KARELIA UNIVERSITY OF APPLIED SCIENCES
Degree Programme in Technology Competence Management
Master Degree

Petri Hukka

IT RISK MANAGEMENT DEVELOPMENT IN ORGANISATIONS

Thesis
March 2019

OPINNÄYTETYÖ
Maaliskuu 2019
Teknologiaosaamisen johtamisen koulutusohjelma
Ylempi ammattikorkeakoulututkinto
Tikkarinne 9
80200 JOENSUU
+358 13 260 600 (vaihde)

Tekijä(t)
Petri Hukka

Nimeke
Riskienhallinnan kehittäminen yrityksessä

Toimeksiantaja
Euroopan metsäinstituutti

Tiivistelmä

Opinnäytetyössä oli tehtävänä kehittää yrityksen IT-riskienhallintaa, tietoturvaa sekä riskienhallintaan liittyviä prosesseja ja toimintatapoja. Teoriaosassa käydään läpi riskienhallintaa, tietoturvaa sekä IT-johtamiseen liittyviä toimintatapoja.

Opinnäytetyö oli kehittämistehtävä, jossa käydään läpi yrityksen IT-toimintoihin liittyviä riskejä, käytännön osuudessa yritykseen tehtiin riski- ja tietoturvakartoitus, jonka pohjalta voidaan arvioida tietojärjestelmiin liittyviä riskejä. Tulosten pohjalta saadaan tietojärjestelmiin liittyvät uhat ja niiden pohjalta luoda riskienhallintaan liittyvät käytännöt ja arviointimenetelmät, joilla riskejä seurataan.

Tulosten pohjalta on tarkoitus kehittää IT-riskeihin liittyvät toimintatavat, luoda yritykselle politiikat, käytännöt sekä riskilistat liittyen tietoriskeihin. Riskienarvioinnin pohjalta tulisi luoda säännölliset seurantamekanismit tietoriskeihin ja tietoturvaan auditoimalla säännöllisesti riskilistoihin perustuen yrityksen IT-toiminnot. Kehittämistyö jatkuu opinnäytetyön valmistumisen jälkeen, jonka pohjalta riskienhallintaa on tarkoitus kehittää eteenpäin.

Jatkokehittämisenä yritykselle tulisi luoda tietoturvasuunnitelma, tietoturvapolitiikka sekä tietojärjestelmien jatkuvuus- ja toipumissuunnitelma.

Kieli	Sivuja 52
Englanti	Liitteet 3

Asiasanat

IT riskit, riskienhallinta, riskien auditointi, tietoturva

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
March 2019
Degree Programme in Technology
Competence Management
Master's Thesis
Tikkarinne 9
FI 80200 JOENSUU FINLAND
Tel. +358 13 260 600 (switchboard)

Author (s)
Petri Hukka

Title
IT risk management development in organisations

Commissioned by
European Forest Institute

Abstract

The aim of this thesis is to consider organisational IT risks, information security, risk processes and the practises related to the risk assessment. The theoretical part handles IT risk assessment, information security and IT leading.

The thesis is a developmental process where company risk concerns related to the IT functions are investigated. In practise the risk and network security checks were made. Based on the results, risks and threats can be defined, and needed guidelines and evaluation methods can be created.

Based on the results it is meaningful to develop the IT guidelines and create policies, best practises and lists which are related to IT risks. There should be regular follow up methods for IT risks in the future and IT functions should be regularly audited based on the risk lists. The development work continues after this thesis, and the risk evaluations are meant to develop further.

For the future the company should develop a security plan, a security policy and a continuity and recovery plan.

Language	Pages 52
English	Appendices 3

Keywords

IT risks, risk assessment, risk management, risk audit, network security

CONTENTS

Appendix

Annex 1 Risk lists
Annex 2 Network security instructions
Annex 3 User security instructions

Abbreviations

RAID	Redundant Array of Independent disk, data storage technology which combines multiple physical disks into one or more logical units.
VPN	Virtual Private Network, extends a user private network over the Internet via secure tunnel to the company private network.
IPS	Intrusion Prevention system, system that keeps on eye on a network any malicious activities or incidents like a security threats.
SSL	Secure Socket Layer, gryptographic network protocol for operating network services securely over an unsecured network.
SMB	Server Message Blocking, used in computer networking for sharing files, printers and serial ports.
CTO	Chief Technology Officer, executive level position in an organisation and is focused on technology level issues within an organisation.
CIO	Chief Information Officer, job position for senior executive IT person, typically reports to the chief executive officer.
CEO	Chief Executive Officer, company leader and in charge of managing an organization, reports to the board of directors.

1 Introduction

> The only truly secure system is one that is powered off, cast in a block of concrete and scaled in a lead-lined room with armed guards – and even then, I have my doubts - Eugene H. Spafford (Harrison 2016, 1).

The former summarized well the security concerns nowadays. To be sure from the security concerns it is better unplug wires from the network. This is the safest way to implement security. Even then we cannot be sure about the security concerns because the external threats can cause security vulnerabilities, such as device theft, human error and so on.

IT risks and network security concerns are a big part of company data networks nowadays. The security concerns should go through the company management; that is the way IT gets guidelines on how the IT risks should be handled and how to setup risk levels.

IT risk list should cover the following items:

- Risk assessment leading and organizing
- Risks related to customers and stakeholders
- Staff security and risk knowledge
- Asset risks
- Information system and software risks
- Software development security
- External risks
- Cost risks
- Timetable risks
- Technical risks
- Operational risks
- Communication and Network Security
- Identity and Access Management

- Risk lists
- Auditing

COBIT5 categorizes the risks as follows:

- IT benefit or value enablement risk
- IT programme and project delivery risk
- IT operations and service delivery risk

(ISACA 2013, 17)

Nowadays, companies have many other things to do than concentrate in security concerns. Do the business to keep wheels running, make strategic plans and with all these things take care of the security concerns so they are done the right way. This is the responsibility of the IT department and the IT manager. The questions regarding how to go through with the company management in a way that they understand the security concerns and if the IT department has enough resources to take care of security policies, encryption methods, checking vulnerabilities etc. remain (Harrison 2017, 1).

In addition there are many regulations for IT, as well as standards and best practises how to take care of the security matters like ISO/IEC27001, TOGAF, COBIT 5, NIST, COSO and ITIL. These are explained more specifically in Section 2.5. From these an organisation should pick up the best practises for itself, follow them and put it in the practice. The organisation should not forget the auditing security issues inside the company. Auditing should be done internally and externally. (Harrison 2016, 15.)

Every organisation should build its own best practices, processes for security issues and how to handle e.g. in case of network attack or hacks (Harrison 2016, 2).

An organisation should build a strong security platform. This is like building a house, it has the strong base where all the building structures are based on. Protect the company business which can be based on the skills of the IT department or individual IT expert how they handle IT policies and protection. (Harrison 2016, 1-2.)

Many factors are affected on the risk handling and how it succeeds:

- The expectations of the risk by management and if they understand the risks which are related to the company functions, especially IT risks.
- The company culture and staff responsibility
- The risk handling should be aware of all company staff members

IT risk management goals:

- Recognize risks, the big and small risks which can threaten the company functions
- Focusing on minimizing the risks with available measures
- To create the formal and repeated method to follow the risks,
    - Audit and recognize the risks
    - Define the effective way to reduce the risks
    - To follow the risks, how they are handled, and how they could be done in a better way and reported on.

1.1 Objectives

The main objectives for this thesis are to develop the IT risk management guidelines, instructions and in practice to implement the security and penetration tests in the organizational IT infrastructure. The security and penetration tests gives the the organizational IT and management the information of the current state of the network threats and vulnerabilities. On the basis of the tests the organization will get the development needs for the organization IT infrastructure and security concerns.

The target is to create regular follow-up methods in the risk assessment and risk auditing and to get the IT risk evaluation to support the organizational management processes. Based on the risk lists an organization can evaluate the IT risks related to the organization business. Regular IT security training is meant to start after the risk assessment.

IT management is handled on a theoretical level based on the earlier publications. IT management functions are handled from the view of risk management and how

it is related to other organizational management processes. The meaning is also to get the organizational management persons to understand the IT risks, IT management guidelines and how those are related to the overall organizational leading and how IT leadership and co-ordination should be lead.

2 The basics of risk management

2.1 Security and risk

In the organisation the security consists of many components such as devices, personnel, human behaviour, security policies, laws and standards.

The security or risk can be described as security assessment or risk assessment. The third concept which is met often in the security area is penetration testing. Penetration testing means that in the test is trying to exploit the system in a legal way to make the system more secure. (Engebretson 2011, 1.)

Security is about controlling the risks. It protects files, the use of them and the systems which they use. Cyber security means, on a basic level, to secure the national functionalities, including national defence. Data protection protects the personal data from irrelevant and incorrect usage. (Järvinen 2016, 3.)

