ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 2012. No. 5(121)
ELEKTRONIKA IR ELEKTROTECHNIKA

TELECOMMUNICATIONS ENGINEERING
T 180
TELEKOMUNIKACIJŲ INŽINERIJA

Company's Information and Telecommunication Networks Security Risk Assesment Algorithm

S. Japertas, G. Cincikas
Department of Telecommunications, Kaunas University of Technology,
Studentų str. 50, LT-51368 Kaunas, Lithuania, phone: +370 37 300985, e-mails: saulius.japertas@ktu.lt, gido@ktu.lt
R. Sestaviskas
Elektrenai Municipal Public Library,
Traku str. 11, LT- 21381 Vievis, phone: + 37068925680; e-mail: ramremster@gmail.com

crossref http://dx.doi.org/10.5755/j01.eee.121.5.1648

Introduction

An information security and protection has the great importance for a state, company or man. At the state level the information security and protection is governed by laws. Meanwhile, at the enterprise level such laws do not exist or are not very clear. But at these days almost all companies and institutions dispose the information which must be protected. In the some companies the information's component consist of almost 100% production. The loss of information or its modification can have not only economic consequences but also sometimes can be a reason of the disaster with the victims of human. All business enterprises use the Information and telecommunications (ITN) networks. However, the use of such network is associated with the threats to the all network, to the network elements or the business itself. So the company's leaders and security service has the problem how to protect information from internal and external threats. The information security's one of the most important aspect is the information loss risk assessment. In the market it is possible to get such risk assessment tools. But they are expensive. Therefore, many of the small and medium-sized companies are not able to use such tools to assess the information loss risk. In addition, many of the existing threats assessment algorithms are adapted to needs of the state or big companies. Therefore, it is not appropriate to use these algorithms in the small and medium-sized enterprises. Some of the international agreements in cyberspace (eg, ACT) can also cause problems for such companies in the information security field.

The aim of this work is to create a risk assessment algorithm which is suitable for the medium and small-sized businesses. In order to do this it is necessary to analyze the company's ITN threats and vulnerabilities.

Information and telecommunications networks security

Today it is difficult to find the company which the information networks are not connected to the global telecommunication networks. Any transmission of data over those networks increases the risk factors for the company's activities. Timely and appropriate information protection reduces or completely eliminates the consequences which are related to the information leakage, loss or other factors. These factors sometimes can be very painful for the company.

The information risk assessment practically is hardly realized due to the necessity to evaluate all losses. These losses must include and the losses which would be incurred due to the failure of the company's security mechanisms. It is difficult to evaluate the current security level because this evaluation is subjective. However, it can be stated that it is necessary to increase the information security level.

Every company should take a safety and protection planning. And this plan must be constantly reviewed due to the dynamic changes of the business and surrounding environmental. The ITN security development cycle is illustrated in the Fig. 1.

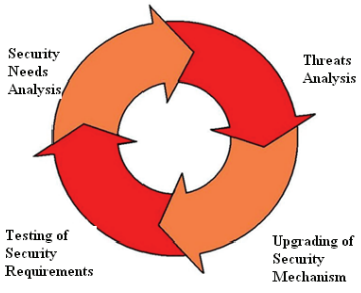

Fig. 1. Information security development lifecycle

The basic information security goals can be summarized in three principles: confidentiality, integrity and accessibility. The real security threat realization is known as an attack.

According to research group Gartner Group methodology, the company's information security can be assessed by the main 6 levels [1]:

- Level 0 (Unaware): the company's management does not focus on information security and no one is responsible for this;
- Level 1 (Aware): the company has some knowledge about information and its security. But this understanding is fragmented and inconsistent;
- Level 2 (Reactive): the company's leaders understand the importance of the information security to the successful development of the company. But company's cultural and organizational barriers does not lead to progress in this field;
- Level 3 (Proactive): the company's leaders understand the information security as necessity for the business improving. In this field the main company's units participate actively;
- Level 4 (Managed): the company understands the information and information security as the critical factor for its activity. The policies and rules are documented and understood.
- Level 5 (Effective): Information security is an integral part of company's culture. The information security staff there is appointed. There is the security strategy and other documents related to risk management.

Risk management methods

The risk management is the instrument which let organize an effective information security framework in the company.

Currently, there are many methodologies for the risk assessment [2-4]: qualitative, quantitative, tabular, Octavia and others methods. But in generally all they are made up of seven main parts [3, 4]:

- The setting of the risk management policy;
- Appointment of staff who will carry out a risk management in the company;
- The selection of the risk assessment methodology and tools;
- Identification of risks;
- Determining whether the level of risk is acceptable;
- Risk reduction or elimination;
- Monitoring of the risk management process.

