Zudin Rodion

ANALYSIS OF INFORMATION RISK MANAGEMENT METHODS

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2014

ABSTRACT

Zudin, Rodion

Analysis of information risk management methods

Jyväskylä: University of Jyväskylä, 2014, 33 p.

Information Systems, Bachelor's Thesis

Supervisor: Siponen, Mikko

A brief overview in the information risk management field is done in this study by introducing the shared terminology and methodology of the field using literature overview in the first chapter. Second chapter consists of examining and comparing two information risk management methodologies proposed by two different guides: Risk Management Guide for Information Technology Systems by National Institute of Standards and Technology and The Security Risk Management Guide by Microsoft. By finding common factors and methods shared by both guides, their shared approach for the information risk management is attempted to be defined.

Keywords: information security management, risk assessment, risk mitigation

TIIVISTELMÄ

Zudin, Rodion

Analysis of information risk management methods

Jyväskylä: Jyväskylän yliopisto, 2014, 33 s.

Tietojärjestelmätiede, kandidaatin tutkielma

Ohjaaja: Siponen, Mikko

Ensimmäisessä luvussa suoritetaan tietoriskien hallinnan alan yleiskatsaus esittelemällä alan yleistä termistöä ja metodologiaa. Toinen luku koostuu kahdessa tietoriskien hallinnan oppaassa esiteltyjen tietoriskien hallinnan menetelmien tarkastelusta ja vertailusta. Nämä oppaat ovat Risk Management Guide for Information Technology Systems, jonka tekijänä on National Institute of Standards and Technology ja Risk Management Guide, jonka tekijänä on Microsoft. Löytämällä oppaiden yhteisiä tekijöitä ja keinoja koetetaan määritellä oppaiden yhteinen lähestymistapa tietoriskien hallintaan.

Asiasanat: tietoturvan hallinta, riskien arviointi, riskien lievennys

ILLUSTRATIONS

Illustration 1: ISSRM domain model(Dubojs et al., 2010)......................................14

Illustration 2: The relationship between Risk Management and Risk Assessment (ENISA Technical Department Section Risk Management, 2007)..........................18

Illustration 3: Risk Mitigation Action Points (Dubojs et al., 2010) 25

CONTENTS

ABSTRACT..2

TIIVISTELMÄ...3

ILLUSTRATIONS..4

1 INTRODUCTION...6

2 INFORMATION SECURITY MANAGEMENT...8

3 ANALYSIS OF INFORMATION RISK MANAGEMENT METHODS..............16

3.1 Guide Structure...17

3.2 Risk assessment 18

3.3 Risk mitigation...23

3.4 Evaluation and assessment...28

3.5 Comparison of guides..28

4 SUMMARY, CONCLUSIONS & FUTURE WORK..30

1 INTRODUCTION

Modern society is increasingly reliant on information processing and global networks. This being the recent trend, economy is also becoming more and more reliant on information and information processing as most of the enterprises in the world do. In such a society, information security is a vital and growing concern.

Information is valuable resource to the people that it belongs, to the people that use it and to the people who wish to get it. Information used in enterprises can be considered as an asset which has it's value, the threats and vulnerabilities those threats can potentially abuse. Thus, the assets which have some value to the organization must be adequately protected.

Because assets must be protected from risks, it is important to know what methods for dealing with risk exist in the information risk management field today. In order to detect those practices, two information risk management guides are analyzed in this thesis.

As information risk management field is ultimately a part of information security management, the first part of this thesis introduces information security management with its history, common terminology and some recommendations.

Lastly, a common approach towards information risk management is attempted to be identified by combining the similarities between the two guides. While this approach can not be proved to be widespread or efficient only by analyzing two information risk management guides, it can be assumed to have some credibility if it is shared by multiple guides. The guides chosen for this thesis are Risk Management Guide for Information Technology Systems by National Institute of Standards and Technology and The Security Risk Management Guide by Microsoft. The reasons for choosing these guides is their free availability and the fame of the organizations behind them.

The research questions for this thesis are:

- What is information security management?
- What practices exist in the field of information risk management?
- What are the similarities and differences between Risk Management Guide for Information Technology Systems by National Institute of Standards and Technology and The Security Risk Management Guide by Microsoft?

2 INFORMATION SECURITY MANAGEMENT

During the last two decades, the impact of security concerns on the development and explotation of information systems has been constantly growing both in public and private sectors. In this sphere, security risk management has become the focal point because it helps companies to identify and implement security requirements in a cost-effective way. There are so many information security threats present that it is nigh impossible for companies to deal with all of them because every safeguard has a cost and companies have limited resources. (Dubojs, Heymans, Mayer & Matulevičius, 2010).

The information security should be considered as a multidimensional discipline. Clearly identifiable dimensions of information security are strategic, organizational, policy, best practice, ethical, certification, legal, insurance, personnel, awareness, technical, measurement and audit dimensions. (Solms, 2001).

Information security in enterprises usually consists of the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk and maximize return on investments and business opportunities.

Information security management refers to the structured process of implementing and managing information security in an organisation. It is composed by a series of sequential actions that aim at protection information and information system's assets with ultimate purpose to ensure business continuity in an organisation.

Recently, information security has moved from the era of mainframe computers up to the current state of the complex Internet. With new developments and innovations, new risks are coming along. In the twenty first century, the scope of information security has widened and its focus is quickly shifting towards a strategic governance, with most of the security challenges related to the human or organizational aspect. (Dlamini, Eloff & Eloff, 2009).

Related to the organizational and human aspect of information security is a threat posed by employees of the organization. Insider threat to information security cannot be eliminated and should be assessed and managed. Human factor is more difficult to comprehend than the technical side of the security. (Colwill, 2009).

Insider threat means the possibility of employee with access to the organizational assets being used or manipulated by a third party in order to access or damage the assets. An example of this kind of activity is social engineering, where the employee is deceived to provide access to the assets for a third party. Other example of insider threat can be sacked employee with an access to the organizational assets and a motivation to cause damage to the organization.