In high availability (HA) networks the company IT systems must be in use 24 hours, every day, 365 days in a year, and these kinds of companies cannot work without IT systems. These companies are e.g. banks, insurance companies and electricity utilities. System updates cannot cause any service breaks for usability, and if those are done, normally they occur during the night, when the users are not logged on to the system. (Jordan & Silcock 2006, 11.)

It is important for the organisational functions that

- Information is correct and up to date
- The system is available only to authorized users
- The information does not get lost or under unauthorized use.

The security policies and risk management are always carried out with the company management, and the company leaders should to commit to these policies. Security policies can be based on the commonly known standards such as ISO 27001.

Security policy is a general and overall policy which says the security role in the organisation. It is approved of by the company management. Security policy is defined as the overall framework on how the security is established in the organisation. The management gives the goals and responsibilities within the organisation. (Harrison 2016, 87.)

2.2 Basic security principles

The security main principles can be seen to consist of these three different areas: availability, integrity and confidentiality.

The availability of the IT systems should be 24 hours every day, every week, 365 days in a year. How it is guaranteed the overall availability of the systems. IT personnel must have a strong experience and technical skills to take care and maintain the complicated IT systems..

The matter that all these things are taken care of internally in the organisations is not enough. External threats fire, water damage, theft, vandalism, and power failure can cause bigger threat and loss of availability even all the things are taken care internally. (Harrison 2016, 4.)

In the organisations IT systems should be built in a way that the business can continue even unexpected failure case happens. For banks and electricity utilities the long downtimes can be a catastrophic. In contemporary society certain organisation’s systems are highly automated and controlled by computers, so in these kind of cases the backup and disaster plans should be up to date and tested.

As a summary from the technical perspective the availability can be handled with the following technical systems:

- RAID (redundant array of independent disks) disk system

- Clustered systems
- Doubled systems, load balancing
- Doubled power lines
- Data backups
- Duplicated device rooms
- Offline usage
- System restoration

(Harrison 2016, 5-6).

The integrity of the system is reached when unauthorized access to the systems is prevented. The external access inside the company network is prevent by fire-walls and other systems by which integrity can be verified. In the case of hacking, the intruder can install a virus or backdoor in the system. Then, the integrity is cracked. (Harrison 2016, 4.)

In certain systems inside the company network there are authorized users who can give the user rights to the company staff. The user who has full rights in the machine can infect the whole machine disk, when in the case of restricted user permissions only the user own profile is infected. This way the cleaning of the machine is easier for the IT personnel. The user can also cause the loss of integ-rity by his/her own operations or by human errors such as accidentally deleting important files or infecting machines with external guest USB sticks.

As a summary, integrity involves

- User privileges with basic user rights
- The system critical files only available for the authorized users
- Databases are protected and accessed only by the main users
- Data lines are encrypted

(Harrison 2016, 4).

Confidentiality means reaching the necessarily confidential level in data handling and preventing unauthorized data usage. An intruder or hacker can use different

methods when trying to access data such as passwords, installing data snooping programs on a user machine, or just trying to get information directly from a user. The company strategic information should always be encrypted when sending to external partners.

All three areas, availability, integrity and confidentiality, should be understood by all levels in the organisation and for all users. Especially the company management should understand what these can mean for the company business, and that a lack of these matters can have negative impacts on the company image. (Harrison 2016, 5).

As a summary and from the technical side, confidentiality could be handled with the following terms:

- Data encrypting
- Encrypted remote connections
    - VPN (Virtual Private Network)
- Controlling access
    - Physical, access control (doors)
    - Technical, user authentication

(Harrison 2016, 6).

2.3 Controls

There are three different types of controls: administrative, technical and physical. The administrative controls include:

- Security documentation
- Risk control
- Personnel security
- Personnel security training

Technical controls include:

- Firewalls
- Authentication methods
- Antivirus programs
- Encrypting methods

Physical controls include:

- Device room locking
- User controls
- Restricted areas, fences
- Camera control
- Fire extinguishing system

(Harrison 2016, 8-11).

In the worst cases devices and programs inside the company are installed without thinking about the functions of them or the security. When something happens users think that those can be repaired immediately. In many organisations the situations can be just like this and all the time in the systems are added more less-secure items, which threatens the company IT systems.

Overall, when we are looking at the organisational security and risk matters, the following items should be defined:

- Defining the systems which will be protected
    - Defining the organisation most important systems
    - Categorizing the system levels
- Risk assessment
    - The risks which are related to the systems
- Information security policy
    - When the risk analysis is done, the security policy is created based on the results
    - Includes security policies and goals
    - Does not include technical descriptions

    - Done with the organisation management
    - Includes the responsibilities and common guidelines
- Information security plan
    - Documentation which includes the organisation security solutions
    - Technical descriptions and guidelines
- Continuity and disaster recovery plan
    - A plan which defines what to do in the case of a disaster, such as fire
    - Availability, integrity and confidentiality is under threat
    - Recovery plan for each system

(Laakso 2010, 11-14).

2.4 Organising risks

Evaluating risks must be done regularly and continuously. The risk management functions can be used when applying project funding, daily leading and IT projects. The security must be notified widely in the organisation functions including the organisation management, IT management and end users.

“The security risk tasks and responsibilities include:

The management

- The overall responsibility of the implementation of organisational security
- Information security as a part of company risk management
- Guarantees the IT resources to implement the security
- Approves of the main principles of security policy
- Requires reporting

IT management

- Prepares the security policies and instructions
- Guides the security principles in the organisation

- Takes care of the risk management functions
- Evaluates the vulnerabilities of the most important IT systems
- Starts the development of the required fixes when notified of a developmental need

Supervisors

- Implement the security principles with the agreed goals
- Report on the security concerns

End users

- Report on security concerns
- If needed take part as an expert in the risk assessment of their own fields."

(Vahti 7/2003, 18-19).

2.5 Security standards

Several kinds of IT standards have been developed for security guidelines, which company security instructions, best practises and standards can be based on. (Harrison 2016, 15)

Examples of security standards, best practises and security frameworks:

- ISO/IEC 27000 standards include
    - International security standards on how to develop and maintain company security.
    - Several different kinds of standards, e.g. overview and vocabulary (ISO/IEC27000), risk management (ISO/IEC 27005), network security (ISO/IEC27033), Applications (ISO/IEC 27034)

- COBIT 5

    - The IT framework for the organisation business (Organisation security framework)
    - Gives optimization for the company IT functions. How to get best benefits from IT resources and IT risks .

- TOGAF
    - Model to develop the organisation architectures
    - Business or technical architecture modelling

- NIST 800-53
    - Series of controls to protect USA national systems
    - The controls are connected to the management functions, operational and technical controls, system integrity and confidentiality.

- COSO
    - Series of controls to protect organisation internal financial threats.
    - Consist of five different parts. Controls are connected to the monitoring environment, risks, technical controls, communication methods and monitoring activities.

- ITIL
    - IT processes
    - Describes the organisation processes, like how the user support is handled in the organisation.

- VAHTI
    - The ministry of finance in Finland
    - Describes the main security principles of the Finnish state and ministries.

(Harrison 2016, 15.)

In this investigation we are not going any deeper into these standards. There are many different standards all over the world, and these are some of the most commonly used.

The organisation security matters should be looked at as a whole, and its requirements should be understood throughout the company in order to be able to think about the organisation's best practises and how they can help the company security concerns.

2.6 Laws and legality

There are several laws related to the cybercrimes in national, international, European level and USA. Each country can have its own laws regarding how to handle cybercrimes. The EU has established General Data Protection Regulation (GPDR), which became valid on the 25th of May in 2018. It handles data privacy on the European level and how EU citizen data should be handled. It covers all organisations on the EU level. The GPDR can cause economic sanctions for the organisation if the data protection is not in order in the organisation. (European Union 2017)

As stated, different types of legal systems exist within different countries,

- Civil laws
- Common laws
- Criminal laws
- Customary laws
- Religious laws
- Mixed law systems

(Harrison, 2016, 58-61).

3 Risk categories

"Risks could be shared for the following eight categories:

- Administrative risks
- Physical risks
- Personnel risks
- Information system risks
- Device risks
- Software risks
- Data risks
- Usability risks”

(Vahti 7/2003, 30-39)

A risk categories is described in figure 1.

