MIKLÓS ZRÍNYI NATIONAL DEFENCE UNIVERSITY

Security risk analysis
# of informatics systems
in the defence sector

by

Mrs Márton Schutzbach

Thesis resume

Consultant:

Dr. István Kun

Dénes Gábor Technical College

Budapest, 2004

1. Definition of the scientific problem

The effort to gain information and the protection of the information gained are as old as human societies. Since the advent of computers, and then, with the development of networks, the means of gaining, processing, relaying, storing and safeguarding the information has considerably changed. The United States launched the development of the requirements of informatics security assessment as early as the late 1970s. Later on, similar issues were nationally released in several countries. Furthermore, with the spreading of informatics networks, a demand emerged, as well, to work out requirements based on internationally standardised agreements. In Hungary, the Prime Minister’s Office publicised a national recommendation called ‘Security Requirements of Informatics Systems’.

Because of the rapidity of the technological progress, the changing of the risk factors, and the introduction of the necessary security measures, it is a hard task, and it also continuously poses new problems, to ensure the security of informatics systems.

The terrorist attack on America starting September 11, 2001, indicated the necessity of the preparation for the most unexpected, both on the part of the informatics leaders and the system administrators.

The increasing application of informatics systems, apart from its advantages, poses new hazard and risks in terms of the infrastructure of the NATO alliance, national infrastructure and the defence sector infrastructure as well. In order that safeguarding may be realised and security may be kept, a multilevel protection must be applied according to the priority of the systems to be safeguarded. Also, the fact that there is no perfect security is to be accepted.

It is included in EU Resolution 2002/43 that the nations should launch informational and educational campaigns with the purpose of increasing the knowledge of how to ensure security for computer networks and information protection. In addition, these campaigns should also focus on the support of the information security management’s practical methods based on international standard agreements. Hungary will gain a European Union membership in 2004. Experts must conduct studies to discover the influence of Euro-Atlantic membership on the security requirements.

Based upon the above, I drew the following conclusions:

- The field of informatics security has become in the focus of attention worldwilde; researches are being made to provide answers to its theoretical and practical questions.
- Demands, both national and international, have emerged to develop requirements based upon standardised agreements.
- An exploration of the risk and threat elements needs to be made so that protection can be employed. Because of the wide panorama of the risk factors, the exploration should be done by applying a many-sided, detailed approach.
- Achieving perfect protection seems wishful thinking, thus special focus is placed on risk assessment that determines the importance and the value of the data to be protected. While considering the risks, it is possible to make a decision as to the measures to be taken, and as to the protection level that is proportionate to the value to be protected. It is to be decided whether or not the extent of risk that remains is acceptable; *the unacceptable extent of the remaining risk* necessitates taking further security measures.

2. Research goals

When starting the thesis, I intended to aim at the following:

- I will study and compare **risk analysis methods and methodologies** that have already been successfully employed in the analysis of the security of informatics systems. In this, I will bear in mind that a study of the working elements and the weaknesses may help conclude to results that can be utilised in the development of a method by which to study the informatics systems of the defence sector, which is in fact the main purpose of mine.

- **I will develop a methodology of risk analysis for the informatics systems in the defence sector,** with regards to the experience and requirements, both national and international, as well as to the particularities of the defence sector.

- Furthermore, my objective is to explore in details and to classify the factors posing threat to informatics security, since the success of the risk analysis to a large extent depends on the knowledge of the threatening factors.

3. Research methods

In order that the set targets may be achieved, I applied the following methods:

- I studied the professional literature, both national and international, related to the thesis subject, and the major international regulations on security, and the statutes that are in effect.
- On issues of security, I conducted consultations with the security experts of the following Hungarian firms and organisations:

  Miklós Zrínyi National Defence University, Dénes Gábor Technical College, János Bolyai Military Technical College, Budapest Technical and Economic University, Kürt Computer Systemhouse Inc., Synergon Informatics Inc., Takarékbank Inc., Disaster Management Directorate of Somogy county, Civil Defence Directorate of Budapest.
- I attended conferences to publicise my views on informatics security for a considerably huge public and to collect views, statements in terms of my work, on the one hand, and to utilise the statements and conclusions of the conferences, on the other.
- I studied the most frequently applied methods of risk analysis in the literature of the profession. I explored laws, I made conclusions and I listed the possible ways of utilisation.
- I analysed the possibilities of the mathematical methods applied in risk management.
- I studied a field of the informatics system of the defence sector, and I applied some of the steps of the risk analysis method developed by me.
- I evaluated the results of my researches, experience and observations.