While users may be aware that their role in the total information security work of the organization is important, there is a gap between the intentions of the users and their actual behavior, as they do not perform many information security actions, nor are they familiar with the way they could take part in the information security work. (Albrechsten, 2007).

According to the above research findings, it can be concluded that the human factor in information security management field is extremely important and shouldn't be underestimated.

In the recent years, new threats to information systems are increasing. The exchange and sharing of information between organizations and entities outside the organization has expanded. Therefore, information systems risk not only affects the security attributes of information and causes direct economic losses in organizations, but takes into account the operations, productivity and the reputation and public image of the organization. (Yu & Ji, 2012).

The economic consequences of security breaches are considerable. Recently, most financial losses are caused by financial fraud, virus (also worms and spyware) and system penetration by an outsider (CSI, 2007).

While small businesses with limited information system infrastructure, whose operation does not require dealing with confidential data usually face minor information risks with minimal impact, large organizations such as international congromelates, hospitals and public institutions should attend information security very seriously. Legal and regulatory requirements which aim at protecting personal data empel them to devote more attention to information security risks. (Enisa, 2006).

The cost-effectiveness being important factor in dealing with information risks, companies can be assumed to adopt only the solutions which will provide significant return on investment. The cost-effectiveness can be found out by comparing the cost of the solution with a risk of it not being used and the cost of business disruption in the case a risk is materialized. In this way, risk management has an important part in the alignment of a company's business strategy with its information technology strategy. (Dubojs et al., 2010).

That is to say, while focusing too much on the security may cause the organization unnesessary expenses, focusing too little will cause expenses because of disruption of business continuity or damage caused to the assets by threats which were not dealt with.

Information security is not an easy task. Considerable and noticeable frustration has emerged related to information assurance and security in different enterprises. Many knowledgeable security specialists believe that organizations routinely fail to comprehend the seriousness of threats to enterprise information assets. (Anderson & Choobineh, 2008).

There are many different definitions for risk, but the most agreed upon one is a definition in ISO/IEC guide 73, where risk is defined as a "combination of an event and its consequence". In the same guide risk management is defined as "coordinated activities to direct and control an organization with regard to risk". (International Organization for Standardization, Geneva, 2002).

Risks can be divided into many different types, such as risks related to the management (e.g., workforce's inability to work due to pandemia), finance (e.g., financial crisis), environment (e.g., natural disasters) and security (e.g., unathorized access). While organizational risk management as a whole considers all kind of risks, information risk management concentrates only on a field of information security.

The common concept of the information systems science risk management is that there are security objectives to reach in order to ensure reasonable protection of the organisation's assets. Assets can be defined as anything that has value to the organisation, and thus needed to be protected. (Dubojs et al., 2010).

Administrators of each organizational unit must be assured that the organization has the needed ability to achieve the mission. They can provide the best conditions for encountering missions with real-world behavior determined on security abilities. Effective use of risk management process helps managers identify the controls needed to maintain IT factors and for this reason most organizations allocate huge budgets for IT security. (NIST, 1998).

In an organization employing an information system, assets related to the information system are vital point to protect in information risk management. Information system can be defined as "a system, whether automated or manual, that comprises people, machines, and/or methods organized to collect, process, transmit and disseminate data that represent user information". Thus, in any given information system contexts, assets may include hardware, software, network, people and facilities being a part of an information system and thus its security (Dubojs et al., 2010). Some examples are people with an access to the data and such things as temperature control system of a server room.

In order to be able to comprehend information risk management guides being analyzed later in this study, terminology of the field must be known. The following terms defined in the information system security risk management model (ISSRM) by Dubojs et al., 2010 are a result from analyzing terms appearing in numerous information security management methods and applicable to information risk management in general and thus are introduced below with some viewpoints from other researches.

Asset is anything of the value to the organizaiton and is necessary to achieving its objectives. In the organizations utilizing information systems, the asset definition can be split into two terms: business asset and information system asset. *Examples: enterprise models, operating system, network, programmers, accessibility controls of the office.*

Business asset is the information, process, skill inherent to the business of the organization that has value to an organization in terms of business model and is necessary for achieving its objectives. All of the business assets are immaterial. *Examples: enterprise models, data management competence*.

IS asset is a component or part of the IS that has value to the organisation and is necessary for achieving its objectives and supporting business assets. An IS asset can be a component of the IT system, but also people or facilities playing role in the IS and therefore its security. IS assets are material with the exception of software. In the larger scale analysis some of the smaller IT assets have to be combined into a bigger IS asset. For example instead of inspecting every single member of an IT security team the IT security team as a whole should be considered as an asset. *Examples: system admininstrator, user database*

Security criterion (security property) is a property or constraint on business asset that characterises their security needs. Security criteria act as indicators to assess the significance of a risk. Assets are subject to risks and risks should be evaluated with respect to the security properties that could be damaged. Traditionally, those properties include confidentiality, integrity, availability, authenticity, non-repudiation and accountability. Out of these, the most essential properties are confidentiality, integrity and availability. The non-repudiation, authenticity and accountability can be added if context requires, but they are generally deemed secondary. The security objectives of an IS are defined using security criteria on business assets. *Examples: confidentiality of risk analysis, availability of the enterprise architecture models*

Confidentiality is a property that information is not made available or disclosed to unauthorized individuals, entities or processes.

Integrity is a property of safeguarding the completeness and accuracy of assets.

Availability is the property of being accessible and usable upon demand by an authorized entity.

