LAPIN AMK
Lapland University of Applied Sciences

INFORMATION SECURITY MANAGEMENT

Lu Huang

Thesis

Technology, Communication and Transport

Programme in Information Technology

2015

LAPIN AMK
Lapland University of Applied Sciences

Abstract of thesis

Technology, Communication and Transport
Degree programme in Information Technology

Author Lu Huang Year 2015
Supervisor Jouko Teeriaho
Title of thesis Information Security Management
No. of pages + app. 53 + 8

The main purpose of the thesis was to present different areas of information security controls based on the international information security standard ISO 27001. The thesis also describes the methods of risk analysis and how to establish, implement, maintain and improve information security system in organizations.

Most of the material was collected from books and various online resources. Some information was taken also from the teaching materials of the information security course.

This thesis report provides basic knowledge of information security management in both theoretical and practical aspects. As a practical part of the thesis, a sample checklist for information security evaluation was created.

Key words ISO 27001, risks analysis, information security plan

CONTENTS

LIST OF FIGURES

SYMBOLS AND ABBREVIATIONS

ISO	the International Organization for Standardization
IEC	the International Electrotechnical Commission
SLE	Single loss expectancy
ALE	Annualized loss expectancy
EF	Exposure factor
ARO	Annualized rate of occurrence
DAC	Discretionary access control
MAC	Mandatory access control
RBAC	Role based access control
ACLs	Access control lists
IDSes	Intrusion detection systems
Namp	Network mapper
VPNs	Virtual private networks
FTP	File Transfer Protocol
POP	Post Office Protocol
SSH	Secure Shell
SFTP	Secure File Transfer Protocol

1 INTRODUCTION

Information security is becoming more and more important in our daily life and it is widely adopted in computing technology. Due to a large amount of security risks in workplaces, it is essential to have good understanding of the information security management to protect the information assets and defend the organization against attacks.

The goal of the thesis is to present the phases and the structure of information security management, which can help the organization to secure the information against different risks. The information security standard ISO 27001 presents methods to establish, implement, maintain, and improve the information security to meet the organization’s own information security requirements. The sample checklist is created to help analysis the information security risks of the organization. The management can use the checklists to audit and evaluate the information security controls of the organization, and help to establish the measures to improve and modify its security policies.

2 INFORMATION SECURITY STANDARD ISO 27001

The International Organization for Standardization (ISO) and The International Electrotechnical Commission (IEC) form the specialized system for worldwide standardization. (Finnish Standards Association SFS 2013, 7.) The ISO/IEC 27001 is the International Standard that specifies an information security management system.

The objective of the ISO 27001 standard is to define the requirements for establishing, implementing, maintaining and continuously improving an information security management system. (ISO 27000 2013.) Some factors that can influence the organization information security management are the organization’s needs and objectives, the security requirements, the organizational processes, and the size or the structure of the organization. The internal and external parties can use this ISO 27001 International Standard to evaluate the organization’s ability to satisfy the organization’s own information security requirements.

3 RISK ANALYSIS

3.1 Risk Analysis Methods

3.1.1 Qualitative Analysis

Qualitative risk analysis does not allocate numbers and monetary values to the components and the losses. Instead, the qualitative methods include different scenarios of the risk possibilities and rank the seriousness of the threats and the effective of the different probable countermeasures. (Harris 2003, 72.) The qualitative analysis techniques contain the judgment, the intuition, and the experience. And the examples are as follows: Delphi, brainstorming, story-boarding, focus groups, surveys, questionnaires, checklists, one-on-one meetings, and interviews. (Stewart - Chapple - Gibson 2012, 253.) The risk analysis teams will analysis the culture of the company and decide the best technique to handle the threats.

In order to have fully analysis of the risks, the person who has experience and education on the threats will be evaluated by the risk analysis team. According to the scenario which describes the threats and the loss potential, the team will respond the possibilities of the threat and the extent of damage that may occur on their gut feeling.

A scenario is approximately one page long, and is a written description of each major threat. (Stewart - Chapple - Gibson 2012, 253.) The functional managers have the responsibility to review the scenario to ensure that it can reflect how an actual threat would be implemented, because they are extremely familiar with this kind of threat. The exposure possibility and the loss possibility can be ranked as high, medium, or low with a rating of 1 to 5 or 1 to 10. (Harris 2003, 72.) The loss potential and the advantages of each safeguard should be mentioned in the report and given to the management when the selected people rank the possibility of a threat. Because these information are essential for them

to make a better choice on safeguards implementation. The advantages of this kind of analysis are the risks ranking, the identification of the safeguard strengths and the weaknesses, and the various opinions from the people who have a good knowledge about these subjects.

Table 1. shows the result about a simple example of a qualitative risk analysis. The team analysis a threat of a hacker accessing the confidential information included five files servers in the company. The team was divided into five different fields of people (the IT manager, the database administrator, the application programmer, the system operator, and the operational manager). And then they rank the severity of threat, the loss potential, and the effectiveness of safeguard on a scale of 1 to 5, 1 is the least severe, effective, or probable. According to the data and result of the analysis, it is obvious that purchasing a firework will protect the company from this threat more than purchasing an intrusion detection system, or establishing a honeypot system. This is the result of concerning on only one threat, however, the management will look through the severity, the loss potential, and the effectiveness of each threat in order to determine the greatest risk and handle it first. (Harris 2003, 72.)

Table 1. Example of a Qualitative Analysis

Threat= Hacker Accessing Confidential Information	Severity of Threat	Probability of Threat Taking Place	Potential Loss to the Company	Effectiveness of Firewall	Effectiveness of Intrusion Detection System	Effectiveness of Honey pot
IT manager	4	2	4	4	3	2
Database administrator	4	4	4	3	4	1
Application Programmer	2	3	3	4	2	1

System operator	3	4	3	4	2	1
Operational manager	5	4	4	4	4	2
Results	3.6	3.4	3.6	3.8	3	1.4

3.1.2 Quantitative Analysis

Quantitative risk analysis uses real and meaningful numbers in all elements of the risk analysis process. The elements include the safeguard costs, the impact, the asset value, the threat frequency, the safeguard effectiveness, the probabilities and so on. Quantitative also provides specific probability percentages of the threats and the risks. In order to determine the total and residual risks, each element within the analysis will be quantified. (Harris 2003, 66-67.)

After determining the scope and the risk analysis, the next step is the data gathering which is the most difficult and time consuming part. The input for a quantitative analysis is different with qualitative analysis, because it bases on real numbers and percentages. It is essential to identify the following components in the analysis: (Harris 2003, 67.)

1. Assign the values to the assets which need to be protected.
2. Identify each threat.
3. Estimate the potential loss of each threat.
4. Calculate the possible frequency of the threat.
5. Carry out the remedial measures.