4. The description of the studies conducted by me (the structure of the thesis)

The thesis subject is structured in the following chapters:

- In the **Introduction,** I listed the motivations for the development of the thesis, and I defined the goals and the methods applied.
- In **Chapter 1,** I dealt with the possibility of the provision of informatics security,

I reviewed the major international regulations on security, the statutes that are in effect and the security standards. I indicated the particularities of the informatics security of the defence sector. I studied the influence of the life cycle of the informatics systems on security.

- In **Chapter 2,** I sought the answer, by studying and comparing the risk analysis methods, to the question of how the many risk analysis methods could be made applicable or be completed for their use in the informatics systems of the defence sector, or how such a method could be developed.

  In the comparison, CRAMM, ITB Recommendation No. 8, COBIT, MARION and IT-Grundschutzhandbuch were included. My selection was based upon the following aspects:

  - Due to the fact that Hungary is about tho join the EU, the subject of informatics security needs to be studied, by me, in the member states of the European Union.

  - Instead of dealing with all the existing recommendations, methods and methodologies, I selected the best known ones such as the French MARION and the German IT-Grundschutzhandbuch, a COBIT made by an international organisation, the English CRAMM, and, last but not least, ITB Recommendation No. 8, because this Recommendation is known as well as used in whole as a basis for operation by each organisation dealing with informatics security in Hungary.

  I named the advantages and disadvantages of the selected methods, and I made their comparison in terms of the following aspects:

  - Level
  - Independence
  - Classifiability
  - Feasibility
  - Applicability
  - Analysis range
  - Result Display
  - Cost-effectiveness
  - Updating
  - User-friendliness

I displayed the analysis of the studied methods in a graphical layout so as to make it more understandable.

In this chapter, I also studied the most frequently used hazard analysis methods – **F**ault **T**ree **A**nalysis (FTA), **E**vent **T**ree **A**nalysis (ETA), **F**ailure **M**ode and **E**ffects **A**nalysis (FMEA), **Haz**ardous and **Op**erability Reviews (HAZOP), **F**ailure **M**odes **E**ffects and **C**riticality **A**nalysis (FMECA).

I found it important to demonstrate the applicability, in the field of risk management, of a special mathematical method called "fuzzy theory".

One of the purposes of the "fuzzy theory" is to develop methods that can classify and resolve problems that are too complex or hard to define by the application of conventional methods.

The determination of the limits of the appropriate set was impossible to accomplish with notions that were *not defined precisely* (e.g. small, medium size, huge). In such cases, the elements relation to the set could not always be determined with certainty, therefore I designated these values by the successive elements of a continuous scale. I summarised the advantages of a risk analysis supported by "fuzzy logic" as follows:

- It is possible to further utilise the numeric results.
- The system structure is simple. There is easy access to the rule base construction.
- It is capable of handling data, no matter if they are precisely and loosely defined.
- Its view is close to one's everyday life view.

- In **Chapter 3**, there is a methodological guide as to the risk analysis of the informatics systems in the defence sector. I highlighted the most relevant factors that supported me in my decision to develop a new methodology for studying the informatics systems in the defence sector.

This chapter includes the assisting means that can be used at certain steps in risk analysis. These means are used to facilitate communications and transparency. They also provide information about the informatics system and the organisation as well as the risk factors.

After studying the technical literature available, especially, by studying and comparing the analysis methods described in Chapter 2, and drawing conclusions from this, I find that risk analysis is best accomplished in the following 5 steps:

(1) ASSESSMENT OF CONDITIONS
(the aim is to get full information about the system and the requirements)
(2) IDENTIFICATION OF HAZARDS, IDENTIFICATION OF RISK FACTORS
(3) ASSESSMENT AND IDENTIFICATION OF DETERIORATING EFFECTS AND DAMAGE
(4) IDENTIFICATION OF DAMAGE FREQUENCY
(5) IDENTIFICATION OF RISKS

Methodologically, the advantages of the five steps are transparency and feasibility (applicability). I also find it essential that I should demonstrate the applicability of the steps of risks analysis.

The sample selected for this purpose is part of the defence sector; it belongs to the informatics system of the Civil Defence Directorate of Budapest.

Due to the wide range of risk factors, I accomplished classification and grouping, with special regards to the risk factors particularly occurring in the informatics systems in the defence sector.

- The overall risk analysis of an informatics system is a huge task. Therefore, in the accomplishment of this task, it is advisable to make some classification so as to ensure transparency. In **Chapter 4,** I dealt with the issues of environmental infrastructure, the applications, cryptography and networks.

The analysis of environmental infrastructure includes the analysis of the area of the building of the computing centre, the building itself, the rooms in the building, the transmission cables, all the air-conditioning equipment, the water pipelines, lighting, phone service, electric power supply, and others.

The organisation may find certain items of environmental infrastructure to be of high importance, and may find it useful that these should be analysed.