Risk is a combination of a threat with one or more vulnerabilities leading to a negative impact harming one or more of the assets. Threat and vulnerabilities are part of the risk event and impact is the consequence of the risk. *Examples: a third party using DDOS attack on a company's web-page, because of insufficient network filtering of the server, leading to the loss of the accessibility of the enterprise database: a thief sneaking to the company's premises because of the weak physical access control, stealing sensitive documents, leading to a loss of confidentiality of business plans.*

Impact is a potential negative consequence of a risk that may harm assets of a system or an organization, when a treat (or an event) is accomplished. The impact can be described at the level of IS assets or at the level of business assets, where it negate security criteria. *Examples: database inaccessibility (IS level), loss of confidentiality of business plans (business level).*

NOTE: An impact can provoke a chain reaction of impacts (or indirect impacts). *Examples: loss of confidentiality of business plans leads to a loss of competitive advantage; database inaccessibility leads to a loss of customer confidence.*

Event is a combination of a threat and one or more vulnerabilities. *Examples: a third party using DDOS attack on a company's web-page, because of insufficient network filtering of the server; a thief sneaking to the company's premises because of the weak physical access control.*

Vulnerability is a characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw in terms of security. *Examples: insufficient network filtering of a server, weak physical access control.*

Threat is a potential attack, carried out by an agent, that targets one or more IS assets and that may lead to harm to assets. A threat is constituted of a threat agent and an attack method. *Examples: a third party using DDOS attack on a company's web-page, a thief sneaking to the company's premises and stealing sensitive documents.*

Targets of the threats to the assets are various, such as networks, software, data and physical components. Typically, the threats are divided between natural disasters and human acts, where the threats caused by humans can be malicious or non-malicious. Some typical examples of malicious human threats are theft, fraud, disclosure of someone's personal data and identity theft. From most reports, it is obvious that the number of security and privacy incidents is growing. (Rok & Borka, 2008).

Threat agent is an agent that can potentially cause harms to assets of the IS. A threat agent triggers a threat and is thus source of a risk. A threat agent can be characterized by expertise, available resources and motivation. *Examples: a third party with little technical skills but equipped with a bot network and motivated by the profits promised by the competitor, insider with accessibility to the premises motivated by the big monetary reward from the third party*

Attack method is a standard means by which a threat agent carries out a threat. *Examples: DDOS, theft of sensitive documents.*

Risk treatment is the decision how to treat the identified risks. A treatment satisfies a security need, expressed in generic and functional terms, and can lead to security requirements. Risk treatment-related concepts describe what decisions, requirements and controls should be defined and implemented in order to mitigate possible risks. Categories of risk treatment decisions consist of the following:

Avoiding the risk (risk avoidance decision) is a decision not to become involved in, or to withdraw from a risk. *Examples: not keeping sensitive documents in the office premises, not to use web forms*

Reducing the risk (risk reduction decision) is action to lessen the probability, negative consequences, or both, associated with a risk. Security requirements are selected for risk reduction. *Examples: implementing network traffic filters to avoid DDOS attacks; keeping sensitive documents in the safe to prevent theft of information.*

Transferring the risk (risk transfer decision) is the burden of loss from a risk with another party. Risk transfer decisions may lead to security requirements about third parties. *Examples: taking an insurance to cover the loss of data; outsourcing the servers.*

Retaining the risk (risk retention decision) is accepting the burden of loss from a risk. *Examples: accepting the leakage of some sensitive information, accepting the unavailability of the service for 2 hours.*

Security requirement is a condition over the phenomena that is desirable from the risk mitigation perspective. Each security requirement contributes to covering one or more risk treatments for the target IS. *Examples: sufficient* *network filtering should be implemented in order to mitigate DDOS threat; physical access control in form of bio-identification should be used to prevent the unauthorized access.*

Control (countermeasure, safeguard) is a designed tool to improve security, specified by a security requirement, and implemented to comply with it. Security controls can be processes, policies, devices or practices that act to reduce risk. *Examples: bio-keys, backup servers.*

Interconnection and relations between all the elements of information security management are described well in the ISSRM model by Dubojs et al., 2010 (Illustration 1):

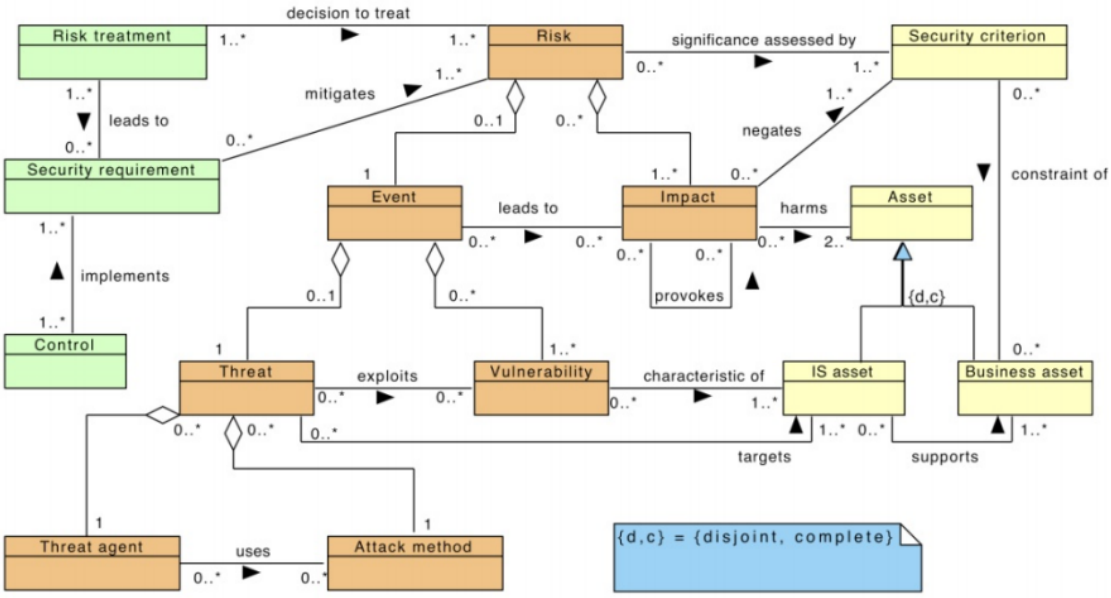

Illustration 1: ISSRM domain model(Dubojs et al., 2010)

The distribution of tasks related to information security management is important part of the management itself. According to OMB Circular A-130.Management of Federal Information Resources 1 the task allocation of information security management of enterprise and its mission among the employees should be the following.