The most popular and commonly used are the instrumental risk assessment tools. The vast majority of risk analysis tools are developed in accordance with the ISO / IEC 27002 standard (replaced an older ISO / IEC 17799 standard), so the new versions of software are oriented to the new standard.

Cobra, *RA2 Art of Risk*, *CRAMM*, *Risk Watch* are the most famous examples of such instrumental tools [2, 4–7]. However, as mentioned above, they are an expensive tools and require a high professionalism of the staff. Therefore, the medium and small businesses do not use them.

A quantitative method. The quantitative risk assessment method uses parameters: the number of annual events *ARO*, the loss caused by single event *SLE*, the potential losses during the year *ALE* and others. These parameters are related as [3]

$$ALE = ARO \times SLE . \quad (1)$$

In work [8] it is suggested to assess the risk quantitatively by using such parameters as factor of the vulnerability (*FA*), expected one-time losses (*EOTL*), the incident's annual frequency index (*IAFI*), the expected annual loss (*EAL*). *FA* is damage to property (the percentage of). *EOTL* is a monetary loss due to the vulnerability of the security

$$EOTL = PV \times FA , \quad (2)$$

where *PV* is the property value.

IAFI shows the frequency of security vulnerabilities over the year. It is quite difficult to set this index because it depends on the probability of an event (which is different in the different companies) and the number of personal which can be related to this event. *EAL* is the expected losses during the year which a company can expect due to the security violations:

$$EAL = IAFI \times EOTL . \quad (3)$$

Instrumental risk analysis tools

As already mentioned, there are many instrumental risk analysis tools in the market and they are all based on certain algorithms and have their advantages and their disadvantages as well.

In particular, it should be noted that not all tools can perform a wide range of functions. The *Cobra* and the *RA2 Art of Risk* work mainly in the framework of ISO standards (we shall call the First Group). Meanwhile, *CRAMM* and the *Risk Watch* perform the much more tasks (Second Group). It can be argued that First Group's tools can be applicable to the companies with the information security up to Level 2 according to the *Gartner Group* method.

In the First Group, the *RA2 Art of Risk* tool is superior to other tools. It has some properties of the Second group. The *Cobra* is no longer updated for a long time. It seems that this product will be removed from the market. The *RA2 Art of Risk* also has a demo version that can be useful in developing the risk analysis and management methodologies.

The *CRAMM* is superior to the *Risk Watch*. The *Risk Watch* has a some modifications dedicated to banks, credit unions, hospitals, power plants and others in order to evaluate information security in the different environments. However, for a full risk analysis it is necessary to use a few tools of the *Risk Watch*. Furthermore, *Risk Watch* is an U.S. product and is more oriented for the U.S. market. *CRAMM*, we think, is the most comprehensive tool. This tool has several versions. One of them is dedicated to such government's institutions as the National Security Authority. The other is used in the large businesses, such as Railway Authority, banks and so on.

Risk analysis and management algorithm

The proposed risk analysis and management algorithm is presented in Fig. 2. It is based on the works [1, 2, 9, 10] and takes into account the small and medium-sized businesses opportunities.

