Risk Assessment for Product-oriented and Knowledge-based Companies

Liang Zhang Gang Luo
Email: liazh885@student.liu.se Email: ganlu417@student.liu.se
Supervis*or:* Shanai Ardi
Email: shaar@ida.liu.se
Project Report for Information Security Course
Linköpings universitetet, Sweden

Abstract

Risk assessment which is a crucial part of risk management process is widely used in many industries. This assessment can help to identify the potential problems and reduce the risks to an acceptable level. Companies might use different process and methods for the risk assessment. This paper focuses on two particular kinds of companies; Product-oriented Company and Knowledge -based Company.

The objective of this paper is to perform the risk assessment to these two types of companies. According to the specific characteristics of each company, different analysis methodologies are chosen and applied. Reflection and lessons learned are also provided in the end.

Key words*:* Risk Assessment, Product-oriented, Knowledge-based, FMEA, ETA

1. Introduction

According to the types of final products or the service provided to customers, companies can be divided to many categories. Two types of companies are investigated in this paper. The first one is the Product-oriented company. This type of organization purely focuses on its product and innovation. It studies the market and its own resources, attempting to create a better market-oriented offer than the competitors. However, the company's knowledge about its customers is often vague and general [1].

The other type of company is the Knowledge-based company, in which knowledge is considered as the most strategically significant resource. This knowledge is embedded and carried through multiple entities including organizational culture and identity, policies, routines, documents, systems, and employees. The ability of a firm to integrate knowledge held by individuals within the organization creates its competitive advantage [2]. Knowledge is created and held by individuals, not organizations [3]. So in this type of company, the employees are the most important assets to the company.

2. Background

A hypothetical anti-virus software company which has approximate 60 employees is created by us to simulate the product-oriented company. The core business of this company is providing anti-virus software with high scanning performance and safe-protect capability to the customers and also providing technical support for the security issues. Most of the engineers are working in the Research and Development Department. An anti-virus upgrade package is delivered per two days. Customers can update their anti-virus software on line. The competition of the anti-virus software market is very fierce as the anti-virus technologies are rapidly developed with the popularization of internet and there are many companies as the competitors in the anti-virus software industry.

As the technical core of an anti-virus software product is a powerful anti-virus engine with a continuously updating virus database, and also in order to take advantages in the competition with other companies, the technology innovation and development are the most crucial concentration of the company. Most of the customers only enjoy this security service. They know it is necessary to have the anti-virus protection for their IT device whereas customers lack professional knowledge about how this technique is realized and what potential threats or security risks they will face. So the requirements from the users are not precisely defined.

The corresponding hypothetical company for the knowledge-based company is a consultant company with 40 consultants. The core business of this company is to provide professional consultants to the IT companies which lack human resource for projects or need particular

technical supports. The employees of this company are the persons with professions in the computer science, software engineering and telecommunication.

The competence and experiences of the employees are the vital resource for the company and the aim of this type of company is to utilize and integrate all these knowledge resource to provide professional and effective consultant service to the customers than other competitors.

3. Theoretical Methods

There are many well-developed theories and methodologies of the risk assessment in the literature. For example, HAZOP (Hazard and Operability studies) which is originated in ICI is a qualitative risk analysis technique that is used to identify weakness and hazards in a processing facility [5]. FTA (Fault Tree Analysis) which developed by Bell Telephone Lab in 1962 is a technique to use logic diagrams that display the state of the system and the relation between system failures. SWIFT (Structured What-If Technique) provides a method in which one uses the lead question – what if – systematically in order to identify deviations from normal conditions.[5] According to the different companies' property and types, proper methods should be chosen to carry out the risk assessment. Within this paper, two kinds of fundamental methods are presented for the product-oriented company and knowledge-based company.

3.1 FMEA analysis

Failure Modes and Effects Analysis (FMEA) [5] is a widely used method to reveal the possible failures and enhance the quality of the product. The FMEA can help to identify potential failure modes, determine their effect on the system or to other components, and evaluate the criticality level for the failure so that it can assist the engineers improve the quality of products during the development phase.