Chief managers should be responsible for effectively applying the necessary resources and stretching the abilities necessary for realization of the mission. They should also be responsible for evaluating the results of risk management activities in decision making.

Senior Intelligence Officers' task should be planning, budgeting and implementing security sectors of IT information.

Owners of information system should be ultimately responsible for making sure that prompt controls are in place for inspection, paying attention to homogeneity, trustworthiness and accessibility of IT systems. In the process of risk management, they must know their roles and to fully support this process.

Operational and business managers should be responsible for business tasks and IT information processes. They must have an active part in the process of risk management as they have the authority in making decisions related to the mission.

IT security program mangers and computer security officers should play a role of a leader in introducing a structured and pleasant way to identify and estimate the value and risk reductions in IT systems supporting the organization's mission. Another important task of IT security program managers is improving the risk management process educational materials in order to make the staff familiar with them as well as making them able to apply the materials.

IT security convoys such as system professionals and security analysts should be responsible for providing security needs due to changes raised in the environment of these systems. They should support operation of the risk management process of the risk management process to identify and estimate the potential risks using security control tools.

3 ANALYSIS OF INFORMATION RISK MANAGEMENT METHODS

Today, security concerns are one of the main concerns of information systems, both at technological and organizational levels. There are hundreds of practitioner-oriented risk management methods in addition to several academic security modelling frameworks available, which makes it difficult for organizations to choose the most suitable approach. The lacking understanding of of the security management domain itself makes the choice even more difficult. (Dubojs, Heymans, Mayer & Matulevičius, 2010).

Risk management is a process aimed at an efficient balance between realizing opportunities for gains and minimizing vulnerabilities and losses. Risk management can also be seen as a process to identify and access risk and to apply methods to reduce it to an acceptable extent (Tohidi, 2011). Its main goal is to help organizations better manage risk associated with their missions (Tohidi, 2011). It is a recurrent activity, that deals with the analysis, planning, implementation, control and monitoring of implemented measurements and the enforced security policy (ENISA, 2006).

Risk management methods consist of guidelines that help to identify vulnerable assets, determine security objectives, assess risks and define and implement security requirements to treat the risks. By using these methods companies can reduce the losses that might result from security problems. (Dubojs et al., 2010).

In this chapter two information risk management methods are going to be under examination. The methods chosen for this study are Risk Management Guide for Information Technology Systems by National Institute of Standards and Technology and The Security Risk Management Guide by Microsoft. After introducing the practices proposed in the respective guides they are going to be compared. By examining these two guides, this study will be able to identify used practices in information security risk management in chapters 3.2-3.4 and to extract the common conventions in chapter 3.5.

3.1 Guide Structure

A. National Institute of Standards and Technology

National Institute's of Standards and Technology guide consists of the following chapters.

First chapter is a brief introduction of a guide containing information about the purpose, objective and target audience of the guide.

Second chapter provides an overview of risk management process with its importance and meaning being briefly introduced.

The last three chapters make up the information risk management process. Third chapter explains the practices of risk assessment, fourth chapter concentrates on risk mitigation while fifth and the last chapter provides brief instructions as to how to evaluate and assess the practiced risk management strategy.

B. Microsoft

Microsoft's guide is divided into the following chapters:

Chapter one provides the reader with a contents overview and a general terminology used in the guide as well as some keys for exercising a successful information risk management.

Chapter two delves deeper into general security risk management practices and consists of the theoretical background to different approaches of risk management as well as their brief comparison.

Chapter three explains Microsoft's view of the risk management and introduces the four phases of the Microsoft's risk management effort, provides a company with instructions for determining its risk management maturity level and defining roles and responsibilities.

Chapters four, five and six act as a core of a risk management guide with the risk management process split into risk assessment in chapter four, conducting decision support in chapter five and implementing controls and measuring program effectiveness in chapter six respectively. The ultimate goal of the whole process is considered to be developing a cost-effective control environment that drives and measures risk to an acceptable level.

Because the risk management methodology proposed in the risk assessment, risk mitigation and evaluation and assessment chapters of National Institute's of Standards and Technology Guide is parallel to the one introduced in the chapters risk assessment, conducting decision support and implementing controls and measuring program effectiveness by Microsoft, those chapters of their respective guides are going to be analyzed and compared.

3.2 Risk assessment

Risk assessment is a part of risk management which aims at identifying, assessing the risks and planning the actions to deal with the risks. While risk management is performed continuously, risk assessment is usually practicioned only at certain time points. The relationship of risk management and risk analysis can be observed from the illustration 2 from OCTAVE (ENISA Technical Department Section Risk Management, 2007).

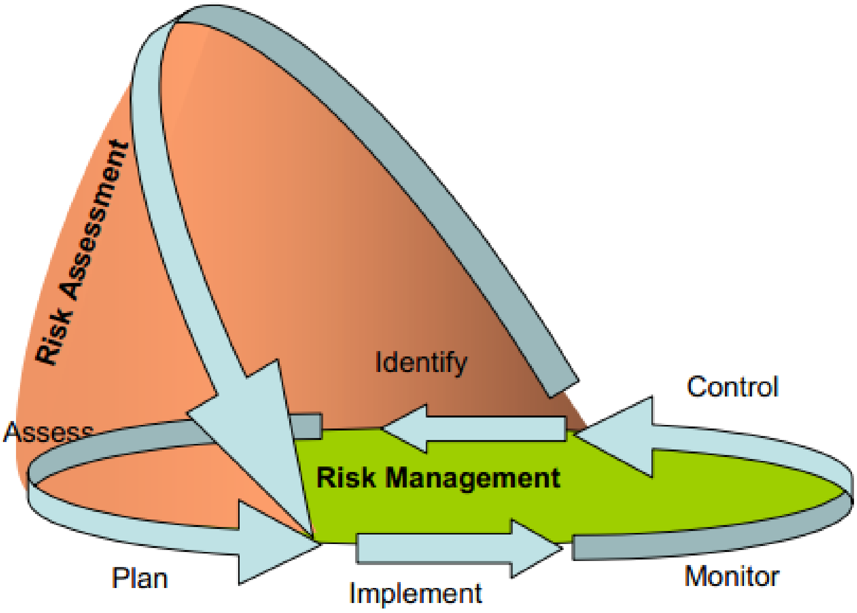

Illustration 2: The relationship between Risk Management and Risk Assessment (ENISA Technical Department Section Risk Management, 2007)

The main challenge in risk assessment is assessing all the risks in a system or organization in a way that by using the output of risk assessment appropriate controls for reducing and eliminating those risks could be introduced. The method to assess risks is generally composed of the four steps: threat identification, vulnerability identification, risk determination and control recommendation. (Syalim, Yoshiaki & Kouichi 2009).