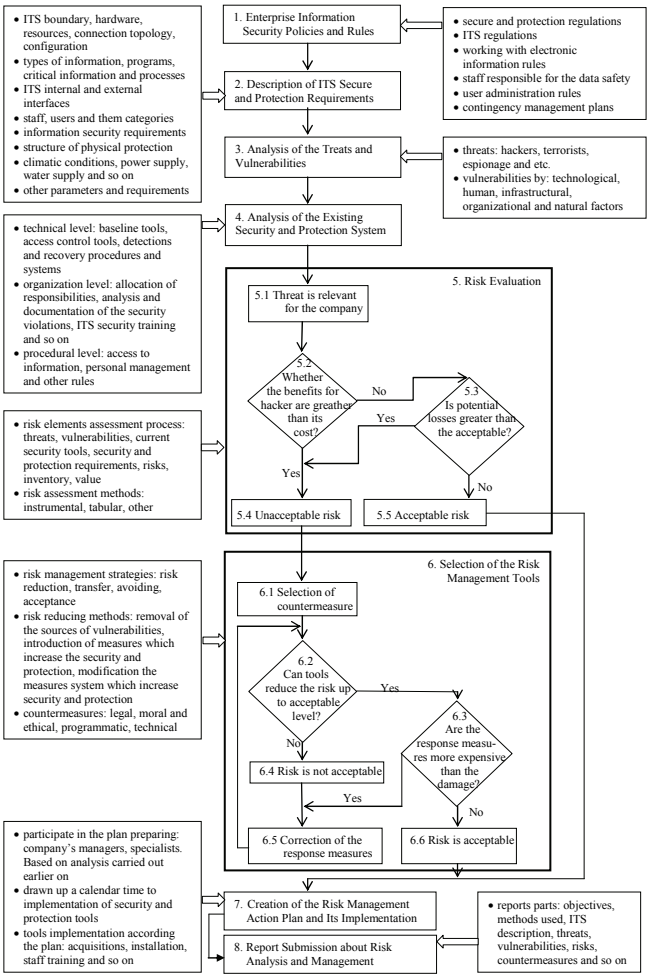

Fig. 2. Risk analysis and management algorithm

The algorithm tries to cover all aspects of risk analysis and management practices and procedures in order to that the algorithm would be as complete as possible. In assessing the security and protection ITN in the enterprise, some steps of the algorithm can be simplified or not included. It is also possible to introduce new elements that are relevant to information security assessment and management in the particular enterprise.

The algorithm consists of 8 steps. It should be noted that this entire algorithm is a closed loop. This means that after step 8 again need to go back to step 1.

Step 1. Enterprise information security policies and rules. Enterprise Information Security Policy is a document in which is defined the enterprise's plans to protect the ITS resources. This policy must be continually updated. The simplest way to ensure a successful security policy is the refusal to prepare an integral document. Only a many number of documents will enable to small and medium-size enterprises develop the security policy which would be flexible and adaptable to the new requirements. A similar opinion is at work [2]. In this document (Enterprise Information Security Policy) should be given the requirements how to use and keep safe the information, how to classify it according to the secure level and so on. This document should include the following parts: safety regulations with the general requirements, the rules for working with all kind of the information, the passwords management policy, the user's identification policy, the users mandate's policy, the virus protection policy, the rules for working with e. mail and so on.

Step 2. Description of the ITN secure and protection requirements. This stage describes the purpose of information systems and its functions, its boundaries, resources, security requirements and so on. Information system description should include the following components: the purpose of the ITS, the objectives and requirements for, ITN boundary, the hardware resources, network topology and configuration, software, the types of the information, internal and external interfaces of the ITN, the categories of the staff and users and so on.

Step 3. Analysis of the treats and vulnerabilities. A threats source can be either of someone's intentional act which is directed to information security breach, or a random situation which causes the damage. Threat detection methodology is usually highly dependent on information systems characteristics.

Step 4. Analysis of the existing security and protection system. In this phase it is assessed the system's resistance (efficiency) to the threats and vulnerabilities which were identified previously. Usually there is evaluated the technical and non-technical (organizational and procedural) levels.

Step 5. The risk evaluation level. The main objective of this stage is to divide the information risks in to acceptable and unacceptable. If there is an unacceptable risk, the risk mitigation measures should be used. The risk management process is omitted if it is an acceptable risk. The step 5.1 shows that the information system due to the violations are vulnerable and therefore it requires risk assessment process. In the 5.2 stage there is compared hacker's benefit and his cost. If the benefits are greater, the motivation of hacker activities must be reduced. In the 5.3 step the potential losses are compared with the acceptable losses. The acceptable level of losses is determined by leaders of the enterprise.

Step 6. The selection of the risk management tools. During this stage the appropriate information risk mitigation measures are selected. They may be technical or organizational. In the 6.1 stage there are studied solutions which effectively reduce the risk. Here is an overview of several alternative solutions and selected the optimal. In the 6.2 stage is checked whether the selected response measures are able to reduce the risk up to acceptable levels. If the measures do not reduce risk to acceptable level, then it is necessary to go to the 6.4 stage (the risk is unacceptable). During the 6.3 stage is evaluated whether the response measures are not expensive than the potential damage and then go to the 6.6 stage. There is considered whether the optimal risk management measures are chosen

Step 7. The creation of the risk management action plan and its implementation. At this stage, there is drawn up a risk management action plan according the

received data in the previously steps. This plan shall be prepared in the presence with the interested managers, project staff and other related professionals in many fields. The analysis of the data can be supplemented and corrected in the same plan if the company's leaders require.

Step 8. After the 7 stage, the preparation of the risk analysis and management report starts. This report should reflect all the main results of the performed work. According this report can be seen the quality and success of the risk assessment and management.

The use of the algorithm. The information's security and protection in the real small company with the staff of 10 people was evaluated by using this algorithm. The company provide its activity in the technological and industrial field (installation of the automation and energy equipment and the trading of its).