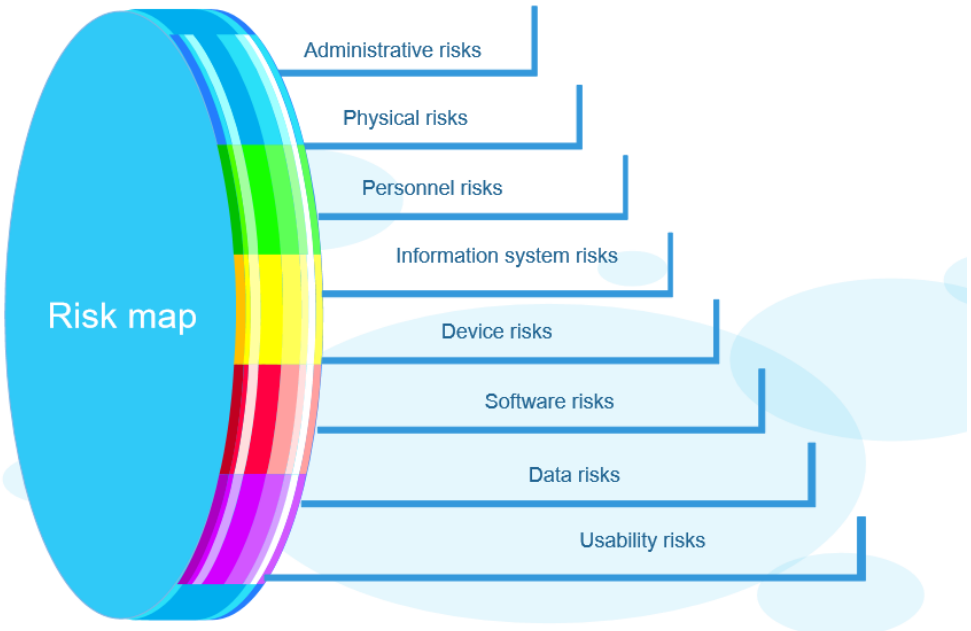

Figure 1. Risk map.

3.1 Administrative risks

The basis for administrative risks is a security policy that defines the main frames and principles of the company management.

Information security is a part of the management process in the organisation, and the company management and board should be interested in how the risk management and security matters are handled in the company.

"The frames to recognize the risks can be:

- Management awareness of security risks
- Overall security leading
- The methods of the security issues
- Personnel security training"

The administrative risks also include the relations to the external partners. The following topics should be looked at regarding the risks connected to the partners:

- Recognizing the risks
- Security solutions
- Visitors and the identification

Some threats are connected to the administrative risks if the processes are not in order inside the company:

- Missing security instructions and rules
- Lack of security training
- Lack of resources
- Lack of monitoring.

The procurement processes are included on all levels of security concerns. The main points should focus on the following items:

- Device purchases

- System development
- Usability and monitoring
- Consultation”

(Vahti 7/2003, 30-31).

3.2 Physical risks

Physical risks can be understood them as asset risks. The threats which meet physical risks are theft, inoperative services, hacked systems or unauthorized use. These threats can cause the loss of image or unproductivity for the organisation. (Harrison 2016, 215.)

The asset risks include the company premises, offices, device rooms, technical controls, water and electricity systems, etc. and how the security concerns are handled in those.

“The following items should be monitored for threats:

- The security of premises
- The main principles of system usability
- Client premises
- Reserve power systems.

The asset threats can include:

- The lack of rules and monitoring
- Technical failures like power cuts and device failures
- Human errors
- Theft in the premises
- Fire”

(Vahti 7/2003, s. 32-33).

3.3 Personnel risks

The personnel risks include job descriptions, substitute arrangements, user privileges, security training and monitoring. The personnel risks can include the following items:

- Human errors
- Antivirus threats
- Identity crimes by using other user accounts

(Vahti 7/2003, 31-32).

3.4 Information system risks

“In the information systems risks include hardware maintenance, configurations, network monitoring, backups, testing, system approval etc. When recognizing the threats, the following concerns should be considered:

- Network monitoring and routing
- Encryption methods
- Firewall systems
- Backup systems.

The information system threats can include these items:

- Lack of regulations and rules
- Lack of monitoring
- Lack of documentation
- Misconfigured user controls
- Human errors
- Incompetence”

(Vahti 7/2003, 33-34).

3.5 Device risks

Device risks include all network devices maintenance, services, guarantees and usability. The access control in device rooms is also included. When recognizing the threath the following items should be handled:

- Rules and guidance
- Monitoring
- Access control.

Device risks include the technical failures, human errors and external damages such as fire or water damage

(Vahti 7/2003, 33-34).

3.6 Software risks

Software risks include operating systems, programs and network monitoring programs. The software security field also includes user control services, backup systems and logs.

Software development must be focused on security concerns. The program must be based on best practises and common guidelines in the security field. Before taking software into use there must be a proper method for testing to recognize internal and external threats. In system development risk evaluation is important. The final result should be an integrate, reliable and useful system.

“The program lifecycle can be described in the following phases:

- Piloting
- Definition
- Planning
- Implementation
- Installation
- Maintenance of the system
- Production environment

- Version upgrades
- System retirement.

The threats connected to software risks:

- Missing security instructions and rules
- Missing staff training
- Missing documentation
- Human errors
- New technologies
- Lack of communication”

The technical risks can be disk failure, component failure, denial of service, and fire or water damage. (Vahti 7/2003, 35-37.)

3.7 Data risks

“The data risks include availability, integrity and confidentiality of files and other data. When recognising the data threats, the following items should be covered:

- Data classification
- User privileges
- Confidentiality agreement
- Data destroying
- IT device recycling
- Data Archiving
- Rules
- Privacy policy.

The data threats:

- Insufficient classification
- Expired user privileges
- Insufficient data disposal

- Insufficient user instructions
- Insufficient archiving systems
- Fire and water damages”

(Vahti 7/2003, 37-38).

3.8 Operational risks

“Operational risks cover the usability of IT devices, support agreements, development, device services, recovery plans, user privileges, backups and the equipment storage.”

If an organisation has outsourced service in use, the risk analysis should cover those too. The outsourcing does not make more risks, the outsourcing can be a good choice to prevent risks. The risks connected in outsourcing can be the delivery process and delays, lack of guidance, and human errors. Remote use is a part of usability risks; the threats included in remote use can be network lines, authentication, support services or administrative risks. (Vahti 7/2003, 37-40.)

3.9 Internal and external risks

Risk can be internal or external risk. Internal risks can include items such as personnel functions, human errors, lack of instructions and guidance. External risks are connected to the partners or external co-operation. The internal and external risks can be also seen as a part of the administrative risks.

Evaluating risk goals involves finding the best methods to act upon in security concerns. The goal is to minimize or delete the bigger risks. The main goal is to get the best level or an appropriate level for the risks in each organisation.

4 Risk evaluations

4.1 Risk levels

Risk levels can be divided in many different ways, and each company can define its own risk levels which are seen best to fit the organisational use.

The following example shows how the risk level can be categorized:

- Low
- Moderate
- High.

The same categorization can be also used to evaluate the consequences of the risks. The actions regarding how to handle the risk should be defined. (Vahti 7/2003, s. 41-46.)

4.2 Risk lists

This section gives some recommendations and guidance which kind of risk lists can be used in the organisation risk evaluation. By using risk lists, organisations can recognize the risks which are connected to the company's IT functions. The risk lists can consist of the following sections:

- Risk leading
- Client and stakeholder risks
- Staff awareness
- Asset risks
- Information system risks.

Each organisation should build the lists which fits best its own company, and the lists can be updated and developed if needed (Vahti 7/2003, 55).

Risk lists are in Appendix 1.

4.3 Auditing

Auditing should be regularly performed depending on how each organisation has defined it. Auditing should be done internally and externally. An organisation makes an internal audit by itself, and the external audit is done by a third party organisation. The risk list can be used when auditing the organisational information security concerns.

The audit process guideline

1. Sets the goals
2. Collect the decision makers to review the business needs
3. Create the scope which systems to test
4. Place the audit team
5. Audit planning
6. Carry out auditing
7. Documentation
8. Communication, to make repair plan

(Harrison, 2016, 861).

In auditing the technical controls to go through the security and risk concerns in the company network are used. Testing can base on vulnerability or penetration testing.

Vulnerability testing can be done manually, automatically or some combination of the both. Vulnerability testing is taking part of the organisation's IT staff and the external security experts. Testing requires deep knowledge of the methods of testing. A test measures the most common vulnerabilities which are commonly known in the systems.

Penetration testing is performed to simulate network attacks against the organisation's IT systems. The goal is to measure the organisation security level to prevent attacks against external threats. In penetration testing tools are used to test if it is possible to bypass organisational security systems.

In vulnerability testing the vulnerability tester tries to recognize vulnerabilities with the scanning tool. The purpose of this is to find a possible vulnerability which

could harm the security of organisation systems. Penetration testing uses an exploitation or many vulnerabilities to show that an attacker can get access to the organisation systems.

In vulnerability and penetration testing among the security professional levels or colours are used when looking at the approach of the security tests,

- Black box testing: the tester does not know anything from the organisation systems. The information will come on the basis of the assessment. Testing is done externally.
- White box testing: the tester has internal knowledge of the organisation systems and can specify more detailed testing itself. The focus is more so on the internal systems.
- Grey box testing: this mixes black and white box testing. This is done externally, and some of the internal information is provided for the tester.

  (Harrison 2016, 865-870.)

In auditing each risk area, for example asset, personnel and information system risk area, is gone through based on the risk lists. Based on these lists we get a view of the areas that require development.