A. National Institute of Standards and Technology

Guide for Information Technology Systems by National Institute of Standards and Technology has an extensive guide for risk assessment. According to the National Institute of Standards and Technology, the risk assessment process can compose of the following nine steps:

First step is system characterization. In order to conduct adequate risk assessment the system itself has to be defined with its boundaries, resources and information. Characterizing an IT system makes it possible to establish the scope of the risk assessment effort, outline the operational boundaries as well as provides information related to the system needed for defining the risk.

As identifying a risk for an IT system requires understanding of a system itself, information about the system must be gathered from several different categories. Usually those categories are hardware, software, system interfaces, data and information, persons who support and use the IT system, system mission, system and data criticality as well as system and data sensitivity.

Gathering of additional information related to the IT system and its data can significantly support risk assessment process. This information includes the functional requirements of the IT system, users of the system, system security policies governing the IT system, system security architecture, current network topology, information storage protection, flow of information to the IT system, technical, management and operational controls being used as well as physical security environment of the IT system and implemented security related to it.

Information gathering can be conducted throughout the whole risk assessment process. The following three information gathering techniques are proposed by Stoneburner, G., Goguen, A. & Freinga, A. (2002).

Questionnaire concerning the management and operational controls planned to be used in the IT system can be developed by risk assessment personnel. The questionnaire should be distributed to the applicable technical and nontechnical management personnel who are related to the IT system.

On-site Interviews with IT system support and management personnel makes it possible for risk assessment personnel to collect useful information about the IT system. Information about the environmental, physical and operational security of the system can also be acquired during the on-site visits.

Document review is the last proposed information gathering technique. Documents such as policy documents (e.g., directives), system documentation (e.g., system operation manual), and security-related documentation (e.g., system security policies) can provide good information about security controls used by and planned for the IT system.

Second step is threat identification also proposed by Syalim et al., 2009. The goal of this step is to identify the potential threat-sources. A threat source can be defined as any circumstance or event with the potential to cause harm to an IT system.

Guide also introduces different types of human threats and emphasizes that motivation and resources for carrying the attack make humans dangerous threat sources. An overview of the different kinds of human threats is introduced with the names of the threat-source, motivations and threat actions. An estimate of the motivation, resources and capabilities that may be required to carry out a successful attack should be created after the identification of potential threat-sources in order to determine the likelihood of the realization of the threat.

An output from the second step should be a threat statement, a list of potential threat-sources that could exploit system vulnerabilities.

Third step is vulnerability identification. According to the guide, analysis of vulnerabilities associated with the system environment must be included in the analysis. The goal of vulnerability identification step is developing a list of system vulnerabilities that could be exploited. The table pairing the vulnerabilities and threat-sources is proposed to be made.

The use of vulnerability source, the performance of system security testing and the development of a security requirements checklist are proposed for identifying system vulnerabilities. Different kinds of vulnerability identification methods are recommended dependent on the state of the IT system.

As a part of vulnerability identification, system security testing is proposed as a method of identifying system vulnerabilities. Automated vulnerability scanning tool, security test and evaluation and penetration testing are the ways proposed in the guide.

During the last step of vulnerability identification, development of security requirements checklist is highlighted. Checklist is to contain the vulnerabilities related to the management, operational and technical security areas of an IT system.

The goal of the fourth step, control analysis is analyzing the controls that have been implemented or are to be implemented to minimize the likelihood of a threat's exercising a system's vulnerability. Control methods, control categories and control analysis technique are also described in this step of the guide.

Fifth step is likelihood determination of a potential vulnerability to be abused. The scale from low to high is provided to assess the likelihood level.

Impact analysis is a sixth step of risk analysis. The information about system mission, system and data criticality and sensitivity is to be obtained before proceeding with the analysis. A loss or degradation of any security goals described in the first part of the thesis has to be estimated on the scale from low to high. Also it should be noticed, that the guide presents only a qualitative method to estimate the impact.

The purpose of seventh step – risk determination is assessing the level of risk to the IT system. Risk level matrix is introduced, which takes into account the threat likelihood and impact with the ultimate purpose of calculating threat impact. The table is provided for assessing the risk scale and estimating the appropriate actions for the senior management to take.

Control recommendations are eight step, which is dedicated to provide the controls that could mitigate or eliminate the identified risks. The control recommendations should be the ultimate result of the risk assessment process and provide input to the risk mitigation process.

Step nine, being the last step of the risk analysis is devoted purely to the documentation of the results of risk assessment process. The output of the final step should be risk assessment report that describes the threats and vulnerabilities, measures the risk and provides recommendations for control implementation.

B. Microsoft

In Microsoft's guide the risk assessment process is split into three steps: planning, facilitated data gathering and risk prioritization. Following text is the chronological description of the process. In the guide, risk assessment is defined as the process to identify and prioritize enterprise IT security risks to the organization.

Planning is described as the most important step of the whole risk management process to ensure stakeholder acceptance and support. The main tasks in the planning step are seen to be aligning the assessing risk phase to business processes, scoping the assessment and gaining the stakeholders acceptance.

Alignment process is recommended to be done prior the organization's budgeting process. This timing is stressed in order to build support and helping the organization understand the importance of security.