First of all, there is performed evaluation of the existing security and protection situation according the 1 – 5 steps. Assessment results are documented (eg, in the form of tables). In this particular case there was defined the 51 vulnerabilities. According these vulnerabilities, there were defined the sources of the threats and potential consequences.

The quantitative estimates according the formulas 2-3 have been carried out after the evaluation of the security and protection situation of this small company. The objective is to evaluate the *TMN*. The quantitative value for each parameter (eg, information, project, etc.) is provided separately (eg, tables). The institution's leader has determined that *TMN* can be 100 Euro. This means that the risk management is not carried out if the loss is less than 100 Euro. According to the result, every potential risks are assigned to three groups: high-loss group, the medium-loss group and the low-loss group. According the company's decision, the loss is the small (low-loss) when < 500 Eu and losses are high (high-loss) when > 1000 Eu. According these calculations, are carried out the remaining steps of: there is selected risk management measures, drawn up the action plan, prepared the report.

Conclusions

1. The existing algorithms for assessing security risks and the instrumental risk assessment tools (which are based on these algorithms) are useful in the government institutions or large companies. Meanwhile, for small and medium-sized enterprises the number of such instrumentals tools in the market is very limited;

2. In this paper is proposed the risk assessment algorithm for medium and small companies which consist of the 8 main steps and the methodology how to use the algorithm;

3. This algorithm and its methodology have been approved in the real small-size company, and gave a positive results.

References

1. **Gartner Introduces the EIM Maturity Model.** Gartner research, 2008. – ID Number: G00160425. Online: http://www.eurim.org.uk/activities/ig/voi/Gartner_Introduces_The_EIM_MM.pdf .
2. Risk Management: Implementation principles and inventories for risk management/Risk assessment methods and tools. – European Network and information Security Agency (ENISA), 2006. – 177 p.
3. **Конеев И., Беляев А.** Информационная безопасность предприятия. – БХВ–Петербург, 2003. – 752 с.
4. **McNeil A. J., Frey R., Embrechts P.** – Princeton University Press, 2005. – 538 p.
5. **Alagna T.** The Black Book on Corporative Security. – Larstan Publishing Inc., 2005. – 440 p.
6. **Vacca J. R.** Computer and Information Security Handbook. – Morgan Kaufmann Publishers, 2009. – 887 p.
7. **Al Zu`bi A. R., Ibrahim Y. K.** Information System's Protection Algorithms, Comparative Analyses // International Journal of Computer Science and Network Security, 2007. – Vol. 7. – No. 12. – P. 294–299.
8. Vageris R. Rizikos analizės vadovas. – Vilnius: Vaga, 2005. – 160 p.
9. **Kouns J., Minoli D.** Information Technology Risk Management in Enterprise Environments. – John Wiley&Sons, Inc., 2010. – 422 p.
10. Risk management guide for small business. – Global Risk Alliance Pty Ltd jointly with NSW Department of State and Regional Development. – Australia, 2005. – 60 p.

Received 2012 01 17
Accepted after revision 2012 03 02

S. Japertas, G. Cincikas, R. Sestaviskas. Company's Information and Telecommunication Networks Security Risk Assesment Algorithm // Electronics and Electrical Engineering. – Kaunas: Technologija, 2012. – No. 5(121). – P. 33–36.

Today the existing algorithms and instrumental security risk assessment tools mainly are dedicated to government institution or large-size companies. In this work there is proposed the risk assessment algorithm for medium and small companies. The algorithm consists of 8 steps. The methodology how to use this algorithm also is given there. The algorithm and methodology have been approved in the real small-size company. Ill. 2, bibl. 10 (in English; abstracts in English and Lithuanian).

S. Japertas, G. Činčikas, R. Šestaviskas. Įmonių informacinių ir telekomunikacinių tinklų saugos rizikos įvertinimo algoritmas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2012. – Nr. 5(121). – P. 33–36.

Šiuo metu naudojami informacinių ir telekomunikacinių sistemų saugos rizikos įvertinimo algoritmai ir jų pagrindu sukurtos instrumentinės priemonės yra pritaikytos valstybinėms institucijoms arba stambioms įmonėms. Šiame darbe siūlomas algoritmas ir jo naudojimo metodas, skirti vidutinėms arba mažoms įmonėms. Algoritmas ir jo naudojimo metodas buvo aprobuoti konkrečioje įmonėje. Il. 2, bibl. 10 (anglų kalba; santraukos anglų ir lietuvių k.).