4.4 Type of attacks

In recent years different kinds of and complex attacks against company networks have increased. Attackers are using more complex systems to bypass company security devices, and there is no end to these matters nowadays. There are companies that do not even know that uninvited guests have been inside the company network. Attackers can easily hide their visits in the network by deleting log files and the footsteps they have left. Some of them are doing this for just fun. Some are in it for the excitement, and others try to get benefits from the company data.

Even if inside the network security devices are in use, it is sometimes hard to identify attacker movements in the company network. Intrusion detection systems can trigger an unauthorized visit, but this is hard to track. Attackers are using

botnet networks to hide visits in the compromised network. They use private, personal home computers, use vulnerabilities on the machines, use different kinds of methods to get unauthorized access in the machine, install malicious programs on a computer by using email attachments or using vulnerabilities in a website. When the program is active, the attacker sends the command to the programs, which tell it what to do and which system to attack. These kinds of compromised systems are called *zombies*, software inside the zombies are *bots* and when an attacker has several systems compromised, they are called *botnets*.

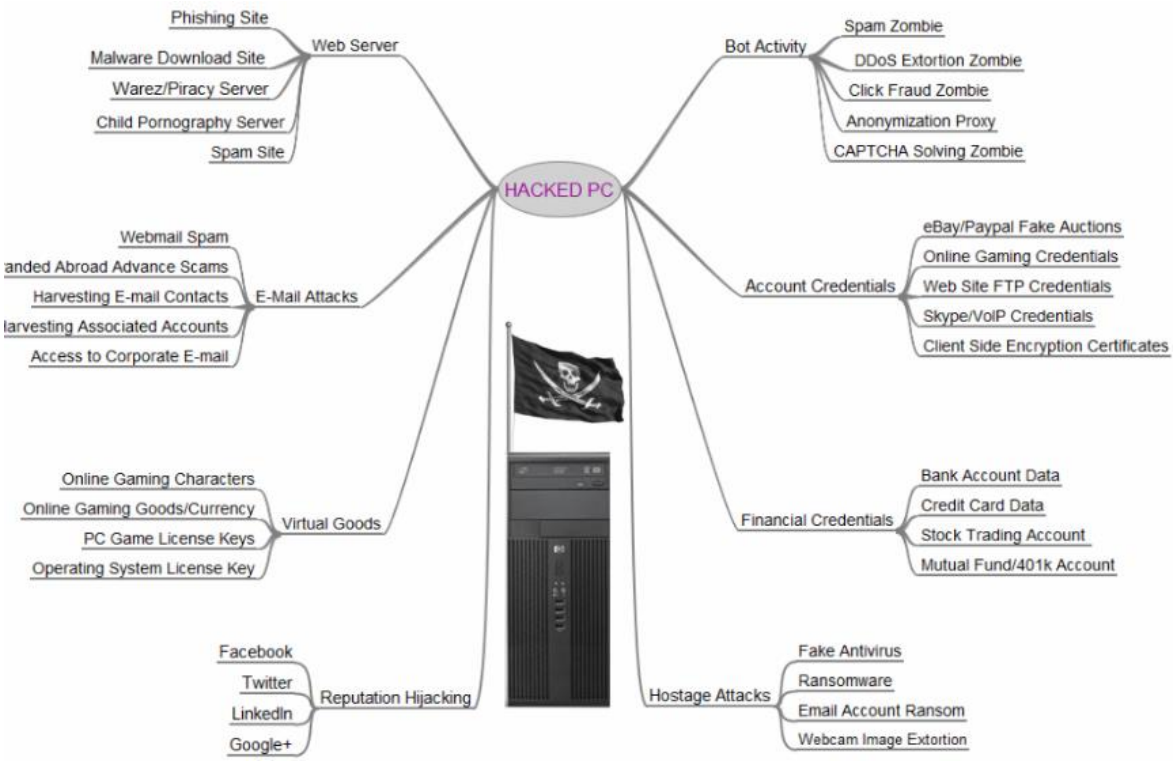

Figure 2. A hacked PC. (KrebsonSecurity 2019)

Even though machines are well-protected with all the latest updates and patches installed, protection can be hard to ensure. There are always functions which may compromise the machines, network devices, human error,

unpatched systems, and updates not installed. There are many ways to get inside a network: exploiting web services, using email attachments, program vulnerabilities, operating system vulnerabilities and so on. So, all the latest patches and updates must be installed, and users should think about which messages and windows to click if getting a strange window on the screen. When we talk these concerns, it is also a big challenge for the IT department to ensure that all systems are up to date and if enough IT personnel who can react quickly if we notice vulnerabilities or compromised systems exist. We can easily ask is it safe enough to use existing digital world services nowadays and if anyone can answer that question. (Harrison 2016 48-51.)

5 Security and penetration testing

5.1 Penetration testing basics

Penetration testing is defined as legal access to A network to find vulnerabilities and to help fix them (Kennedy, O'Gorman, Kearns, Aharoni 2011, 1).

Penetration testing can also be described as a simulation of how attackers can get access to the company network. Penetration testing is not just running a scanner; one must also be able to think about the mode of operation in which the attackers act.

Penetration testing can also be called:

- Pen testing
- Hacking
- Ethnical hacking
- White hat hacking

Penetration testing and vulnerability assessment can be mixed, but it is good to separate these two concepts. A vulnerability assessment is *a method* for recognizing potential security risks within the systems. Penetration testing is *an action* which shows that the security holes exist. (Engebretson 2011, 1.)

A common way to describe penetration testing phases is shown in Figure 3. A reconnaissance step is based on the investigation of the system features, such as system version, to find out the possible unpatched features in the system. In the scanning-step the aim is to try to find the open ports or services in the system. In the exploitation-step the system is a puppet so that the attacker can run commands on the system. In the maintaining access -step the existing connection is kept online in the vulnerable system so that the attacker is not recognized.

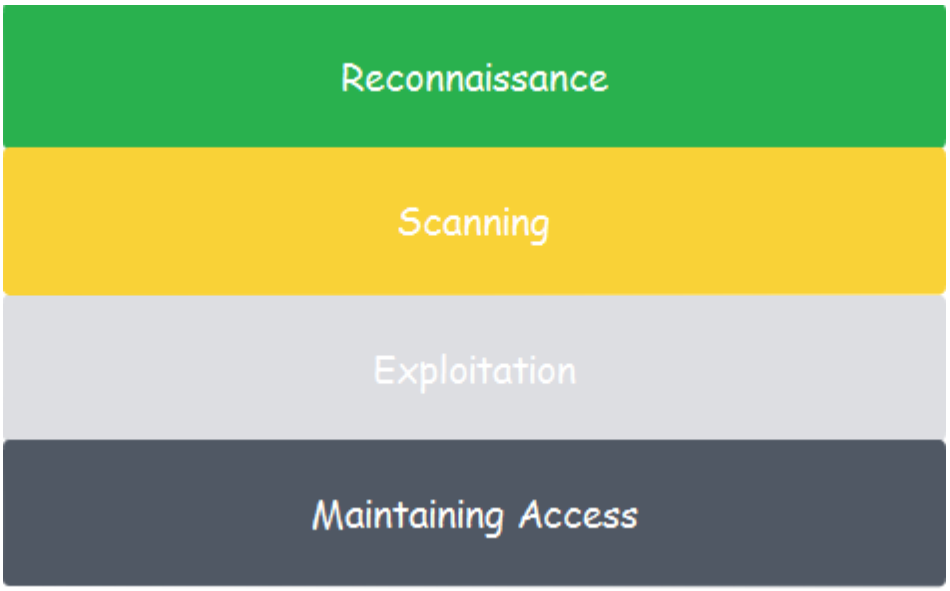

Figure 3. The penetration test steps (Source: Engebretson 2011, 11).

Penetration test steps can be divided into seven different categories:

- Pre-engagement interactions
- Intelligence gathering
- Threat modelling
- Vulnerability analysis

- Exploitation
- Post exploitation
- Reporting.

Penetration test types can be classified as overt and covert tests. Overt test is as “white hat” test and covert test as an unknown test. In overt test the organisation network features are known and recognized, so it helps to identify the security threats. The covert test is carried out without knowing any of the organisation systems. Its aim is to test the IT department’s ability to recognize attacks against the company network. (Kennedy 2011, 2-5.)

5.2 Security and penetration testing in company X

A penetration and security testing was carried out in company X during February 2017. Tests were made internally and externally consisting of the data network, security devices, servers and workstations. The applications which were running on the scanned systems were inspected.

5.3 Methods

Methods which were used in testing were based on two-phased scanning. An internal and external scanning which were made as overt and covert method.

The two-phased scanning phase was done on the external and internal networks, and the scanning methods used were ICMP, TCP and UDP scans, vulnerability scripts, Web crawling and Fuzzing. The targets were public web services.

The hosts were scanned for all known security concerns, web application configurations, application vulnerabilities and operating system known security vulnerabilities.