According to the quantitative risk analysis, single loss expectancy (SLE) and annualized loss expectancy (ALE) are needed in this kind of analysis step. The SLE is a dollar amount that represents the company's potential loss amount when a threat happened. (Harris 2003, 69.)

asset * exposure factor (EF) = SLE

SLE * annualized rate of occurrence (ARO) =ALE

The exposure factor represents the percentage of the asset loss caused by the identified threat. (Stewart - Chapple - Gibson 2012, 249.) For example, if a facility has the asset value of $560,000 and a fire took place, 40 percent of the facility was damaged, thus the SLE should be $224,000. The annualized rate of occurrence (ARO) is the value that represents the estimated frequency a threat will occur within a year. The range is between 0.0 (never) to 1.0 (always). For example, if the probability of a fire taking place in facility 25 times in 100 years, thus the ARO value is 0.25. Then the ALE value is $56,000 ($224,000 * 0.25 = $56,000). The ALE value means that if the management wants to protect the asset from the risk, $56,000 or less per year can be spent for protection. It is important to know the possibility of risk, the severity of risk and how much money can be spent to protect against the risks. (Harris 2003, 70.)

3.1.3 Checklists

Many international and national information security organizations provide checklists, which can be used to audit information security in an organization. The checklist contains questions, which cover all areas of the information security. By answering the questions, the organization can find out, which security controls should be paid attention to and which should be improved. A sample checklist is presented as appendix at the end of this thesis.

4 INFORMATION SECURITY POLICY

4.1 Content of Information Security Policy

The information security policy can help the organization to know the specific management direction and to meet the information security goals based on the business requirement and the regulations. The information security policy should be visible support from the management at all levels. It is essential to announce the information security policy to all employees and relevant parties, and even when some changes of the policy is made.

The information security policy should describe the target state of the data security of the company and the policy achieving this ideal state. The policy document should contain statements concerning:

1. A definition of the information security
2. A general description of the information security goals and the principles to the company
3. Setting the security controls, including defining the risks, analyzing the risks and doing the risk assessment.
4. Explain the information security policy and describe the important management requirements for the organizations.
5. A statement of specific responsibilities for the information security management
6. Documentation the references (ISO/IEC 2005, 7.)

Lapin AMK’s information security policy is presented in Appendix 2

5 INFORMATION SECURITY PLAN

5.1 Organization of Information Security

5.1.1 Internal Organization

The objective of the internal organization is to manage information security within the organization's overall administrative structure. (University of Miami School of Medicine 2006.) Firstly, it is essential to have the management commitment to the information security. The management should support the security including the clear direction of organization, the demonstrated commitment, specific task, and the performance of information security responsibilities. (ISO/IEC 17799 2005, 9.) Secondly, different parts of the organization representatives with related roles have the responsibility to coordinate the information security activities. And the information security responsibilities should be clearly defined according to the information security policy. In order to authorization process the new information processing facilities, the definition and implementation are required. In addition, the authorization processes include authorizing the purpose and the use of new facilities, checking the hardware and the software, and approving the use of personal owned information processing facilities.

Moreover, it is necessary to identify or periodically review the confidentiality and non-disclosure agreements. Because these agreements can reflect the organization's needs for the protection of the information. (ISO/IEC 17799 2005, 11.) And then, the organizations should keep in touch with the relevant authorities so that they can anticipate and prepare for the changes of law or regulations in advance. To keep a good contact with the special interest groups and the professional institute are necessary as well. (ISO/IEC 17799 2005, 12.) At last,

> "*the organization's approach to managing information security and its implementation should be reviewed independently at planned intervals,*

> *or when significant changes to the security implementation occur."* (ISO/IEC 17799 2005, 13.)

5.1.2 External Parties

The objective of the external parties is to maintain the security of the organization's information. And the external parties have the responsibility to maintain whether the information processing facilities are accessed and processed normally. (ISO/IEC 17799 2005, 14.) At first, before the external parties have access to the information processing facilities and the organization's information, it is necessary to identify the requirements for appropriate controls by using the risk assessment. When dealing with customers,

> *"all identified security requirements should be addressed before giving customers access to the organization's information or assets."* (ISO/IEC 17799 2005, 15.)

In addition, the organization should address all identified risks and the security requirements in the third party agreements. In order to meet those specifying security requirements, it is useful to consider the following terms. For example, the information security policy, the controls to ensure asset protection, the awareness of user and administrator, the access control policy and etc. (ISO/IEC 17799 2005, 17.)

5.2 Assets Management

5.2.1 Risk of Data Assets Security

In order to better manage the assets, it is important to define different kinds of data assets security risks at first. There are some specific data assets security risks as follows. For example, some important data assets are not recognized, the data assets have no named owner and the data assets are not classified. And sometimes, the owner of the data assets does not know his responsibilities and does not know how to handle the classified data. Moreover, if the

organizations do not carry out the clear rules for protect and handle the data, these potential data assets risks may bring bad influences to the organizations.

5.2.2 Responsibility for Assets

The responsibilities for assets is to protect and maintain the organizational assets. All assets should be account for, and each asset should have a nominated owner who is responsible for the protection and maintenance of the asset.

Firstly, as for the inventory of assets, all assets should be clearly accounted for. The inventory of all important assets should be maintained and updated frequently. It is important that the organization identify each major asset and assign owner. It is not enough just create a document or list all the assets. The asset inventory should include all the necessary information that can recover from an accident, including the asset types, the position, the backup information, and the commercial value. In addition, the ownership and the information classification should be developed for each of assets. It will be of great help during the recovery of major assets. There are many types of assets, including the information, the software assets, the physical assets, the services, people and intangibles. The inventory of assets helps to ensure the effective of asset protection and help to understand the commercial value of each asset to the organization. (Layton 2007, 133-134.)

The ownership of assets is also essential in the information processing environment. The asset owner should have the responsibility for ensuring the information and the assets are classified and checking access restrictions and classifications frequently. (ISO/IEC 2005, 20.)

As for the acceptable use of assets,

> *“rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.”* (ISO/IEC 2005, 20.)

All the employees, the contractors and the third party users should obey the rules of acceptable use of assets. (ISO/IEC 2005, 20.)

5.2.3 Information Classification

The information classification aims to ensure that all information assets receive the appropriate level of protection based on its value, sensitivity, criticality, and legal or the business requirement to the organization. The asset owner has the responsibility to define and periodically review the information classification. The controls of the information classification should be taken into account the business requirements as well as the associated impacts. In addition, it is important to come up with special handling measures to protect the information asset in the information classification scheme.

The reclassification for the information need to be carried out periodically, and the owner should be care of this process. However, the over-classification may cause the undue and unnecessary expenses for every large organizations. It is easier to gain support and funding from the management when the plan and the strategy were developed. And it is essential that information security mangers review the information classification guidelines and process, which can prevent the unnecessary risks involved into the organizations. (Layton 2007, 135-136.)

After the information was classified, the information labeling and handling should be developed and implemented to support the classification scheme. The procedures for information labeling should focus on the information in physical and electronic formats. The types of information which requires labeling include the paper reports, the screen displays, the recorded media, the electronic information, and the file transmissions. However, if the physical

labeling is not possible when some information in electronic form, the electronic labeling should be used. (Layton 2007, 136–137.)

5.3 Application Security

5.3.1 Application Security Risks

In order to protect the application more efficiently, the employees need to obtain the ability to define different kinds of application security risks. There are some specific application security risks as follows. For example, the security specifications for applications are not defined, encryption of data is not used to protect applications, and the backup of source code does not exist. And sometimes, the organization forget to update user when the software was updated and the older version of software are not stored. If all these risks are not defined and analysis in advance, it will cause huge threats to the organizations.

5.3.2 Security Requirements

The application security is to protect the applications by using the software, the hardware, and the procedural methods. (Rouse 2013.) A number of the threats can lead to the security issues in applications. Thus, it is necessary to meet the security requirements of applications.