FMEA was developed in 1950s and is a mandatory requirement in the aerospace and automobile industry as it is an effective way to reduce the potential threats. This method is widely used in the modern industry and in several enterprises, a FMEA analysis is required to be included as part of the design process in order to provide reliable, safe, and customer pleasing products.

FMEA is an inductive and qualitative method which can be successfully executed as the following steps [6];

- Identify the functional components of the product or system
- Identify the failure modes of the components
- Evaluate the effect caused by the failure modes on the system and other components
- Evaluate the likelihood of the occurrence, the severity and the detection rating of these failures.
- Prioritize risks with Risk Priority Numbers (RPN)

According to the IEC 60812, Edition 2, Failure modes and effects analysis [4], the action and mitigation taken to handle the failures can also be considered in the FMEA analysis. This area is not discussed in the paper as the main purpose of the FMEA is used to identify the Risk Priority for the target product.

3.2 ETA analysis

Event tree analysis (ETA) is another kind of risk assessment method which is widely used to identify the various outcomes of an event in safety and mission-oriented systems. In many scenarios, an initiating event may result in a wide spectrum of outcomes. In most systems, barriers are designed to stop or reduce the effects of the initiating event. Examples are fire fighting systems and gas detecting systems.

Event tree analysis is an inductive method to analyze the progress. It is based on binary logic in which an event either happens or not. It starts with an initiating event, and is followed by some barriers to protect the system. With the true or false value for each barrier, a series of possible paths can be generated. The consequences are followed through these paths. Each path is assigned a probability of occurrence so the probability of the possible outcomes can be calculated [9]. This method can be used both qualitatively and quantitatively, depending on the objectives of the analysis [10].

An event tree analysis is usually carried out in seven steps [8]:

- Identify (and define) a relevant accidental (initial) event that may give rise to unwanted consequences
- Identify the barriers that are designed to deal with the accidental event
- Construct the event tree
- Describe the (potential) resulting accident sequences
- Determine the frequency of the accidental event and the (conditional) probabilities of the branches in the event tree
- Calculate the probabilities/frequencies for the identified consequences (outcomes)
- Compile and present the results from the analysis

4. Practice and Analysis

4.1 FMEA for the product-oriented company

In a product-oriented company, the product itself is the core competitive power to obtain the customers and market share. To the hypothetical anti-virus company, the

professional performance and reliability are the most important traits of the anti-virus software. Though scientific design processes and modern development model with fully testing mechanisms and help to ensure the product works and protect customers against the failure, some problems are still hard to detect during the developing phase and which might cause potential failures.

The FMEA method use a systematic way to consider all the possible failure situations and their interactions on other models so that a more complete and sophisticated analysis is made to assist the engineers to minimize the likelihood of those failures.

To do an effective FMEA analysis, a worksheet should be created for each stage in the life-cycle of the system. This worksheet mainly contains the following columns [5] [6] [7]:

- Function (columns 1): The function performed by the system components.
- Failure mode (columns 2): All the possible ways the components can fail to perform its function are listed in this column.[5]
- Failure cause (columns 3): The reasons cause the failure mode happen.
- Failure effects (columns 4): The consequences of each failure mode and the influence to the system.
- Severity rating (columns 5): Failure effect ranking. This number can be given from 1 (no danger) to 10 (critical). It helps engineer to prioritize the failure mode and their effects.
- Occurrence rating (columns 6): Frequency (probability) for the specific failure mode. The number can also be defined from 1 to 10. A higher number indicates a higher frequency.
- Failure detection (columns 7): The methods of detection of the failure mode
- Detecting rating (columns 8): From these controls an engineer can learn how likely it is for a failure to be identified or detected. The number is again from 1 to 10. A high detection number indicates that the chances are high that the failure will escape detection.
- Risk Priority Number (columns 9): After ranking the severity, occurrence and detectability the RPN can be easily calculated by multiplying these 3 numbers: RPN = Severity rating x Occurrence rating x Detecting rating [6].