To effectively manage risk across the organization, all organization functions included in the risk assessment should be documented in the risk scope. Risk assessment should be scoped as well by defining the areas of the organization to be evaluated and gaining executive approval before advancing.

Gaining Stakeholders Acceptance process is considered vital for risk assessment. Working with stakeholders informally and early during the process making sure they understand the importance of the risk assessment is viewed as a best practice. Pre-selling is proposed as the best way to gain the acceptance. It involves informal meeting with stakeholders before requesting for a formal commitment.

Second step of risk assessment process is called facilitated data gathering and is further divided into three steps. First one describes data gathering process in detail and focuses on success factors when gathering risk information. Second one describes the detailed steps of gathering risk data. Third one describes the steps to consolidate the collected data into collection of impact statements.

Data gathering process is not only being described in detail, but hints for conducting successful data gathering are also provided. Such things as the importance of building support between the information security group and business owners, building goodwill and proper discussion strategies are included in this section.

After providing the guidance described above, the guide continues to delve deeper into communication strategies in the form of instructions for risk discussion preparation. It should be noted that this section of the guide concentrates on preparation for the discussion and reclassifying and redefining the collected information in order to make the discussion with non-technical personnel and stakeholders more feasible. Checklist is provided for collecting input material for risk assessment process.

Facilitated data gathering section continues with guidelines for identifying and classifying assets. Grouping the assets into business scenarios such as purchase orders and database population is recommended to make categorizing the assets easier.

While according to the guide the assets can be either tangible or intangible, both categories require the stakeholder to provide estimates in the form of direct monetary loss or indirect financial impact. A third asset category between tangible and intangible assets is also introduced. Such things as file sharing or networking are examples of assets from the third category. Those kind of assets have both physical servers and digital data, thus being considered as both tangible and intangible asset.

In the next paragraph, asset classification scope is introduced with three categories: assets with high, medium and low business impact called (HBI), (MBI) and (LBI) respectively. The classification helps the organizations to concentrate on the most essential assets first when managing the risk.

Next organizing risk information is recommended. One proposed way is organizing the information by defense-in-depth layers with physical, network, host, application and data categories.

Next part concentrates on transforming the threat and vulnerability related vocabulary into familiar terms for non-technical stakeholders. Some tips are also provided for performing risk assessment in general.

Gathering the stakeholder estimate on the extent of the potential damage to the asset is the main point of the next part, which is called Estimating Asset Exposure. A three-step grouping from low to high exposure is proposed to be used. Similarly in the next chapter, which concentrates on estimating the probability of threats, similar three-step grouping is recommended with low, medium and high probabilities.

The following part of risk assessment is about facilitating risk discussions. Five tasks for the data gathering discussion are proposed: determining organizational assets and scenarios, identifying assets, identifying vulnerabilities, identifying existing controls and the probability of an exploit. Covering examples as well as brief instructions for every discussion phase are described in the guide.

The last task of the facilitated data gathering step is defining impact statements. The output of this phase is a list of statements describing the asset and the potential exposure from a threat or a vulnerability. A list is going to play a major role in the risk prioritization phase of risk assessment.

The risk prioritization is described to be consisting of the three different tasks. Task one is determining impact value from impact statements, task two is estimating the probability of the impact and task three is combining the impact and probability values for each risk statement. This chapter mainly consists out of introduction of different tools as well as descriptions for estimating required variables. After results of risk prioritization process have been summarized, they are recommended to be reviewed with the stakeholders.

Microsoft security risk management process mainly applies a qualitative approach to identify risks. A guide, however, propose a quantitative approach to be used to deal with the high priority risks. This is followed by a multitude of different tables and formulas for employing the quantitative evaluation of risks.

3.3 Risk mitigation

A. National Institute of Standards and Technology

According to the guide by National Institute of Standards and Technology least-cost approach should be taken along with implementing most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and missions.

First part of risk mitigation part of the guide introduces risk mitigation options, which are risk assumption, risk avoidance, risk limitation, risk planning, research and acknowledgement and risk transference.

Risk assumption means accepting the potential risk and continuing operations or implementing controls to lower the risk to an acceptable level.

Risk avoidance means avoiding the risk by eliminating the risk cause and/or consequence.

Risk limitation is limiting risk by implementing controls that minimize the impact of the risk.

Risk planning is managing risk by developing a risk mitigation plan that prioritizes, implements and maintains controls.

Research and acknowledgement is lowering the risk of loss by acknowledging the vulnerability and working on it.

Risk transference is transferring risk by using other options to compensate for the potential loss.

Self-explanatory risk mitigation chart (Illustration 3) of the guide is pivotal for providing decision makers with a way to decide when to take action to mitigate the risk.

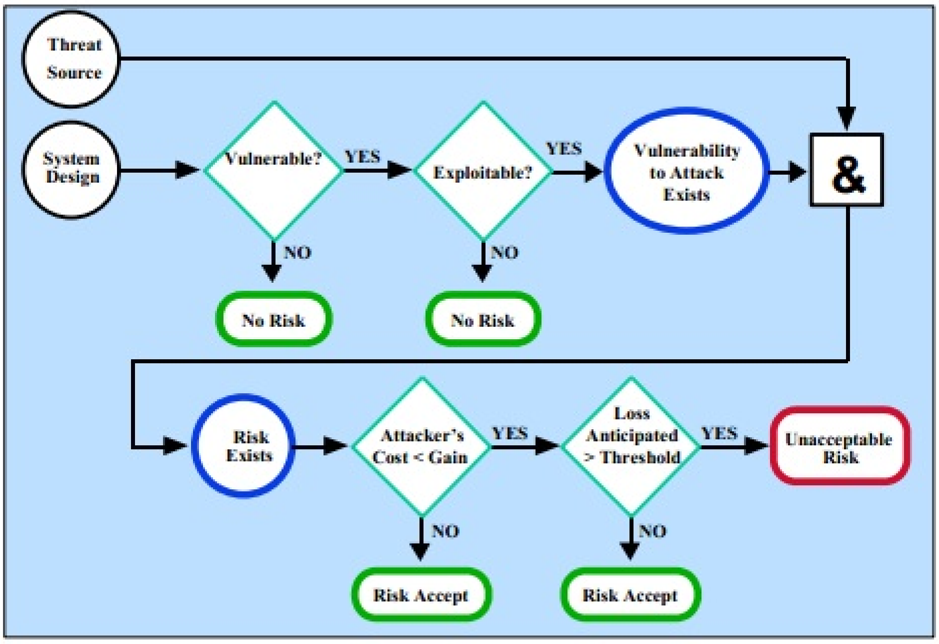

Illustration 3: Risk Mitigation Action Points (Dubojs et al., 2010)