When a company is purchasing the software, the company should check the background and the licenses of software provider. The background information includes software provider’s economical status, reliability, level of information security, quality of user support, other customers and the continuity of support in all circumstances. And there are some security requirements for software. It is important to define the security level for application and document software development. People should obey the principles when access to the software and use the logs. In addition, the encryption methods can be used to protect the software.

Some internal security requirements of application also need to be taken into account. For example, manager should integrity check the input data including the account number, the social security ID and some related information. And manager need to ensure the correctness of the input data by checking the right characters, the upper and lower limit of input. When inputting into the application, the manager should account for the size of the data in order to prevent the buffer overflow attack. Also the manager should authorize the users by using the principle of least privilege and should always check again before the user process an activity. (Andress 2011, 149.) These methods are useful to avoid the unauthorized access. In addition, it is important to secure the data transmission between the systems and authenticate the receiver in the data transmission.

Furthermore, there are some update security requirements of application. Before updating the software, it is necessary to do the risk analysis and impact analysis of changes. When do the testing, the testing data should be planned and protected carefully considering all possible user interfaces. After the updates, the manager should intensify monitoring and auditing, and check the possible appearance of the backdoors or the spyware. Also the old software version should be backuped if recovery is needed.

5.4 Access Control

5.4.1 Access Control Risks

In order to better manage the access controls, all the personnel should be familiar with different kinds of access control risks. There are some specific access control risks as follows. For example, the unauthorized persons from outside can access to the sensitive data, the user authentication procedures are not strong enough, and the access rights are given without checking whether the user is authorized to the data. Furthermore, sometimes the organizations forgot to remove the user rights when the worker leaves the company. All of these threats can create huge damages to the organizations.

5.4.2 Identification, Authentication, Authorization, and Accountability

When a user decided to access to a resource, it is necessary to check whether this person has necessary credentials, and whether this person obtains the necessary rights and the privileges to do so. After the user meets all the requirements and accesses to the resource, it is also essential to track the user's activities and enforce the accountability for user's actions. (Harris 2003, 110.)

The identification is a method of establishing the subject's (user, program, process) identity. The identification needs the use of username or other public information. The identification component requirements include each value should be unique, following a standard naming scheme, non-descriptive of the user's position or tasks and the identification should not be shared between users. As for the authentication, it is a method of proving the identity. Authentication can be provided with the use of passwords, the cryptographic key, the token, or biometrics other private information. (Muhammad 2013.) The accountability was done by auditing, logging, and monitoring and in order to ensure the subjects can be held accountable for those actions. (Stewart-Chapple - Gibson 2012, 11.) Figure 1. illustrates the steps when the subject accesses to the object.

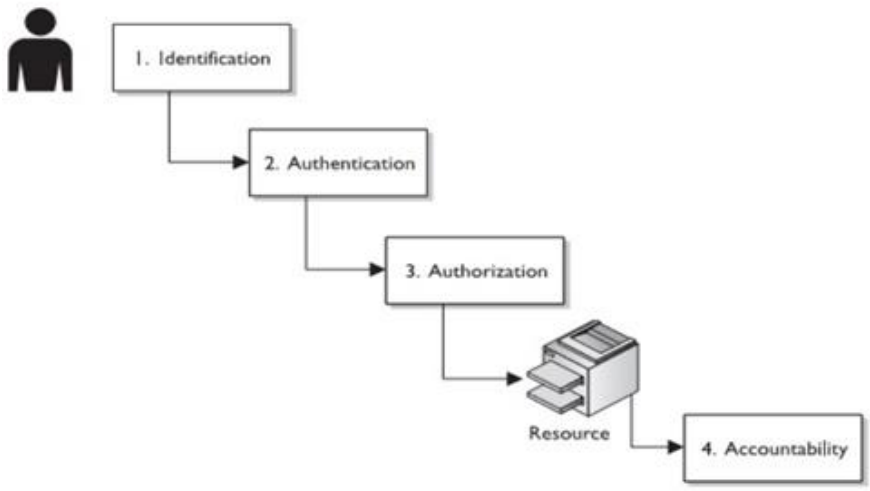

Figure 1. Steps for Subject to Access an Object (Harris 2003)

5.4.3 Access Control Models

The access control model is widely used to rule how the subjects access to the objects. The most common access control models that people will encounter in the security world include the discretionary access control (DAC), the mandatory access control (MAC), and the role based access control (RBAC). (Harris 2003, 135.)

The discretionary access control (DAC) is a model of access control based on the discretion of the owner. It allows owner of the object to control and define the subject access to that object. For example, the user who creates a new file is the owner of the file. As the owner, the user has the right to modify other users' access permissions to this file. (Stewart - Chapple - Gibson 2012, 22.)

In the mandatory access control model, the owner of resource cannot determine who can access it, however, the access is determined by the people who has the authority to set access on the resources. (Andress 2011, 42-43.) The MAC model relies on the use of classification labels which can represent the security domain. The users are given the security clearance (secret, top secret, etc.), and the data is classified in the same way. (Harris 2003, 136.) The subjects are labeled by the level of clearance, and the objects are labeled by the level of classification or sensitivity. After identifying the labels and assigning the labels to the subjects and the objects, the system makes decision about the access permissions based on the labels. In a MAC system, the subjects have permissions to access the objects which are in the same or a lower level of classification. Furthermore, the labels enforces need to know the rules. It means someone who has sufficient clearance but without need to know the information is not authorized to access to all secret data. (Stewart - Chapple - Gibson 2012, 24.)

The role based access control (RBAC) is a model of access control that define a subject's ability to access to an object based on the subject's role or the

assigned tasks. The type of roles depend on the job descriptions or the work functions within an organization. (Stewart - Chapple - Gibson 2012, 26.) The owner of resources can choose people to access to this information, and determining the role and what kind of rights and permissions to the person. For example, the data custodian (network or system administrator) does the creating of the role. The security administrator distributes the rights and the permission to the person who is decided by the data owner. (Harris 2003, 137-138.)

5.4.4 Access Control Techniques and Technologies

The different access control techniques are used to support different access control models. The example of access control techniques are as follows. The rule based access control is based on specific rules that set determines whether an access request should be granted or denied. This control is compulsory because the rules which are set by administrator cannot be modified by the users. It means that everyone is restricted by the rules regardless what type of identity the person is. (Harris 2003, 140.)

The constrained user interfaces limit the user's environment within the system, thus restricting access to certain functions or resources.

> *"There are three major types of restricted interfaces: menus and shells, database views, and physically constrained interfaces."* (Harris 2003, 140.)

When the menus and the shell are restricted, the users only have the permission to implement some options of commands that are given by the administrator. The database views are mechanisms used for limiting the users' access abilities by not allowing the users to see the data that is contained in databases. For example, if the database administrator wants the managers to check the employees' work history information, but not the salary information. Thus, the manager only has the permission to access to the work records field. The physically constrained interfaces restrict the users' functionality by setting

specific keys on the keyboard or press buttons on the screen. For example, when someone wants to get money from the ATM machine. Although this machine can accept different kinds of commands and the configuration changes in this operating system, the users are restricted by implementing these functions. The withdrawal, the view balance, and the deposit funds are available to the users by pressing the buttons. (Harris 2003, 140-141.)