A summary was made of the discovered vulnerabilities. The risk evaluation was done on the basis of all vulnerabilities in the system, vulnerabilities were bundled together. Even though one critical vulnerability in the system may be found. the

other technical feature was affecting the risk level so that the risk can be seen low. (LANWAN 2017)

Risk levels were categorised to four levels,

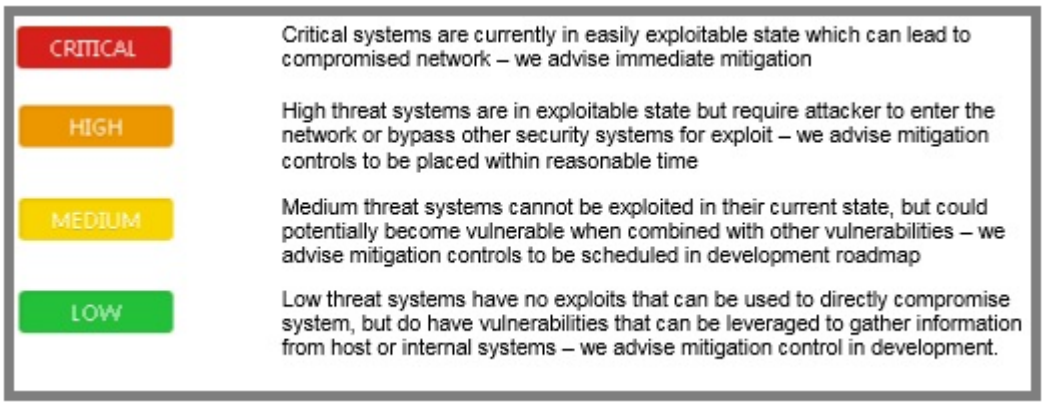

Figure 4. Risk levels (LANWAN 2017)

The following scans were made on the network:

- Public network test
    - Host based auditing for all public IPs in a company network
    - Port, operating system and service level security test
    - A test on the defined targets, based on the open ports, services and the operating system level. Evasion and anonymity mechanisms were used for scanning.
- Web service security test
    - A test for the web services where the operating systems and add-ons were scanned for the most known vulnerabilities. These included XSS Injections and Command Execution vulnerabilities, including OWASP TOP10.
- Application test

- The application level test is based on the previous tests. The aim was to find incorrect configurations and application vulnerability security holes (including OWASP TOP10).

- Firewall test

  - By-pass test on firewall and IPS (Intrusion Protection System). Firewall and IPS blade functionality were tested by using evasion techniques, such as fragmenting, splicing, firewalling and traffic replay.
  - Firewall stress test. In this Denial of Service (DOS) testing artificial traffic was created on the target.

- Internal network test

  - Internal network scanning. The internal network structure and the current situation was valuated.
  - Desktop vulnerability scanning.
    - Port, operating system and service level were scanned and all found vulnerabilities were listed.
  - Server and network device vulnerability scanning.
    - Port, operating system and service level scanning were made.

- WLAN validation test using best practices

A written summary was made based on the findings of the scans, threat level definition and mitigation. On the basis of the report development and corrective methods can be started.

5.4 Network and user security instructions

Every organisation should have common security instructions in place. The personnel should have guidelines how to act in case of data security concerns. The guidelines for the personnel and overall security guidelines for the company network on how security issues are taken care of on both the personnel and company network level. done. A Simple network security instructions are presented is in Annex 2.

Furthermore, same simple guidelines should be used by in use for all end users, in other words, users who are using information systems during working days. The simple principles are shown in Annex 3.

6 IT management and risk leading

In this section IT management is handled in general, regarding how it is connected to the risk management. The IT risks and security concerns should be part of the company management awareness. The goals and development should be included in performance management. The management persons should have some kind of view about the company security risks, not on the technical side, but overall view on the which kinds of risks is included in IT risk map.

The aim of the risk analysis is to:

- Evaluate the security needs and requirements
- Evaluate internal and external IT risks
- To clarify the requirements of the legislation
- To clarify stakeholder needs
- To define the security levels, risk lists and the methods of how to develop security

(Vahti ohjeet 2003, 10).

The information security is a part of the management process in the organisation. In each company, it must be taken care of that all the required operations are done to maintain and develop security concerns in the organisation.

The company management and board should also be interested in how the risk management and security things are handled in the company. Even in cases

where the company management does not have interest in security and risk concerns, those ought to be gone through together so that they at least are aware of how the things are done. The interest will wake up on that phase when the security and risk things start to take effect on the company business and image. Recovering from image loss takes time and this is sometimes not understood inside the organisation.

Also if the things are not handled well, in the worst cases the security and risk things can effect on the company funding if company is applying funding from external resources, in this kind of applications security and risk requirements can be defined how those should be handled inside the company and the funding is granted based on these kind of requirements. (Jordan & Silcock 2006, 6.)

The company leaders who are telling how well the company IT systems are taken care, working well and in order can be proud of it, but how many leader or the board member really knows how the IT and other risks are taken care in the company. (Jordan & Silcock 2006, 11.)

In IT risk assessment the co-operation with the company management is very important. The risk analysis can be done within the IT department and by the IT manager, but the risks and all related issues and views must go through with the company management. Company board must be aware of the risks which are related to the company business functions. Other IT related issues should be handled also with the company management or at least the company management should be to some extend to be interested in the IT concerns and how those are handled. IT decision makers and IT manager should represent IT related concerns clearly and avoid the use of difficult IT language. The things should be explained clearly for the management persons. This is the way an organisation can develop and reduce risks within the business.

Some organisations have researched how the IT departments and IT management is arranged in the organisations. On the basis of research articles every second IT manager belongs to the company management group. One of the companies which participated in the research commented on the IT functions, “IT is for our organisation very, very important, but they don’t see it as important” (Myl-

lymäki 2015, 35.). This kind of comment describes very well what kind of problems can connect to co-operation between the IT management and management group.

In the CxO Mentor research article company business representatives express that 34 % of IT managers belongs to the organisation management group. In the same article 89% see IT to be important as a competitive factor for the organisation; 52% of the respondents consider IT as a part of the company strategy, and 25% of the IT managers can participate in business strategy work. (CxO Mentor Oy 2011.)

IT department functions are seen as hard to perceive. Business representatives see that IT professionals keep the IT functions as a secret and complicated, but on the other hand communication was clear and understandable, and the IT costs were controlled, correct and transparent. (CxO Mentor Oy 2011.)

What kind of things are related to the views that IT are seen complicated and secrecy. There are different kind of views from both sides, business owners and IT. As overall the main co-operation barriers are missing leading culture, process ownership, project culture and IT terminology. The main barriers which business owners sees on their side in co-operation with IT is:

- lack of ownership in processes
- IT terminology
- lack of leading
- a bad image of IT
- lack of IT decision-making

On the other hand, IT sees the barriers as:

- lack of leading
- process ownership
- the data ownership
- lack of project culture
- IT terminology

Overall, the main barriers are lack of leading as overall, IT communication, project culture, experiences, IT skills and staff relations. Here are the main differences on the views and co-operation. (CxO Mentor Oy 2011.)

How we can improve the co-operation between the company management and the IT. For the company management guidelines,

- Keep IT as a part of company strategies
- Support financially IT functions
- Take IT as a part of decision making
- Support co-operation

IT guidelines,

- The business is a client for IT
- IT service level and cost development
- Resources in communication and interaction
- Take care of the infrastructure planning if the company management does not take care of it

(CxO Mentor Oy 2011).

Overall, the IT manager should have the real decision making on the processes and work independently within the budget. IT matters are handled with the management group where the IT manager is an expert and gives his or her own recommendation on how the IT functions and strategies are implemented in the organisation. In every company there should exist an IT steering or management group which defines the future plans and development of the organisational IT environment.

6.1 Outsourcing vs own IT

IT functions can be arranged by outsourcing, then all the IT issues are handled by the external provider. In this kind of business a big amount of money is trans-

ferred between the client and the service provider. The competition between service providers is really hard. One can choose which cloud, application and server platforms to use, and the overall company IT functions can be taken care of by outsourcing.

Can anyone be sure how the systems are taken care in the external provider networks, can the critical data be moved to the external network and is it even allowed within the company rules. These questions are nowadays handled by the IT managers and company decision makers. Which systems are sensible to outsource and does the company allow to move any critical and secure information to the cloud services. The agreements between the service provider and the customer must be written very accurately. The company needs to focus in the outsourced network on the items like the backup maintenance, data owner, reporting and the co-operation meetings with the outsourcing company.

In any case the companies are dependent on the third party partners, the systems, applications and services. Operator networks and phone services are normally delivered by the external service providers and in really specific cases those are handled on their own. As overall the companies should use certified personnel when doing system updates and installations in outsourced network services. How to do on the case if the external partner goes to a bankrupt and systems are located inside this kind of company. How are the functions and plans handled in the company when this happens, moving systems into to the own device room does not go quickly and is time consuming. Which part would be then sensible to outsource, basic IT support functions, installation services or daily basis user support. Another question is does the support functions work as well as if they were taken care of on their own, and is it enough fast and reliable? (Jordan & Silcock 2006, 11.)