A FMEA worksheet [Appendix A] is made by us for this product. According to the characteristics and main functions of the anti-virus software, four core businesses areas are abstracted as the Function items in the first column. For each function, we consider the possible ways of failures as the Failure mode which could occur and analyze the corresponding root cause for these failures. Then the effect or the influence of these failures which related to the Severity rating in the column 5 are analyzed and the actions to detect these failures are defined which determine the Detecting rating in the column 8. After that, three important indexes are calculated. (As this anti-virus company is a hypothetical one, so the data is mostly come from author's experiences and hypothesis). Finally, the RPN is calculated by multiplying these three indexes; Severity rating, Occurrence rating and Detecting rating.

The outcome of this worksheet is the RPN. It is easy to determine the areas of greatest concern with the PRN. From the results, the license verification and manual virus scan get a high RPN number. It means more attentions and efforts need to be paid in these areas. With the severity rate, occurrence rate and detecting rate for each failure mode, corresponding strategies and improvements can be made during the development to solve these potential problems.

It is not always the failure modes with the highest severity numbers that should be treated firstly. Because there could be failure mode with less severity but has a high occurrence rate. So the RPN is the most accurate and persuasive index to show which failure modes should be handled with the highest priority. Once the actions against the failures have been implemented, a new RPN should be calculated to confirm the improvements.

4.2 ETA for knowledge-based company

For the consulting company, employees are one of the most valuable assets. They accumulate a lot of knowledge in their brains from their previous experience. For the new problems, they could find proper solutions quickly by searching in their knowledge database. The human resources department of the company tries to develop good policies to retain the consultants. When they are doing the risk analysis, they need to consider all the scenarios that would make the employees leave. Event tree analysis method is a good choice because various outcomes could be found from an initiating event.

[Appendix B] is a risk analysis example using the method of event tree analysis by this company. It analyzes what will happen in different situations if a consultant wants to leave. If the consultant withdraws the leave request finally, there will be no loss for the company. The probability is 50%. On the other hand, if the consultant insists on leaving, the company could have two choices for the project that the consultant is working on. One is to recruit a new consultant, and the other is to recruit and make a subcontract. Both the recruiting expenses are the same, which is 20,000 SEK. If the company selects subcontract, then the total expense

will be 20,000 SEK plus the subcontract costs. So the total loss will be 55,000 SEK. If the company wants to recruit a new consultant, there will be two situations for the delay of the project. If there is no penalty, the loss will be only the recruiting fee 20,000 SEK. If there is penalty, the total loss will be the recruiting fee plus the penalty, which will results in 80,000 SEK.

The company applies the event tree analysis methodology and gets four scenarios for the event if a consultant wants to leave. From the four different outcomes, the company can priority them and improve the existing procedures to avoid the worst cases.

5. Reflection

In an FMEA, the attention is in many cases too much on technical failures, whereas human failure contributions are often overlooked [5]. So when the method is applied, the human failure can be considered as a component of the whole product or system. Another limitation of the FMEA is that all components are analyzed and documented, also the failures of little or no consequences [5]. The result is that a large amount of documents are required. This can be improved with a well-defined components prioritized list so that some failure modes with very low influence can be ignored.

There are some negative aspects for event tree analysis too [11]. First of all, there is no standard for the graphical representation for the event tree. For each analysis, only one initiating event can be studied. This method is not well suited for handling common cause failures in the quantitative analysis either.

6. Conclusions

For a product-oriented company, the company concentrates more on the technology and quality of the products. The FMEA method provides a systematic view of the products and helps engineers to detect the potential failures so that the action against the problem can be taken in advance.

For a knowledge-based company, accumulated knowledge and experience is the most valuable asset. Usually there are two existing forms of knowledge: the written knowledge and the experience owned by the employees. All scenarios that might do badly to the knowledge should be evaluated when doing risk analysis. Event tree analysis is such a methodology that visualizes the event chains in different scenarios following an initiating event. The results may be used to identify improvement opportunities and make recommendations for improvements.