The access control matrix is a table that outline the access relationships between the subjects and the objects. When a subject attempts an action, the system will determine the authorization of the subject by evaluating the access control matrix. The access control matrix presents specific rights authorized by each user for each file. The ACL which corresponds to a column of the matrix shows the authorized users and granted different level of authorization. (Stewart - Chapple - Gibson 2012, 34.) The capability table is bound to a subject and indicates what objects that subject can access. The capability corresponds to the row in matrix. The capability table and ACLs are different. Because the subject is bound to the capability table, however, the object is bound to the ACL. (Harris 2003, 141.)

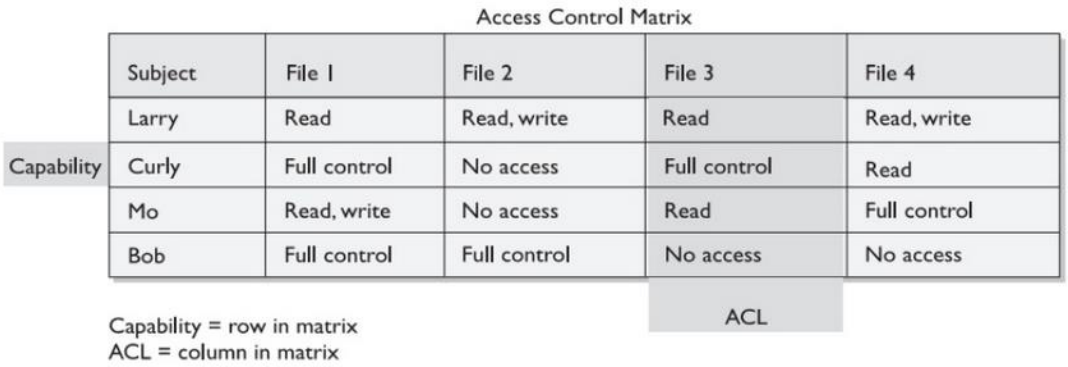

Figure 2. Access Control Matrix

The access control lists (ACLs) can be used in some operating systems, the applications, and the router configurations. The ACL is bound to an object and indicates what objects can access it. The ACL corresponds to the column in the matrix. (Harris 2003, 142.)

The capability table is bound to a subject and indicates what objects that subject can access. The capability corresponds to the row in the matrix. The capability table and the ACLs are different. Because the subject is bound to the capability table, however, the object is bound to the ACL. (Harris 2003, 141.)

In the content based access, the access decisions are based on the sensitivity of the data, not only on the subject identity. It is always used in the databases and the type of Web-based material a firework allows. The database content shows which users have right to access to the specific information in the database table. (Harris 2003, 142-143.)

5.4.5 Categories of Access Control

There are three categories of access control, which include the administrative control, the technical control, and the physical control. In the administrative controls, the management should define the roles, the responsibilities, the policies, and the administrative functions to manage the control environment.

The first step to set up a security foundation in the organization is a security policy. The policy can shape and limit the organization depending on the laws, the regulations, and the business objectives. The procedures, the guidelines, and the standards of the security policy can provide details that indicate what kind of personnel control should be used when an employee is hired, terminated, or promoted. The management also needs to build a supervisory structure. Each employee should have a corresponding superior, and the superior has the responsibility to monitor employee’s actions. In many organizations, it is essential to carry out the security awareness training in order to prevent several security incidents. Finally, the security procedures should be tested to ensure that all pieces fulfill the organization’s security goals and the objectives. (Harris 2003, 148-149.)

The physical controls can ensure safety and security of the physical environment. The technical controls, also called the logical controls, use the hardware and the software technology to implement access control. The technical controls can protect the integrity, the availability, and the confidentiality of resources by restricting subjects' access to the objects. (Harris 2003, 151-153.)

5.5 Physical Security

5.5.1 Physical Security Risks

There are some main physical security risks that the organizations need to face and deal with in order to reduce a great amount of loss. For example, the premises has no electronic access control system, the personnel have no visible ID cards when moving in premises, and the negotiation rooms have no sound isolation. As for the natural disaster threats, the thunderstorm, the fire or the water may cause big damage to the information system. Thus, it is important to define, analysis and find out good measures to handle the risks before happening.

Figure 3. Major Categories of Physical Threats (Andress 2011)

5.5.2 Physical Security Controls

The physical security controls are the devices, the systems, the people, and other methods that can be used to guarantee the security in a physical sense. The Deterrent, the detective, and the preventive are three main types of physical controls. Although each focus on different aspect, all of them are related to each other. (Andress 2011, 99.)

The deterrent controls aim at preventing the people who might want to violate the security controls. According to the pure detective controls, the sign of a specific item can indicate other controls may be in place. For example the signs in the public places that indicate that video monitoring is in place, and the yard signs with the alarm company logos which can be found in the residential areas. Although the signs do nothing to prevent people from violating the security controls, the signs can point out that there may be some bad effects to do so. (Andress 2011, 99-100.)

The detective controls aim at detecting and reporting undesirable events that are taking place. For example, the physical intrusion detection systems can monitor the unauthorized activity, such as the opening doors or windows, something being broken, and the temperature changes. Such systems can also monitor for the undesirable environmental conditions such as the smoke, the fire, and the excessive carbon dioxide in the air and so on. (Andress 2011, 100.)

The form of human or animal guards is also a kind of detective system. This type of monitoring has both the positive and the negative aspects. The bad point is that the living being may be less focused than the electronic system because of the distraction. (Andress 2011, 100.) However, the benefit of guards is that such guards can learn and recognize different attacks, and then make decisions and judgment calls under various emergency conditions. (Stewart - Chapple - Gibson 2012, 755.)

The preventive controls aim at physically preventing unauthorized entities. For example the simple mechanical lock can be used to prevent unauthorized entry including the businesses, the residences and other locations. The preventive controls also contain the fences, the bollards, the guards and the dogs. (Andress 2011, 100-101.)

5.5.3 Protecting People

Comparing to the equipment, people are more fragile. For example, under the extreme temperature, the liquids, the gases, or the toxins can be harmful to human. Also the variety of living organisms can be dangerous to people, from the large animals, to the insects, to nearly the invisible molds, the fungi, or other microscopic organisms. Furthermore, those kinds of movements such as the earthquake, the mudslide, the avalanche, the building structural issue can be harmful to the individuals. The energy anomalies such as the equipment with poorly maintained shielding or insulation, or the mechanical faults that could expose the people to the microwaves, the electricity, the radio waves, or other harmful emissions. The smoke and the fire can also be very dangerous to the people according to the burns, the smoke inhalation, the temperature issues, and other similar problems. (Andress 2011, 101-102.)

The safety of people is the most important concern in the physical security. When the emergency is taking place, saving people is the prior choice comparing with saving the equipment and the data, even if we might lose all the equipment in the data center and the potentially data that we could not replace. The evacuation is one of the best methods to keep people safe. Where, how and who are three main points that we should take into consideration when planning an evacuation.

First, it is essential to get everyone to the same place in order to make sure that people are at a safe distance. And it is easier to account for everyone if people evacuate orderly. Secondly, the route that people will follow to reach the

evacuation meeting place is also important. When planning the route, people should consider which route is the nearest to the exit and avoid the route which is dangerous and unusable in emergencies. Thirdly, the most important part of the evacuation is to ensure whether all the people escape the dangerous places.