The control implementation process itself is divided into several parts in the risk mitigation section of the guide. Starting from prioritizing control implementation actions based on the risk assessment report in step one and continuing with evaluating recommended control options in step two the methodology continues with conducting cost-benefit analysis in step 3.

In step 4 appropriate controls should be selected, with responsibility being assigned in step 5. Step 6 is dedicated to developing a safeguard implementation plan with the methodology culminating in seventh step with the implementation of selected controls.

The controls can be divided into three categories with several different subcategories.

Technical security controls are technical in nature and can be applied both to the hardware and software. These controls may range from simple to complex measures and usually involve system architectures, engineering disciplines and security packages with a mix of hardware, software and firmware.

Management security controls focus on the stipulation of information security policy, guidelines, and standards, which are carried out through operational procedures to fulfill the organization's goals and missions

Operational security controls, implemented with accordance with a base set of requirements and good industry practices, are used to correct operational deficiencies that could be exercised by potential threat sources.

After implementing controls, a cost-benefit analysis is proposed to be done in order to determine which controls are required and appropriate for their circumstances. It consists of determining the impact of implementing the new or enhanced controls, determining the impact of not implementing the said controls, estimating the costs of the implementation and assessing the implementation costs and benefits against system and data criticality.

As the final step of risk mitigation by National Institute of Standards and Technology, dealing with residual risk which is the risk remaining after the implementation of new or enhanced controls. It is extremely important to note that if the residual risk has not been reduced to an acceptable level, the risk management cycle must be repeated to identify a ways to reduce the risk to an acceptable level.

B. Microsoft

The first part of Microsoft's risk mitigation process is called Conducting Decision Support phase and it is a part of risk assessment. In this study, however, it will be inspected as a part of risk mitigation and program evaluation for the sake of parallelism with the Risk Management Guide for Information Technology Systems.

The six steps of Conducting Decision Support phase are defining functional requirements, selecting control solutions, reviewing solutions against the requirements, estimating the degree of risk reduction that each control provides, estimating cost of each solution and selecting the risk mitigation strategy.

Defining functional requirements must be defined for each risk discussed and the deliverable "Functional Requirement Definitions" is to be produced from the Defining Functional Requirements step of risk mitigation.

In the second step Identifying Control Solutions list of potential new controls for each risk should be came up with. The controls are divided into several categories.

Organizational controls are procedures and processes that define how people in the organization should perform their duties. *Examples include: responsibilities, documented security plans and training*

Operational controls define how people in the organization should handle data, software and hardware. Preventative controls in this category are such things as temperature and humidity control systems and backup systems. Detention and recovery controls can be of either physical security or environmental security nature.

Technological controls are controls involving software, hardware and/or firmware. Preventative controls in this control group can be related to authorization or access control. Detention and recovery controls in this category can be audit systems and anti-virus programs. Management controls can include for example cryptography or identification.

In step three of Conducting Decision Support, Security Risk Management Team must approve the control solution in order to make sure that the control is aligned with the defined functional requirements.

In the fourth step estimating the degree of risk reduction resulting from the control implementation should be considered. All the ways in which the control may impact the risk are recommended to be considered in order to create an accurate picture of risk reduction. This step is supported by a list of questions meant to be used when evaluating the amount of risk reduction for any given control.

The goal of the fifth step is estimating solution cost for a control implementation. The IT engineering team should determine how much acquiring, implementing and maintaining each one would cost. The training cost for IT staff and users as well as costs caused to productivity and convenience are all important parts of estimating a cost for the solution.

After five steps of Conducting Decision Support have been finished, the appropriate risk mitigation solution should be selected in the final step of the process. This is done by comparing the level of risk after the mitigation solution to the cost of the mitigation solution itself. The controls selected in this Selecting the Risk Mitigation Solution step are to be implemented in the next step which is called Implementing Controls.

During the Implementing Controls phase, plans to implement the control solutions specified during the Conducting Decision Support phase as well as reports of their deployment should be created.

Time is an important part of implementation plans as every plan should contain a explicit time frame of implementation in addition to the team assigned for the execution of implementation. Reports should be created by the implementing teams to be submitted to the Security Risk Management Team and other related entities.

The rest of the Implementing Controls section is organized around the Microsoft defense-in-depth model, which is a multilayer model consisting of physical, network, host, application,- and data layers. The guide contains links to recommendations describing controls for protecting every layer of the model as well as guidance related to planning and deploying the solutions.

3.4 Evaluation and assessment

A. National Institute of Standards and Technology

Last part of the Risk Management Guide for Information Technology Systems is dedicated to evaluation and assessment. This part stresses the importance of ongoing risk evaluation and assessment in order to fulfill a successful risk management program. It provides some guidelines for a good security practice as well as giving some hints for success.

B. Microsoft

The Measuring Program Effectiveness Phase, being the final part of Microsoft's guide provides information about required inputs and participants for evaluation and assessment of implemented information risk management solutions. The Organization's Security Risk Scorecard is highlighted as an important tool to be created to act as communication and demonstration device of risk management in organization.

Assessing implemented solutions by verifying the correct working of the controls is considered important. Automated tools by Microsoft and other vendors are recommended to make this process easier. Penetration testing and collection of feedback is proposed as alternative methods for measuring program effectiveness.