References

[1] Lona Matheson. Comparing Product Oriented and Customer Centric Organizations. 2006 http://e-articles.info/e/a/title/Comparing-Product-Oriented-and-Customer-Centric-Organizations/

[2] Knowledge-based theory of the firm http://en.wikipedia.org/wiki/Knowledge-based_theory_of_the_firm. Retrieved on 2009-4-23

[3] Grant, R.M. " Toward a Knowledge-Based Theory of the Firm," Strategic Management Journal (17), Winter Special Issue, 1996, pp. 109-122

[4] IEC 60812, Edition 2, Failure modes and effects analysis, January 2006.

[5] T. Aven "Risk Analysis: A ssessing Uncertainties beyond Expected Values and Probabilities" 2008 John Wiley & Sons, Ltd. ISBN: 978-0-470-51736-9, pp. 64-69

[6] Onodera, K. "Effective techniques of FMEA at each life-cycle stage" Reliability and Maintainability Symposium. 1997 Proceedings, Annual,13-16 Jan. 1997 Page(s):50 – 56

[7] Failure mode and effects analysis from Wikipedia http://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis . Retrieved on 2009-4-23

[8] Marvin Rausand, Arnljot Hø yland, " System Reliability Theory: Models, Statistical Methods, and Applications" , Wiley-Interscience, pp. 108, ISBN 0-471-47133-X

[9] " Quantified Risk Assessment Techniques – Part 2 (Event Tree Analysis - ETA)", http://www.theiet.org/factfiles/health/hsb26b.cfm?type=pdf" , 2009. Retrieved on 2009-4-13

[10] Marvin Rausand, " System Analysis - Event Tree Analysis", http://www.ntnu.no/ross/srt/slides/eta.pdf, 2005. Retrieved on 2009-4-17

Appendix A

FMEA worksheet for the anti-virus company

Function	Failure mode	Failure cause	Failure effects	Severity rating	Occurrence rating	Failure detection	Detecting rating	Risk Priority Number (RPN)
Scan suspect files to find the virus manually	Some unknown viruses are ignored by the scan	Malicious viruses may have a new format or be pretended as a normal format	Viruses cannot be detected and cause safe leaks	10	3	Update the virus database and do the scan again.	8	240
	Some unknown viruses can not be removed completely	The virus can clone itself repeatedly or change the name automatically	The viruses cannot be killed and do harm to customers' system	10	5	This kind of virus will be isolated and stopped and give alert to customers	5	250
Scan the viurus automatically with real-time protection	Real-time protection is violated by viruses and cannot work	Intelligent virus can find the anti-virus processes and block it	Automatic scan doesn't work and cannot protect customers' system in real time	8	4	Give a high priority of the anti-virus processes and avoid unauthorized modification.	4	128
	The real-time scan cost too much resource of users' computers	Anti-virus software require adequate resource to work or the customer's computer with a low device configuration	Work efficiency and performance of customers' computer will be affected.	3	4	Optimize the software design and update the device configuration of customers.	2	24

Function	Failure mode	Failure cause	Failure effects	Severity rating	Occurrence rating	Failure detection	Detecting rating	Risk Priority Number (RPN)
Update the virus database	Users cannot retrieve the latest database from server	The network between the database and the customers' computer doesn't work or the database is crashed	Customers cannot get the latest virus database.	7	2	Maintain the database with high reliability and insure a robust network connection	1	14
	The update database package cannot be installed successfully	Some software or hardware conflicts happen in customers' computer	The local virus database cannot be updated	7	1	Provide a guideline and effective technical supports to customers	1	7
Licence verification	Licence is cracked illegally	Hackers or some individuals crack the licence to use the software free of charge	Cause economic loss to Anti-virus company	9	7	Improve the anti-pirate technologies and seek help to the law	7	441

Appendix B

Event Tree Analysis for the consult company