In addition, at least two people are needed to be responsible for this process. One person is left in the building to help people evacuate dangerous areas and ensure everyone get out of building, and another person at the meeting place to ensure that all the people have arrived safety. Furthermore, it is important to train the people to equip with the ability to evacuate safely and respond quickly and properly when in emergencies or the signal to evacuate has been given. (Andress 2011, 102-104.)

A variety of the administrative controls can also be carried out to protect the people. The administrative controls may be the policies, the procedures, the guidelines, the regulations, the laws, or similar bodies, and may be instituted at any level from the informal company policies to the federal laws. One of the most common methods that companies use to protect the people is the background check. If a person who will be hired by a company, this company will do an investigation to check his or her criminal history, the verification of previous employment, the verification of education, the credit checks, the drug testing, and other items.

Another type of check should be used when a person is terminated from employment. Thus, this kind of process is to ensure that employee has returned all company property, and has no right to access to the systems or the areas anymore. The company should also ask the employee to sign the paperwork, the nondisclosure agreement (NDAs), and other agreements depending on the different position and the local or the federal laws. (Andress 2011, 104-105.)

5.5.4 Protecting Data

Second only to the safety of person is the safety of data. It is very important to prevent the physical storage media from the attackers, the terrible conditions or other threats. The adverse physical conditions may be harmful to the physical media on which the data is stored, and each type of the media has its particular weakness. (Andress 2011, 105.)

The magnetic media generally involves a variety of movement and magnetically sensitive material on which the data is recorded. The strong magnetic fields may damage the integrity of data stored on magnetic media. Jolting such media when it is being read from or written to, can cause various negative consequences. The flash media stores data in the nonvolatile memory chips. This kind of chips has better performance than other types of media, they are not sensitive to the temperature, and can survive brief immersion in the liquid if properly dried later. The optical media is very fragile, such as the CDs and the DVDs. They are very sensitive to the temperature and even the small scratches on the surface of the media may cause it unusable. Thus, the purpose-built media storage vaults are used to prevent the threats that may destroy the data on the optical media. (Andress 2011, 105-106.)

In order to protect the data, the people need to ensure that the data is available when someone need to access to it. The equipment, the media on which the data is stored and any terrible physical conditions may affect the availability of data. Not only the people need to have the data available when needed, but also it is vital important to render the data inaccessible when it is no longer required.

Sometimes, the people stores the data in several computing-related devices, such as the computers, the disk arrays, the portable media devices, the flash drives, the backup tapes, the CD or the DVD media, and similar items. It is essential to erase the data before disposing it because the media or the device

may contain some sensitive data. In the early 2000s, a research was conducted on more than 150 used hard drives purchased from different sources, most of which were purchased from the eBay. When the people analyze the content of devices, a large number of them still contained sensitive data such as the e-mail messages, the medical data, and the financial data including more than 6500 credit card numbers.

Not only these devices that obviously contain the storage and the potentially sensitive data, but also various office equipment such as the copiers, the printers, and the fax machines may have internal storage, which is in form of the hard drive. Such storage media may contain the sensitive data which can be found in copies of documents processed by the drive. If the people do not erase the data from the storage media when these devices are retired or repaired, the sensitive data may be exposed and released in the public. Thus it is essential to remove all the residual data when the devices are not used anymore. (Andress 2011, 106-107.)

In order to maintain the availability of data, it is necessary to maintain the backups. The people need to backup both itself and the equipment that are used to provide access to the data. In addition, the data can be backuped in many ways. People can use the redundant array of inexpensive disks (RAID) in various configurations to prevent losing data from the hardware failures. The people can replicate the data from one machine to another through network, and make the copies in backup storage media. (Andress 2011, 107-108.)

5.5.5 Protecting Equipment

The extreme temperature can be very harmful to the equipment. When there are a large number of the computers and the associated equipment, it is necessary to keep the temperature in a reasonable level. In addition, the liquids can do harm to the equipment, which will cause corrosion in various devices, the short circuits in the electrical equipment and some other similar effects.

Living organisms can also be harmful to the equipment. Some insects and small animals may have access to the equipment, which will cause electrical shorts, interfere with cooling fans, chew on wiring, and generally wreak havoc. The movement in earth and in the structure of facilities may cause a large amount of damage to the equipment. The energy anomalies can also be very harmful to the electrical equipment. When the power is not temporarily sending the standard amount of voltage, the equipment may be damaged. Moreover, the smoke and the fire can damage the equipment, which will create the extreme temperatures, the electrical issues, and a great number of terrible consequences. (Andress 2011, 108-110.)

When planning a new place to move, the site selection is extremely important. The cost, the location, and the construction are important for the site selection, but the security requirements of the organization should always take precedence. (Stewart - Chapple - Gibson 2012, 749.) In order to protect the equipment and ensure the safety of the people and the data, the site should not located near the natural disasters such as the floods, the storms, the tornadoes, or similar conditions. In addition, the areas that have the potential for civil unrest, the unstable power, the poor network connectivity, or similar issues are not good places to select. Thus, the people should be aware the potential site selection issues that may have bad effects and plan for such events. (Andress 2011, 110.)

It is very important to have securing access to the equipment and the facility. At the facility, the door should be locked at all times, and the badge or the key needed to enter the building. The keys are the most common and cheap forms of physical access control devices, which deployed to prevent the visitors or the unauthorized people entry to the facility. The badges can be as simple as a name tag, or as complex as a smart card for proving identity. The badges often include the pictures, the magnetic strips, and the personal information in order to help for security guard and provide permissions to access to a facility or specific workplace. (Stewart - Chapple - Gibson 2012, 757.)

Maintaining proper environmental conditions is crucial to protect the equipment. Because computing equipment is always sensitive to the changes in power, humidity, temperature, and electromagnetic disturbances. Thus, the facilities should equip with the emergency electrical power, and the systems that can change the humidity to an expected condition. (Andress 2011, 111.)

5.6 Human Resources Security

5.6.1 Human Resources Security Risks

In order to better manage the human resources, there are some human resources security risks that the organizations need to take measures to deal with. For example, the organization recruits the people who are not capable or educated enough for their jobs, the organization does not learn from information security faults, and the organization does not explain the responsibilities to the whole personnel. Furthermore, during termination of employment, the worker copies sensitive information and leaks sensitive information to the outsiders. All of these risks may make bad effects on the organizations.

5.6.2 Before the Employment

Before the employment, it is essential to ensure that all relevant parties including the employees, the contractors, the consultants, and the third-party users understand their role and responsibility to information security. In order to reduce most common threats, some measures should be taken such as properly screening and educating all the users of the organization’s information systems and the resources.

Firstly, the information security managers must document the users in the information security policy and communicate them accordingly, which can widen their roles and the responsibilities scope beyond the employee role. And then, all candidates for the employment should undergo a background check. The management should check and verify information based on the workers’ roles

and the access to the systems. Typically, the more access a user has to the sensitive data, the more background check in detail should be. The background checks should correspond with any applicable laws and meet any specific business requirements. All candidates should provide at least one personal and one business reference and supply some personal identification, such as a passport, the social security card, the driver's license and so forth. It is very helpful for the management to make an appropriate decision based on these.

