 pp. 223-232

7. W.G. de Ru, J. H. P. Eloff. “Risk Analysis Modeling with the use of Fuzzy Logic”, Computer & Security, Vol. 15, Issue. 3 Elsevier Science B.V. 1996 pp. 239-248

8. Michael E .Whitman “Enemy at the gate: Threats to information security”, Volume. 46, Issue. 8 (August 2003) Year of Publication:2003. pp. 91-95

9. P. Guymer, G.D. Kaiser, and T.C. McKelvey “Probabilistic Risk Assessment in the CPI”, Chemical Engineering Progress, January 1987 pp. 31-45

10. Tullahoma, Tennessee. “Applications of qualitative modeling to knowledge-based risk assessment studies” Year of Publication: 1989 pp. 92-101

11. Saltmarsh, T. J., & Browne, P. S. (1983). “Data Processing - Risk Assessment” In M. M. Wofsey (Ed.), *Advances in Computer Security Management*. Bath, Avon, UK: Wiley Heyden Ltd (1 ed., Vol. 2, pp. 93-116)

12. J.C. Williams, A data-based method for assessing and reducing human error to improve operational performance, 4th IEEE conference on Human factors in Nuclear Power plants, Monterey, California, 6-9 June 1988, pp. 436-450.

13. Swain, A. D., and H. E. Guttman, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications* NUREG/CR-1278, Sandia National Laboratories 1983.

14. Embrey, D.E.. *SHERPA: a systematic human error reduction and prediction approach. Paper Presented at the International Topical Meeting on Advances in Human Factors in Nuclear Power Systems. Knoxville, Tennessee.* , 1986

15. J. Reason. “Generic error-modelling system (GEMS): A cognitive framework for locating common human error forms” In J. Rasmussen, K. Duncan, and J. Leplat, editors, New Technology and Human Error, chapter 7 John Wiley and Sons Ltd., 1987, pp. 63-83

16. P. Guymer, G.D. Kaiser, and T.C. McKelvey “Probabilistic Risk Assessment in the CPI”, Chemical Engineering Progress, January 1987, pp.37-45

17. E.J Henley and H. Kumamoto, Reliability Engineering and Risk Assessment, Prentice Hall, Englewood Cliffs, NJ, 1981

18. Rasmussen, Jens and Svedung, Inge “Proactive Risk Management in a Dynamic Society” Swedish Rescue Services Agency, Karlstad, Sweden, 2000

19. Lin D.and Morris R.(1997), *Dynamics of Random Early DetectION* September 1997

20. http://www.vtt.fi/nuclear/riskanalysis/#