As a final note, reassessing new and changed assets as well as security risks is highlighted as an important part of security risk management.

3.5 Comparison of guides

First thing worth noticing is the scale difference of studied guides. Risk Management Guide for Information Technology Systems by National Institute of Standards and Technology is 41 pages long while Microsoft's Security Risk Management Guide is three times the length with its page count of 121.

Both guides have similar approaches to risk assessment. It is worthwhile noticing that both guides proposed starting the analysis process from characterizing the targets for risk management, defining assets, threats and vulnerabilities and continuing with control and impact analysis ultimate goal being discovering the desirable security controls to be implemented.

The noticeable difference is the Microsoft's guide's extensive focus on the ways to execute the proposed actions in the guide. While National Institute's of Standards and Technology guide concentrated on what to do in the risk management process, Security Risk Management Guide by Microsoft described in detail such things as who and in what way should be involved in the risk analysis process.

Microsoft's guide had a clear description and guidance as to how to facilitate the discussions, what terminology should be used, what are the timings and methods for communication during the risk management process.

While the guide by National Institute's of Standards and Technology also had a short part and information about the roles of people taking part in risk management, Microsoft's scale in this aspect was noticeably bigger.

Cost-benefit analysis and taking expenses into account in general was also covered more extensively in the guide by Microsoft. While Risk Management Guide for Information Technology Systems had only a few pages dedicated to simple cost-benefit analysis, Microsoft's guide stressed the importance of expenses in the justifying the acceptance of information risk management in general and had a wide variety of cost-estimation methods.

There are other minor differences in proposed methods and tools, but the baseline of the guides is the same. Information risk management consists of the risk assessment, risk mitigation and evaluating the results. Defining the system, assets, threats and vulnerabilities and examining their relations to each other can be seen as bread and butter of information risk assessment. Risk mitigation could be conducted as developing potential ways for mitigating the risks, evaluating their costs and amount of risk reduction and selecting the best practices to apply for the most critical information risks.

4 SUMMARY, CONCLUSIONS & FUTURE WORK

Information security management is a multidimensional discipline, which is composed by a series of sequential actions that aim at protecting information and organization's information assets from threats. The main goal of information security management can be seen to be ensuring business continuity in organization. Other goals are minimizing business risk and maximising return of investments of business. Information risk management is a field of information security management which concentrates on assessing and mitigating information risks.

There are numerous practices in the information risk management field today proposed by hundreds of guides and methodologies. The practices advocated by Risk Management Guide for Information Technology Systems by National Institute of Standards and Technology and The Security Risk Management Guide by Microsoft have recommendations regarding to communication, assessing, mitigating and evaluating information risk as well as organizing the data collection process for these processes. These practices are described in the third chapter of this thesis.

Risk Management Guide for Information Technology Systems by National Institute of Standards and Technology and The Security Risk Management Guide by Microsoft have similar approach to information risk management. Risk management is advocated to consist of the risk assessment, risk mitigation and evaluating the results of risk mitigation. Risk assessment is recommended to begin from characterizing the targets for risk management, defining the assets, threats and vulnerabilities ending with control analysis, impact analysis and control proposition. Risk mitigation is proposed to contain cost and performance evaluation for risk mitigation options, and selecting the most optimal practices to be implemented.

Future research prospects could be related to an interview based empirical study in attempt to find out what information risk management practices are used by different organizations and whether the organizations base their information risk management on singular guides or develop their own information risk management methods.

BIBLIOGRAPHY

Albrechsten, E. (2007). A qualitative study of users' view on information security. Computers & security 26 (2007) 276–289

Anderson, E. E. and Coobineh, J. (2008). Enterprise information security strategies. Computers & security 27 (2008) 22–29

Broderik J.S. (2001) Information Security Risk Management – When Should It be Managed? Information Security Technical Report, Vol 6, No. 3 (2001) 12-18

Colwill C. (2009). Human factors in information security: The insider threat Who can you trust these days? Information security technical report 14 (2009)

CSI (2007). CSI Survey 2007. The twelfth annual computer crime and security survey.

Dlamini M.T., Eloff J.H.P and Eloff M.M. (2009). Information security: The moving target. Computers & security 28 (2009) 189–198

Dubojs, É., Heymans, P., Mayer, N. & Matulevičius, R. (2010). A Systematic Approach to Define the Domain of Information System Security Risk Management. *Intentional Perspectives on Information Systems Engineering, 2010,* 289-306.

ENISA Technical Department Section Risk Management. Risk management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, Geneva, 2006

ENISA Technical Department Section Risk Management. Information Package for SMEs, Geneva, 2007

ISO/IEC Guide 73 Risk management - Vocabulary - Guidelines for use in standards. International Organization for Standardization, Geneva, 2002

ISO/IEC 13335-1 Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management. International Organization for Standardization, Geneva, 2004

MICROSOFT. (2006) The Security Risk Management Guide.

NIST special Publication 800-18 co-authored with Federal Computer Security Managers' Forum Working Group. (1998). Guide For Developing Security Plans for Information Technology Systems.

OMB Circular A-130.Management of Federal Information Resources. Appendix III. November 2000.

Rok, B. and Borka, J-B. (2008). An economic modelling approach to information security risk management. International Journal of Information Management 28 (2008) 413–422

Solms, B. (2001). Information Security – A Multidimensional Discipline. Computers & Security, 20 (2001) 504-508

Stoneburner, G., Goguen, A. & Freinga, A. (2002). Risk Management Guide for Information Technology Systems. *Recommendations of the National Institute of Standards and Technology*

Syalim, A., Yoshiaki, H. & Kouichi, S. (2009). Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide

Tohidi, Hamid. (2011). The Role of Risk Management in IT systems of organizations. *Procedia Computer Science 3 (2011), 881-887.*

Yu, Z. and Ji, Z. (2012). A Survey on the Evolution of Risk Evaluation for Information Systems Security. Energy Procedia 17 (2012) 1288 – 1294