Moreover, the organization should state the terms and the conditions of the contractual agreement to the employees prior to employment. Such complex legal document might be difficult for the employees to fully understand how this applies and affects them. Thus, the company should allow enough time for the candidates to review it by their legal counsel, and this time should be mentioned in the offer letter acceptance timeline. (Layton 2007, 139-141.)

5.6.3 During the Employment

During the employment, it is essential to make sure that all the parties, the internal and the external are aware of the information security threats and the vulnerabilities because they relate to their environment and their responsibility for the information security matters.

As for the management responsibilities, it is necessary to document and publish the information security policies, the procedures, and the guideline to protect the organization and the employees. And all the employees should follow and adhere the information security policy. All users of the organization's information processing facilities should receive the information security awareness, the education, or the training which is specifically aimed at the roles and the functions in the organization. The Information security policies are global in the nature and should be a high priority communicates to all employees when any modifications or additions take place. There is no doubt that the management should clearly define and publish the disciplinary actions and the associated

process for the employees who have violated the information security policy. (Layton 2007, 142–143.)

5.6.4 Termination of Employment

The management has the responsibility to ensure that the internal and the external parties' end or the change employment status in a secure manner. All the users should return all organizational assets when the employment is terminated. Moreover, the management should ensure that the logical and the physical access rights are terminated and removed immediately in the event of the termination or some other significant change event. (Layton 2007, 144-145.)

5.7 Operations Security

5.7.1 Operations Security Risks

There are many different kinds of operations security risks that the whole personnel need to face and deal with. For example, there are no descriptions of processes in the organizations, there are no instructions how to handle the classified information, and the instructions of daily tasks do not exist. Furthermore, sometimes the staff members do not know their responsibilities and do not know how to use the network and the computer in a secure way. All these risks are very dangerous to organizations.

5.7.2 The Operations Security Process

The operation security can do the maintenance to ensure the network, the computer system, the applications, and the environment run correctly and securely. Following the operations security process, the company can easily stay in the secure condition all the time. The process is to identify the information which needs to be protected, analyze the threats and the vulnerabilities, and find out the methods to tackle with those threats and vulnerability. (Andress 2011, 85.)

The most important step in the operation security process is the identification of critical information assets. And then, it is necessary to analyze the threats starting with the critical information which is identified in the first step. With the list of critical information, it is easily to determine what kind of harm could be caused if the critical information being exposed. Also it is essential to analysis the vulnerabilities which can lead to serious breaches to the security of the organization. The assessments of the risks are good for determining what issues need to be concerned with during the operations security process. And the risks are constituted by matching the threat and the vulnerability. After determining the risks that may occur according to the critical information, the organization needs to carry out measures to mitigate them. Such measures can also be called as the countermeasures in the operations security. When a countermeasure for a specific risk was found out, the manager can mitigate either the threat or the vulnerability. (Andress 2011, 85-89.)

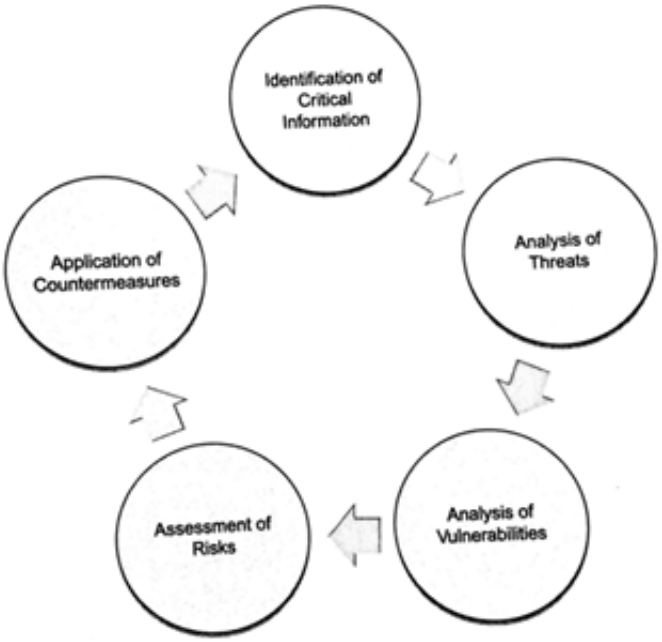

Figure 4. Operations Security Process

5.7.3 Law of Operations Security

The laws of the operations security can represent a distillation of the operations security process. And these laws can emphasize some of main concepts of the operations security process. The first law of the operations security is to be

aware of the actual and the potential threats in the critical information. It is important to understand the source of the threat and the consequence of exposing the threat in different location. And then, it is better for manager to discover specific countermeasures for the risks. This first law equates to the second step in the operations security process.

The second law of operations security is to evaluate the information assets and decide the critical information, which is similar to the first step in the operations security process. The third law of operations security is to take measures to protect the critical information from the adversaries or the competitors. These security measures are needed to prevent the breaches and can save a great number of financial damage. (Andress 2011, 89-91.)

5.8 Network Security

5.8.1 Network Security Threats and Solutions

In the world of the network security, we may encounter a great number of security threats that cause massive harm to the network. Due to the information is vulnerable to attack when it is passed between the computers, it is essential for the network security managers to spare no efforts to maintain the network periodically. In addition, it is useful to introduce the biggest and dangerous threats in detail, and to make everyone aware of the security problems and handling measures in the network. Following are some of the biggest network threats.

Firstly, a virus is a program or piece of code that can be easily loaded to the computer unconsciously and cause a great amount of damage to the computers. (Beal 2007.) The virus always contains in the email attachment. When the person opens an email attachment, the malicious code was downloaded to the computer and causes the computer to freeze. An effective way to prevent the viruses inserted to the computer is to train the staff never open any email

attachment. However, this method has little work to stop the worms from infecting the network.

A worm is similar to a virus but worm can reproduce, execute independently and spread through the network connections on its own. Whereas, the virus needs a host program to run. (TechFAQ 2013.) Once the computer is infected by the worm, it can make quick copies of itself, spread itself through the network and finally infect entire network. Thus, it is essential to use the virus protection software and keep the anti-virus up to date to protect against malware. (ITSecurity 2007.)

The Trojan horse is very dangerous, which disguises itself as something innocent and embeds on the apparently harmless programming, the website, or the data. Once the Trojan Horse is downloaded onto the computer, it begins to execute the predetermined actions that it was designed for. (Thigpen 2010.) The solution to prevent the Trojan Horse is to use the security suites, such as the Norton Internet Security which will protect the people against downloading the Trojan Horses.

The spam takes up a great number of the daily emails around the world. The spam costs very little to the sender, but the results in great amount of money to filter out this potentially malicious menace by the recipient. However, the spam is not the biggest threat in the network because even though the recipient may get annoying. And the plenty of emails do not destroy any physical elements of the network. The solution to prevent the spam is to utilize the spam filters. In addition, it is an effective way to protect your network from the spam by requiring the employees to use personal and company account separately, and the company account should not be used for any online service. (ITSecurity 2007.)

The phishing is an email fraud method that designed to trick the recipients to steal the personal account and the financial information. Typically, the

messages come from some e-commerce sites such as the eBay and the PayPal. (Rouse 2007c.) The phishing email would include a link to an insecure website. When someone clicks on this link, the new page will require reenter the personal account details. Finally, the credit card number and the password will be stolen by the phishers. (ITSecurity 2007.) Actually, the phishing is one of the worst security threats through the network, because lots of people use the computers linked to the network, it would be vulnerable to give out the personal information by accident. The solution to prevent the phishing is to use the phishing filter to filter out malicious emails. In addition, the company can educate employees never to enter the personal information through the email in order to prevent phishing form the hackers.