The operation of informatics applications is an important field of informatics security, therefore, I gave a more detailed study to the necessary availability, the assessed financial losses, and the probabilities of failures. Using scores to evaluate the above factors, the possible risk can be determined in numbers.

Cryptography is basically designed to ensure by means of algorithms that confidential data can only be accessed by those authorised to.

I named both the advantages and disadvantages of the two types of cryptography methods, i.e. the one with a symmetric key and the one with an asymmetric key. I dealt with mathematical problems providing a base for the algorithms of cryptography, and their applications.

I studied the influence of the progress of the informatics systems on cryptography security.

I took into account that, apart from the fact that cryptography can be cracked, the access of data by unauthorised ones takes place mostly because of the insufficient protection of the communications channel or some human factors or the insufficient security level of the organisation of data handling.

Although they have several advantages, the networks that are becoming bigger and bigger have increased the security risk factors. This does not mean that it is only individual stations that will have a future. Networking without the necessary security measures, however, may have considerable risks.

In this subchapter, I dealt with collapses of systems, frauds, major errors, studies of attacks, computer viruses, worms, and Trojan programs.

In order that the network security of an organisation may be provided, measures that have already been proven workable ought to be used, e.g. security measures, security planning, firewalls installed, application of crack-protection systems, or the use of the latest virus-killer softwares.

In the analysis, it is necessary to study the applicability of the measures that have already been proven workable.

In the analysis of attacks from the outside, an assistant to risk analysis could be the process of “ethical hacking”. To support the organisation being studied, the information coming from this hacking can be utilised by highly trained experts or by a group of highly trained experts.

In fact, the success of the risk assessment process is considerably dependent upon an extensive exploration of the risk factors. To make sure that this exploration would cover all the factors, I classified them, in the first place, as *human, logic, physical and environmental factors.*

In the analysis of certain parts of the informatics systems, I highlighted the hazardous points and situations that need to be studied in a particular field. *It is possible to classify the risk factors in terms of the particular parts of the system.* In addition to the classification mentioned above, risk analysis can further be assisted by a *catalogue of risk factors*. Based upon this, I introduced a system of the risk factors, as classified by five aspects. This classification suggests the introduction of the issue of responsibility too.

- In **the last chapter,** the results are summarised, and the conclusions are drawn. The analysis of the applicability of the thesis is also covered while possible further researches are suggested.

5. Conclusions summarised

The detailed description and analysis of the issues designated as the research goals are accomplished in the thesis chapters, respectively. I drew the following summary conclusions regarding the research goals, respectively:

- I **defined** the basic technical terms that I was using in my thesis. I **reviewed** the statutes, standards and recommendations to be considered while introducing informatics security. I **classified** the standardised requirements of the different security classes.
- Keeping in mind the interests of the defence sector, I **selected** different risk analysis methods, and I **analysed** the their advantages and disadvantages. I created a system of aspects for comparison. Based upon that system, I **evaluated** and **compared** the procedures selected, and I displayed the results of the comparison in a diagram.
- I **analysed** and **compared** the applicability of the two most frequently used hazard analysis methods (**F**ault **T**ree **A**nalysis and **E**vent **T**ree **A**nalysis). I **summarised** the hazard analysis processes that are used all along the whole life cycle of informatics systems.
- I **worked out** a risk analysis methodology guide for the risk analysis of the informatics systems in the defence sector. I **developed** a system of informatics security risk factors.
- I **focused** on certain parts of the informatics system. I **paid special attention** to the relevant security factors of particular parts of the informatics system.

6. New scientific results

In my research of informatics systems security, I consider scientific results the following:

1) The comparative analysis of the selected risk analysis methodologies (COBIT, CRAMM, ITB Recommendation No. 8, MARION, IT-Grundschutzhandbuch).

2) The risk analysis methodology developed for the risk analysis of the informatics systems in the defence sector.

3) Informatics security risk analysis factor classification.

7. The applicability of the results; recommendations

By working out my thesis, I intended to contribute to

- the theoretical and practical development of the field of informatics security;
- the development of the informatics defence infrastructures that could be use in higher education;
- the identification of attacks on the informatics systems, since this identification is the first step of developing a successful informatics security system.

I recommend that my thesis should be used:

- In the informatics system security analysis of the Centre for Crisis and Conflict Management Training and Research that is being established.
- In the development of the training materials of the Centre for Crisis and Conflict Management Training and Research.
- In monitoring the factors that threaten the informatics systems, which helps prevent hazardous situations.
- The general methodology can be applied either directly or through minor modifications while monitoring what has been modified.

- My result can be utilised by the users not only within the defence sector but in the banking sector or the administrational fields as well.
- In higher education, the comparative analyses can directly be utilised in researches.
- To accomplish prevention, the risk analysis methods developed by me can be applied in the security risk analysis of informatics systems in the defence sector.