6.2 Project control

Very often IT projects have become disastrous and has caused loss of money for the companies as well as loss of image. Normally the IT project is established by the project group, which puts the functions in use and follows the project phases. It is good to think about if is there some basis to establish a project group. The

establishment of the project group depends also on the size of the company, and it is also good to think about what kind of benefit we get from the project group so that the time which the project groups spends does not go for nothing.

For bigger projects it is sensible to arrange a project group to follow and monitor the project functions. There must be a responsible person who leads the project and is responsible for the project. The company benefits from the project group work if the company management is involved in the project and it is not only formal. The handled issues are real in the project meetings. The meetings are not just discussion forums, and there are decisions made which help the project to go forward. In the meetings the things which are handled are discussed with other participants and not only from the view of the project leader. The project leader is given full responsibility, the power to run and finalize the project, not to disturb him or her with the useless matters. (Jordan & Silcock 2006, 121.)

Simple project phases,

1. The methods and suitability
2. Requirements, specifications and architecture
3. Starting the project
4. Testing, acceptance and introduction
5. Follow up

(Jordan & Silcock 2006, 123).

6.3 Centralized IT

In centralized IT model all the functions are controlled by the one centralized IT organisation. The functions can be part of the parent company or differentiated in subsidiary, this way the parent company buys the IT services from the subsidiary. This kind of model is used in the municipal and state level IT function re-organisation. One differentiated company delivers all IT services to the municipality. (Myllymäki 2015, 16.)

In the centralized model whole architecture planning is uniform. The costs and investments are centralized which makes them effectively to monitor. (Myllymäki 2015, 16.)

IT organisation which is centralized will get benefits in purchases because the volumes is bigger than in tiny organisations, device investments gives cost savings with the bigger volumes. System development is faster, flexible and the system will not be fragmented when the development is under one unit. (Myllymäki, 2015, 17.)

When we look the HR policy in the centralized IT organisational level, all IT experts are collected together, information flow, changing information and the substitute arrangements are easier to handle. Changing ideas is faster and easy when all the IT persons are under the same roof. On the other hand the functions in the centralized model are not so flexible than in distributed model, handling support request are slower and can cause frustration to the end users. In many centralized environments is in use a ticketing system, through the system is handled all the support requests. Support requests can also be isolated in many different expert layers so that the basic requests are handled by the IT support department and the deeper expertise requests are handled by the special experts. Centralized IT department is described in Figure 5. (Myllymäki 2015, 17.)

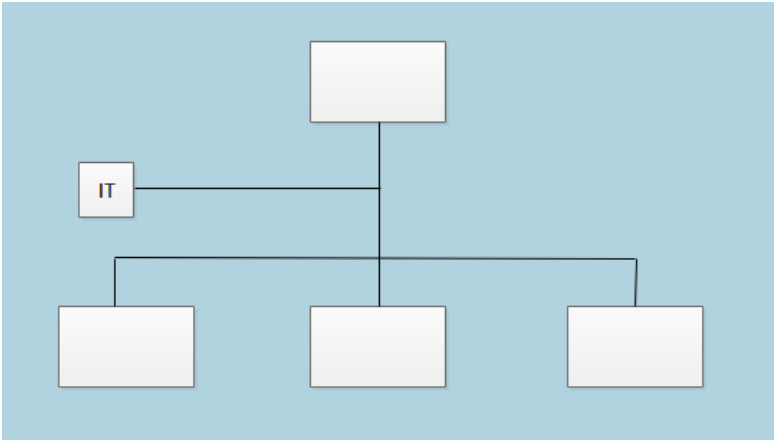

Figure 5. Centralized IT

6.4 Distributed IT

In distributed IT organisation each company unit has own IT department, which takes care of the IT functions inside the unit and is independent. Monitoring IT costs, architecture and investments is difficult. IT function in distributed IT organisation is more flexible and faster than in centralized IT organisation. End users will get answers quicker when IT requests are handled locally. (Myllymäki 2015, 18.)

In distributed model resources are put to handling same issues, the architectures are fragmented and the information is spread all over the organisation. The cost structure can come high. In distributed organisation staff amount is low and substitute arrangements can go complicate due the lack of IT staff. (Myllymäki 2015, 19.)

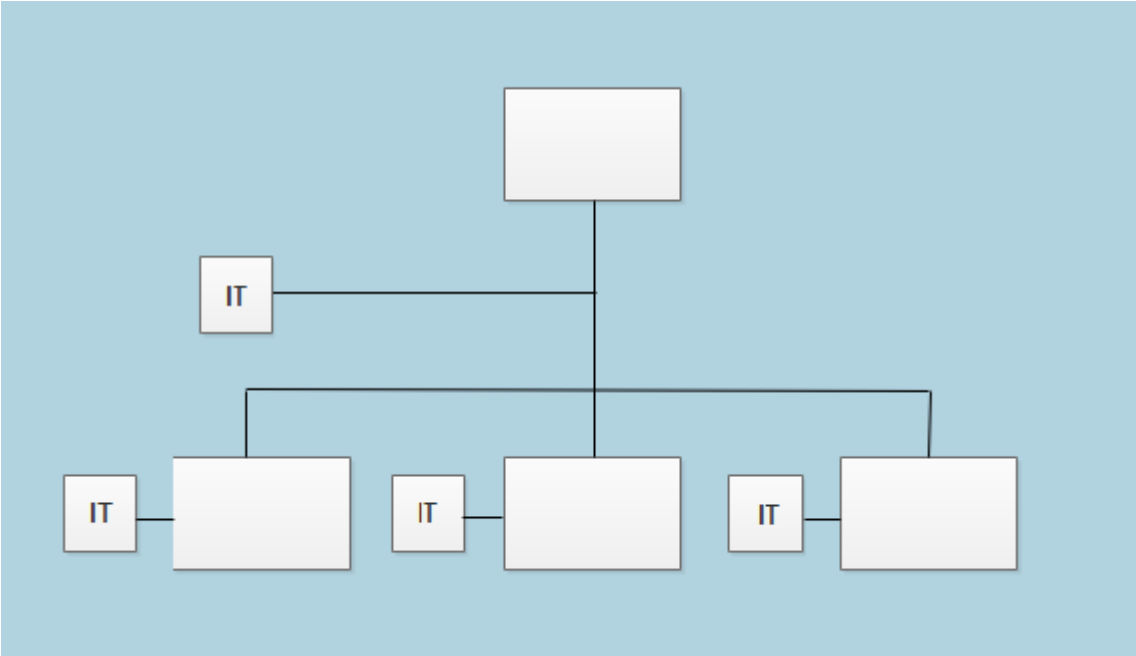

Figure 6. Distributed IT

6.5 Boundaries in IT

In IT organisation we can describe four different boundaries, described in figure 7,

- Boundary in the management and owners
- Boundary in end users
- Boundary in business
- Boundary in co-partners and resellers

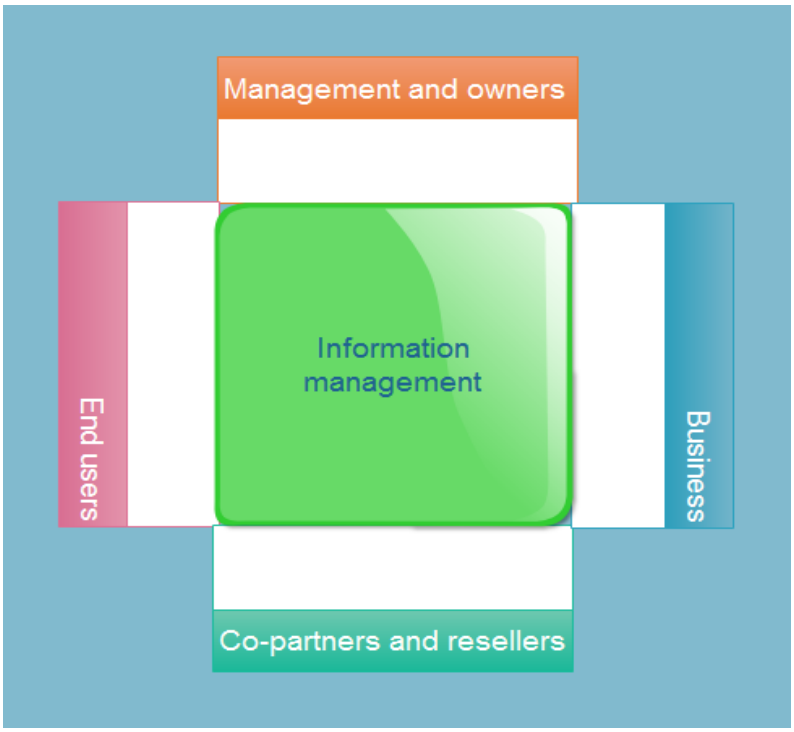

Figure 7. IT boundaries

The boundary in the management is simpliest between the IT manager and his or her supervisor. In the large organisations there can be many levels and units between the IT manager and the management. These boundaries are important because through them IT get the guidelines how to build infrastructure, budgets, system development and all other related IT functions within the company. (Myllymäki 2015, 48.)