The packet sniffer is a device or a program that capture the data streams through the networked computers. The packet sniffers can monitor and record the information that comes through the networked computer. Sometimes, the honeypots are used to grab the personal information by setting up the unsecured Wi-Fi access points for people use in the public places. The solution is to educate the employees to never access to the internet through the unsecured connection. It is also important to let the employees know how to identify the honeypots and be vigilant when entering the sensitive data. (ITSecurity 2007.)

5.8.2 Protecting Network

It is a good way to add security in the form of the network design to prevent different threats. In addition, in order to increase the security level of the network, the company can also use the firewalls and the intrusion detection systems (IDSes).

As for the security in the network design, the network segmentation can be used to protect against the attacks. The network segmentation is a method that can divide the network into multiple smaller networks. Every small network

called as the subnet has the ability to perform its own small network. Thus, the manager can easily control the traffic between each subnet by allowing or blocking the access through the flow of traffic based on different conditions. The monitoring network traffic is easier than before as well. (Andress 2011. 116-117.)

The firewall is a network security system for controlling the traffic that flows in and out of the network based on the rules. The firewall acts as a barrier between the internal network and the Internet. (Rouse 2014.) In addition, the firewalls can be either the hardware or the software.

There are some types of the firewalls as follows. Firstly, the packet filtering firewall is one of the simplest firewall, which only filter the packets. The packet filtering will carefully look through each packet's destination IP addresses, the port number, and the protocol. The packet filtering firewalls have some advantages such as easy to operate, cost low, and fast. (Edwards 2007.) As for the application-level firewall, it acts as an application proxy. The application level firewalls have the ability to monitor and block malicious threat to protect the sensitive information based on the specific set of rules and the configured policy. (Goodwin 2007.) The application firewall aims to control the network traffic on any OSI layer up to the application layer. The IT administrators can build the application level firewalls to warn when the predefined condition of event occurs. However, the stateful firewall is able to track of the state of network connection. (Andress 2011, 118.) This kind of firewall can identify the traffic as well, only the packets that match a known connection will be allowed by the firewall.

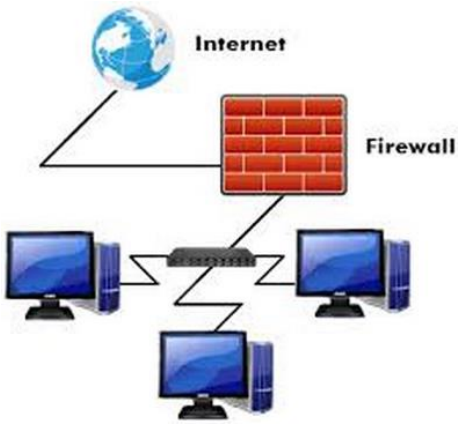

Figure 5. Firewall

The intrusion detection system can be divided into two types: the signature-based detection and the anomaly- based detection. The signature-based IDSes can detect and compare different types of attacks based on the database of the signatures in this system. This is a reliable way of protecting network from known threats. However, it may not work when the attack that is new and the construction does not match the existing attack signatures. Thus, this is one of the weakness of the signature-based IDSes method. (Andress 2011, 120.) Another IDS detection method is the anomaly-based detection. The anomaly-based detection can detect the network traffic that against the baseline or something out of ordinary. It is totally different with the signature based detection, because the signature based systems only detect attacks that signature were developed. The drawback of anomaly-based intrusion detection is the high false positive rate. (Edwards 2008.)

5.8.3 Protecting Network Traffic

Besides protecting the network from intrusion, it is also essential to take measures to protect the network traffic. In order to protect the network traffic, it is important to use security measures to protect the wireless network. In addition, the VPNs can be used to secure the connections for the unsecured networks, the secure protocol also can be used as general security measure. (Andress 2011, 129.)

When sending the sensitive data through the network, the data might be intercepted, and the eavesdropper can collect the information from the sender. The data can be intercepted from both wired and wireless. The wireless networks are the major security risks which can lead to the data exposure. For instance, many free wireless networks are available in the restaurants, the airports, the offices, the hotels and other places. Although it is wonderful to get access to the Internet for free without the password and any encryption, it still has the potential security risks.

However, the risks also exist even the password is needed for accessing to the network, such as in a hotel. If someone is on the network in the hotel, the person maybe looks through others data who are also on the Internet. In particular, the wireless access points which are attached to the network without authorization can also be called as the rogue access points. It may cause serious network security problems when the rogue access point was established in a poor or no security.

In addition, it is possible that the network intrusion detection may detect the information from the rogue access and deal with the attack at once, however, there is no guarantee for this. Thus, the typical solution to find out rogue facility is to document legitimate and authorized devices on the wireless network carefully, scan other devices by the tools such as the Kismet. It is also necessary to use the encryption to protect the network traffic that access through those authorized devices. (Andress 2011, 122-123.)

The virtual private network (VPNs) is a safety and stable tunnel which pass through a chaotic public network. The VPN is also defined as a temporary and safety connection that is established through a public network such as the Internet. The VPN aims to provide the credible connection and the safety data transmission within the distributed enterprises, among the business partners, the corporate offices and the remote users. (Moore 2008.) The message of the

VPN transmit messages to the intranet network via the public network architecture. It use an encrypted channel (Tunneling Protocol) to achieve confidentiality, sender authentication, message accuracy and some other effect of private message security. The VPN can be used in unsecured network such as Internet to send reliable and secure message.

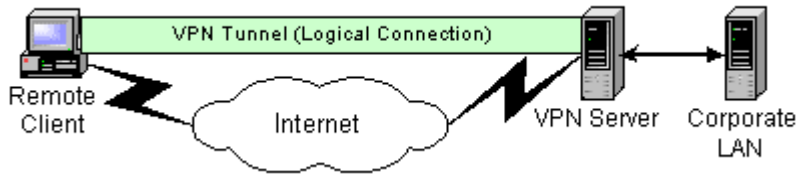

Figure 6. VPN Connection

The general way to ensure the security of data when transmitting through a network connection is to use the network security protocols. The network security protocol aims to avoid unauthorized access to the network sensitive data. In the network security protocols, the cryptography and the encryption methods are widely used to protect the data. (Janssen 2010.)

Many traditional network protocols such as the File Transfer Protocol (FTP), the Post Office Protocol (POP), and the Telnet are insecure. Because such protocols transmit the passwords and the data in clear text through the network. It is very easy for the attackers intercept the sensitive data from the network traffic. Thus, the people can use the secure protocol when sending the message. For instance, the people can use the Secure Shell (SSH) instead of the Telnet, and use the Secure File Transfer Protocol (SFTP) instead of the FTP. (Andress 2011, 123-124.) Using the SSH is a good way to encrypt all the data before transmitting in order to prevent the DNS fraud and the IP fraud. Another advantage is that using the SSH can also accelerate the speed of the transmission, due to the data has been compressed before sending.