6.6 Management and company owners

The most important decisions which are made for company IT services are always done with the company management, in some cases these kind of decisions can be handled with the company board too. The IT manager should always be a member of the company management group, otherwise the IT infrastructure development and investment decision making can go more complicated. At least in the company management group should be one business leader who understands the overall IT world and functions. If there are IT issues in the management group meetings which does not fit on the meeting minutes these can be handled in two different way,

- Extended management group is established to handle IT issues
- IT steering group is based to handle IT issues

(Myllymäki 2015, 53.)

The extended management group fits on the middle size companies and the steering group is meant mainly for the bigger companies. Steering group chairman is normally the supervisor of the IT manager and secretary is the IT manager itself. The other participants are the business leaders within the company and the IT key experts. From the IT side most important members are the IT leader and IT architecture responsible person. (Myllymäki 2015, 54.)

The composition of the management team has been discussed widely within the company management trainers, literature and guidance when it is connected to the IT functions and management. Most of them is guiding in every case that in sensible lead companies IT decision maker should be always part of the company management group. IT means an IT professional person, not a person who pretends like an IT expert, so it means real IT professional person who has worked in the IT field for years.

If we look the research which have made about the management group compositions. 34 % of the IT managers were belonging in the company management group as overall. 80 % of the IT managers who’s supervisor was CEO was belonging in the management group. Only 11 % of the IT managers were belonging in the management group who’s supervisor was the financial manager. (Myllymäki 2015, 53.)

Who is supervising IT manager. Every third part of the IT managers had CEO to supervising them, 42 % has the financial manager as a supervisor, 9 % strategy and development leader and 7 % HR leader and 9 % someone else. (Myllymäki 2015, 56.)

As overall to get IT working in the companies the most important IT related investments and plans should always go through with the company management, together to make a sensible funding and plans for the future. Not so that individuals have different opinions and everyone wants to lead IT, the overall IT responsibility must have in the IT department and IT leaders together with the company management. IT must support the company business and strategic goals, IT does not build the systems for itself, but for the company and the people who are working in the company so that the people can do their work better, easier and efficient way.

6.7 End users

For the end users IT support functions should be arranged simple way, through one channel. We can call it as a helpdesk function. A company can have one email address where all support requests are sent. From the mailbox, helpdesk experts are handling the request, the requests can be categorized so that some of them are more urgent than the others. User can also communicate with helpdesk via phone or through the network chat. Nowadays it is widely used a ticketing system. When user send a request to the helpdesk email, an automatic ticket is created in the system and based on the ticket the service request is forwarded to the correct helpdesk person. When using the ticketing system it is easy to follow up, the IT and company management get reports how fast and efficiently IT support teams works. (Myllymäki 2015, 58.)

6.8 Business

In the business or business relationship management section the co-operation between the IT and business functions should be fluent and the communication in order to get benefits for the organisation.

The business relationship management means,

- Constant and continuing dialogue between the business or management and IT
- Ability to recognize the changes in the IT technology
- Try to find new solutions and technologies for the business
- To understand the customer needs and solve the problems
- IT understands the view of the customer and is able to prioritise the problem
- High customer satisfaction

The base in the business is the co-operation between the IT responsible and business responsible person. These two equal persons should be focus on to bring value and development for the business functions, this way the business get the biggest benefits on its functions. (Myllymäki 2015, 62-64.)

6.9 Co-partners and resellers

The values which IT and IT services produces for the business comes on the devices, programs and services. This is very important to take care because it gives high value for the business and business productivity.

In the partner relationship we can see 3 different views and the meanings,

- Strategic
    - To discuss with the partners what we have achieved when working together or using the partner services
- Tactical
    - Agreements
    - Preparing new agreements
    - Handling orders and quotes

- Operative
    - Going discussion with the partners and resellers. If there exists problem those are handled together and tried to do better in the future.

(Myllymäki 2015, 69-70.)

One important boundary is connected to the ITIL services. In ITIL system the support functions are shared in different levels, in first level the support requests are received and forwarded to the next level for handling the problem. Support person then contacts to the end user, if the problem can't be solved it is forwarded to the next level, deeper expert level. These main users are focused more detailed on the system than the end users. In the best scenarios the main user can have important role as an business developer which way the business can develop the systems on the basis of the main user skills. (Myllymäki 2015, 73.)

6.10 Main responsibilities of IT

Gartner group which is an international company has done ICT research and consultation from year 1979. Gartner has published five different function which IT should do,

1. IT leading
2. Develop the overall architecture
3. Develop company business
4. Follow the future techniques
5. Partner co-operation

Gartner shares these five items so that the first 3 belongs to the CIO (Chief Information Officer) and the two last for the CTO (Chief Technology Officer). In small organisations all five are the responsibility of the CIO or the part of the items can handled by other IT organisation members. (Myllymäki 2015, 77.)

On the basis of Gartner research they have defined that organisations should have “CIO office” where the IT functions are leaded. CIO office will handle the main functions in the organisation compared to the IT services. CIO office functions,

- IT leading
- Co-ordinate the overall IT architecture
- Strategic IT purchases
- IT budget handling

(Myllymäki 2015, 81.)

As a summary IT should be part of the management and in the organisation should be IT management group or steering group. The management or steering group can’t be too wide, it can harm and slow the decision making, so the configuration should be a compact. The management or steering group is not meant to handle tiny issues. It will draw and decide the organisation important IT infrastructure strategies, financial, services and development needs. (Myllymäki 2015, 108-111.)

7 Summary and conclusions

In this section is handled the results and recommended further actions. In this development thesis it was meant to go through the organisation information security concerns and IT risk management on the basis of security checks and penetration tests. In the IT management part is handled the IT management functions in general level and how the overall organisation management is related to the risk management.

The IT management section on this thesis was handled in theory level and it was based on the earlier research and articles. Related to the IT management it would be beneficial for the organisation to establish IT management group, steering

group or risk management group, the group members are the organisation management persons with whom the most important IT plans and development needs are handled. Regular reporting from the risk concerns should be delivered to the organisation management. General level each organisation should have an IT group where responsible management persons are participating when important IT decisions are made related to the organisation IT infrastructure. Most important future development and plans should be handled with the company management and reported at least once a year so they are aware of the infrastructure changes.

When thinking about the organisation structure, teams and departments in each organisation should have its own department for each expert areas who are reporting to the company management group. IT department should be independent and should be in every case a part of management group, whether is it handled IT plans or not. In many cases in the management group is handled information technology key issues without having expertise on those. Even it seems that there is no connection in the IT matters when handling the management agenda in the meetings, certain aspects or views can come from IT point of view crucial. IT needs are often seen depreciated, because the technical aspects are not understood or seen difficult to understand. IT staff should simplify the IT terms and try to get technical aspects in understandable format.

In this organisation certain parts of the IT functions are working separately and are separate from the IT management point of view. The all IT functions should be unified under one team, not so that the software development is done separately under independent team without the real IT staff knowing what they are doing.

Like it is mentioned earlier in CxO Mentor Oy articles the organisation management should keep the IT as a part of company strategies, support IT financially and take it as a part of decision making. IT departments must see the business as their client, take care of the cost development in the IT infrastructure plans and should have resources in communication and interaction. If the company management does not take care of the infrastructure planning together with IT, IT should take care of it. The most important fact is that the IT manager should have the real decision making power on the processes and should be able to make independent decisions within the budget.

On the basis of risk lists the organisation can start to evaluate and develop IT risk assessment and get the organisation management to be aware of the IT risks. From the IT management perspective it is the meaningful to get the organisation management to become aware of the IT leading guidelines and how they are connected to the company business, security and risks.

A distributed organisation structure gives its own challenges, on this manner the IT risks and security concerns should also be handled and taken care regularly in the remote offices.

The risk and network security development will continue after this thesis. Regular security training, risk evaluation and risk auditing needs to be taken care in the organisation coming processes. The security training for the organisation staff has already started as a development functions in the security concerns. IT management processes should be unified in the organisation level, so that all IT functions would get to work smoother and centralized, not creating separate units to take care of the IT solutions. The main IT developments and plans should be handled also with the organisation management group.

The found network security vulnerabilities were not so high what was expected. The major part of the systems was up to date, not any bigger vulnerabilities were not met and the existing vulnerabilities were fixed by running some updates. Internally the major part of the vulnerabilities was fixed by running an update patch or removing the existing vulnerable program. Externally the vulnerabilities were met on the web systems and those were mainly related to the internal software development. The external vulnerabilities were not on high level and the existing concerns could be avoided by updating the operating system and the system programs. In pentesting the vulnerabilities were met in the same external services even though the risk level for those was in low level. The vulnerabilities can easily fix by running update or restricting access in the external systems.

In generally on the basis of the security principles, security standards and penetration tests the risk evaluation and auditing should be done regularly in the organisation. The auditing is based on the risk list, the organisation needs to define the timetable which fits best for them. The regularity should be cover also the

security and penetration tests. The security concerns needs all the time follow up and reaction in recognized vulnerabilities. Security development is based on the security reporting and the necessary repairs are done on the basis of the report. In this development thesis the risk lists are created which are based on ISO 27001 and VAHTI-instructions, Ministry of Finance in Finland. Risk lists can be developed during the years to fit organisation needs.

Disaster and recovery plans for the core IT infrastructure needs to define and developed within the organisation. Personnel security training must arrange regularly and it should be part of the organisation risk management. IT policies and best practises needs to be defined for the organisation.

Reference

Harrison, S. 2016. Certified Information Systems Security Professional (CISSP)

Jordan E. & Silcock L. 2006. Strateginen riskienhallinta

VAHTI. 7/2003, Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa

COBIT5 for Risk, ISACA. 2013. [Viitattu 4.11.2016]. Saatavissa: http://www.isaca.org/cobit/pages/risk-product-page.aspx

ISO 27001. Tietoturvallisuusstandardi. [Viitattu 4.11.2016]. Saatavissa: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

ISO 27005. Riskienhallintastandardi. [Viitattu 4.11.2016]. Saatavissa: http://www.iso.org/iso/catalogue_detail?csnumber=56742

Wikipedia, Brute-force attack. [Viitattu 23.05.2017]. Saatavissa: https://en.wikipedia.org/wiki/Brute-force_attack

KrebsonSecurity. The Scraps Value of a Hacked PC, Revisited. [Viitattu 18.2.2019] Saatavissa: https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

Engebretson, P., 2011. The basics of hacking and penetration testing

Kennedy D., O'Gorman J., Kearns D., Aharoni, 2011. Metasploit, The Penetration Tester's Guide

Myllymäki, R. 2015. Tietohallinnon organisointi

CxO Academy. Tietoturva kuuluu tietohallinnon vastuulle. [Viitattu 1.5.2016]. Saatavissa: https://asiakas.kotisivukone.com/files/cxomentor.tarjoaa.fi/tiedostot/cxo_mentor_tietoturvan_johtaminen_2013-05-17.pdf

Järvinen P, 2016. Luentomoniste

Laakso M, 2010, PK-Yrityksen tietoturvasuunnitelman laatiminen

Other electronical references

Risk lists

Administrative and management awareness of the security

	Yes	No
Is the company management aware of IT risks ?	☐	☐
Is the information security concerns reported to the management ?	☐	☐
Is the responsible security person nominated in the organisation management ?	☐	☐
Is the information security policies reviewed regularly with the organisation management ?	☐	☐
Is the information security policies done, communicated and approved by the company management?	☐	☐
Is the information security taken care in projects ?	☐	☐
Is the IT most important systems and functions understood within the organisation ?	☐	☐
Are there contact information with the authoritative organisations ?	☐	☐
Is the IT device room and office premise fire security taken care ?	☐	☐

Are the situations recognized which can cause disaster for the company functions ?	☐	☐
Are there any background check for new employee candidates ?	☐	☐
Is the information security responsibilities attached in the employees and partner contracts ?	☐	☐

Security risk controls

Is the disaster recovery plan as a part of the company strategy ?	☐	☐
Has the company knowledge of security concerns ?	☐	☐
Is there a mode of operation for antivirus ?	☐	☐
Does the disaster recovery plan exists ?	☐	☐
Does the security instructions exists and informed ?	☐	☐
Is the use of systems followed in non working hours ?	☐	☐
Is there a responsible person for developing security instructions ?	☐	☐
Does the security group exist in the organisation ?	☐	☐
Is there a plan for network attacks and malicious software ?	☐	☐
Does the mobile device policy exists ?	☐	☐

IT risks for clients and stakeholders

	Yes	No

Is the IT risks handled when choosing a partner ?	☐	☐
Does the partners have a security policy ?	☐	☐
Is the company security principles attached on the partner agreements ?	☐	☐
Is there a separate principles when handling organisation data by the partners ?	☐	☐
Is there security methods in use when partner is using organisation data or connections ?	☐	☐

Staff security and knowledge

	Yes	No
Has staff trained for security basics ?	☐	☐
Is there rules for acceptable use of asset ?	☐	☐
Does staff recognize which data is most important ?	☐	☐
Is there a disciplinary process in security breaches ?	☐	☐
Is staff trained to follow security guidelines ?	☐	☐
Is there a process to handle a security concerns ?	☐	☐
Does staff know where to report security concerns ?	☐	☐
Is the security policies part of employee orientation ?	☐	☐
Does staff recognize which data is most important ?	☐	☐
Does new staff members sign the agreement use of data systems and security ?	☐	☐
Is there a proper process for deleting user access after contract has expired ?	☐	☐
Is it possible to copy or take with the company critical		

data after contract has expired ?	☐	☐
Is the organisation important data stored in locked rooms ?	☐	☐
Is the disposal of important data instructed ?	☐	☐
Is staff guided in the case of fire ?	☐	☐
Is the substitute arrangements in order ?	☐	☐
Is staff trained for basic use of IT equipment ?	☐	☐
Is staff guided to use secure passwords ?	☐	☐
Is there instructions for backup and restore ?	☐	☐
Is backup monitored ?	☐	☐
Is there a guide for Internet etiquette ?	☐	☐
Is there a guide for email etiquette ?	☐	☐
Is antivirus functions automated ?	☐	☐
Is disk encryption in use on the machines ?	☐	☐
Is IT personnel training taken care that they have latest information of IT system development ?	☐	☐

Premise security

	Yes	No
Is the office premises locking in order ?	☐	☐
Is the IT device room locking in order ?	☐	☐
Does camera control exist in the premise ?	☐	☐
Is the access control in use ?	☐	☐
Is the fire alarm system in use ?	☐	☐
Is the external entry in the premises protected ?	☐	☐
Is there a guard system in the building ?	☐	☐

Is there a responsible person taking care of the access control ?	☐	☐
Is the entry on the premises restricted ?	☐	☐
Is the guest access in order ?	☐	☐
Is the device room protected in fire case ?	☐	☐
Is the leaving of the premises practised ?	☐	☐

Data security

	Yes	No
Is unauthorized access prevented in company network ?	☐	☐
Is the local network restricted from guest networks ?	☐	☐
Is data classification in use ?	☐	☐
Is data encryption in use ?	☐	☐
Is the antivirus protection in use ?	☐	☐
Is the email scanning in use on case of viruses ?	☐	☐
Is the reseller processes in order and professional level ?	☐	☐
Are licenced programs in use ?	☐	☐
Are there valid backup systems in use ?	☐	☐
Is it practised to restoring data ?	☐	☐
Is there a responsible person to taking care of the antivirus ?	☐	☐
Is data backups stored safely ?	☐	☐
Is data and system logs recorded ?	☐	☐
Is data logs protected ?	☐	☐
Is there a responsible person to grant user accesses ?	☐	☐

Is the substitute arrangements in order in IT department ?	☐	☐
Are the systems monitored automatically ?	☐	☐
Is the device purchases done from the trusted organisations ?	☐	☐
Is the system guarantees in order ?	☐	☐
Is the end user machine guarantees in order ?	☐	☐
Does the network documentation exists ?	☐	☐
Is the disposal of machines and media in order ?	☐	☐
Is data system audit or risk assessment done ?	☐	☐
Is risk assessment done regurlarly ?	☐	☐
Is UPS system in use for most important systems ?	☐	☐
Is data backups automated ?	☐	☐
The external use of company network is prevented ?	☐	☐
Is the use of the systems restricted for authorized staff ?	☐	☐
Is the granting of privileges instructed ?	☐	☐
Every user has own username and password ?	☐	☐
The employees has only access on the data which they need ?	☐	☐
Is the disposal of documents instructed ?	☐	☐
Is the device inventory in use ?	☐	☐

(ISO 27001, Vahti 2003)

Network security instructions

1. User privileges in computers without administrator rights
2. Antivirus program up to date
3. Multifactor authentication in use
4. VPN (Virtual Private Network) connections in use
5. Disk encryption in use
6. Phone management software in use. User phone security policies centralized through organisation
7. Take care of passwords. Stored safely e.g. in usb stick or by a security program e.g. Keepass
8. Mobile phone security code in use

(Järvinen 2016)

User security instructions

1. Do not click “Yes”, if not sure what does it mean. Read it carefully before click the link.
2. Do not use other user credentials without permission
3. Don’t leave printings on the table
4. Do not use guest usb stick in the personal machine
5. Do not use files on the guest machine
6. Think about which attachments to open from email
7. Use auto save when working
8. Do not speak organisation security matters to the external persons
9. Do not speak company business or secret issue in common places e.g. in train
10. Backup most important files
11. Avoid open WLANs. If need to use, do it with VPN on
12. Use always VPN when possible

(Järvinen 2016)