5.8.4 Network Security Tools

It is essential to use the network security tools to maintenance the network security. The tools are the same with the tools that attackers use to penetrate the networks. It is easier to locate and repair the security holes over the network by utilizing these tools. However, the tools can only be used to deal with known issues rather than updated, unpublished, or new attacks. (Andress 2011, 124.)

Firstly, the attackers can access to a wireless device and bypass all the security measures that manager made. However, if the managers did not take measures to deal with the unauthorized wireless devices, it would cause serious consequence that the network will have a big hole and the people do not know it. (Andress 2011, 125.) Thus, some tools need to be used to detect the wireless devices. The Kismet is a wireless network detector, a sniffer, and an intrusion detection system for 802.11 layer 2 wireless LANs. (Kershaw 2011.) In addition, the Kismet can run on Linux and in BackTrack CD.

The scanner is one of the main tools for security testing and assessment. The scanners can be divided in two types: the port scanners and the vulnerability scanners. One of the best known port scanners is the Namp (Network Mapper). The Namp can discover the hosts and the services on a network and an operating system detection. In addition, the Namp can provide further information on target host by analyzing the specially crafted packets that was sent by the Namp. (Andress 2011, 125.)

The protocol analyzer or the packet sniffer are the network security tools that can be used to detect the network related problems. The packet sniffers can intercept the network traffic through wired or wireless network. On the network, what network traffic that people can see by the packet sniffers depends on the structure of network. Thus, the packet sniffer might see only certain segment of it. After the raw packet data is collected through the network traffic, the packet sniffing software will analyze it and then use a human understandable way to

present to the people. The network technicians can find out the problems on the network and take measures to handle the matters immediately. (O'Donnell 2014.) The Tcpdump is a common sniffing tool that can run under the command line and can detect the network activities. The Tcpdump runs most on the Unix-like operating systems. However, the WinDump is the port of the tcdump for Windows. The Wireshark, originally named the Ethereal, is also a sniffer that is very similar to the tcpdump. But the wireshark has a graphical front-end, and it obtains filtering, sorting and analysis tools. (Andress 2011, 126-127.)

The honeypot somehow can also be viewed as a network security tool. The honeypot is a computer system on the network that is established to detect, monitor, and trap the attackers. (Rouse 2007b.) The honeypots intentionally to present the vulnerabilities of the network to attract the attackers, which can serve as bait for the attackers. However, the vulnerabilities which are displayed by network technicians to bait attacker is totally false. Actually, doing like this, the honeypot can monitor how the attackers penetrate other people's computer systems and catch the attackers to improve the network security. The honeypots can also be expanded into larger structures by using several honeypots in a network, it is known as honeynet. (Honeynet Project 2006.) The honeynet can be used for the large scale monitoring of the malware activity. And the honeynet is a worthwhile target that seems like a network including the real applications and the services. (Rouse 2007a.)

5.9 Privacy Protection Legislation

There are some basic principles for each organization to set up an information privacy legislation. Firstly, each person has privacy right. The personal information including way of the life, the religion, the family conditions and some other privacy information. Thus, those personal information, the home of each person, the email and the telephone calls should be protected by the corresponding company. However, if the person is suspected of sever crimes, there can be exceptions to this person's privacy.

5.9.1 Law of Personal Data Register

When registering the personal information, the organization should take specific care. In the working life, the employer need register the workers' personal data. In the business areas, the customer registers are required. Also the personal data registers exist in institution, for example the student register in the school or the tax register.

There are some main regulations for registering the personal data. Firstly, the company or the organization should declare the purpose of the register. The target person also has right to know the purpose of the personal data collecting. If the personal data will be put on the website, the organization should get the permission of person at first. The normal purpose for registering the personal data are voluntary acceptance from the person, for relevant connection, and obeying some laws. Also there exist some special purposes which conditionally justify collection, such as for the direct marketing, the scientific research and the credit rating.

However, there are some information that cannot be registered including the race and the ethnicity, the political and the religious views, the trade union membership, the criminal acts (except the police registers), the state of health (except hospitals) and etc. Furthermore, the registered person has some rights in order to ensure security of the personal information. The registered person has right to check the information and require the correction of false information. And the registered person can forbid that personal data is for commercial use. Meanwhile, the organization should inform the registered person about the existence of information in registers.

5.9.2 Law of Privacy Protection in Working Life

The law of privacy protection in working life aims at the employee registers. At first, the company can only register the personal information which is necessary for the employment. And the company should get the information directly from

the employee, or ask employee's permission to collect the information through other sources. And then, the company needs to have the health information from the employees. If this information is needed for example for the payment of salary, the health information should be get from the employee or the agreement from medical institutions. Meanwhile, the company should keep the health information separately and only specific persons in this company have right to see the medical documents. Also, the employee need to perform the drug tests if the drugs may risk other people's lives, the security of the state, the traffic security or some other factors that can lead to serious consequences. The psychological tests sometimes are also needed for evaluating employee's training needs and the qualification for the job. But the company is not allowed to have a genetic test for workers.

It is possible for the company to use the video control to increase the safety of employees, customers, property, production process and the prevention of risk situations. But the video control is not allowed to use for the surveillance of a single worker or the named workers. And all the staffs must be informed openly about this video control. The company is allowed to open workers' mailbox with the help of the administrator in following conditions. For example, when the employee cannot open the email because of the illness, when the company needs fast reaction for the business issues, or when the emails require the response because of the obvious present tasks.

6 INFORMATION SECURITY INSTRUCTIONS FOR PERSONNEL

6.1 Internet and Email Policy

Nowadays, the Internet and the email are widely used for searching and communication. However, the email or the internet always does not protected safety. Thus, the confidential information will be easy revealed in unencrypted via the internet. The email and the internet should be carefully used each time. (Ministry of Finance 2014.)

There are some important internet and email policies that the people need to obey as follows. Firstly, at the workplace the internet and the email are only for official use, the private email address is only for the personal communication. The confidential information must be encrypted by the information management before sending through the internet, and the employees need to learn how to use the encrypted products in case of the unpremeditated sending information unencrypted. In addition, the information management need to install all necessary programs for each computer. Because it is completely forbidden downloading through the internet if the reliability of the software and its source are confirm which is based on the organization specific instructions. Also it is very important to empty the internet cache and the cookies when using the public terminals or a computer in possession of other people.

When sending the emails, the work-related-email must only be received and directed to the email system of one’s own organization. If any work-related email is sent to the personal email, the employee should have the responsibility to follow the official duties to deal with it. Sometimes, the email attachments may contain the malware (virus, worms or Trojan horse). Thus, the employees should not open the suspect email message and act only follow the instructions or the contact information management. Finally, when an employment relationship ends, the corresponding email address and the email box should be deleted. The official mail should always be available to the employer.

6.2 Passport Policy

There are some important passport policies that the people need to pay attention to. For example, do not disclose the passwords to others, create strong security passwords, and change the passwords immediately when it may be disclosed. The employees should not use the user ID or the password given by the organization for the internet services. In addition, it is important that the use of the shared accounts should be approved by the owner. A shared account password should be changed sufficiently often when some user’s right ends or someone is not in this group.

7 CONCLUSION

The information security management are widely used all around different organizations. A good knowledge of the information security management can assist the organization to prevent the security risks, protect the sensitive information and reduce a great amount of loss. In order to let readers know how to better manage the information security of organization, the author presented different security controls based on the international security standard ISO 27001. For example the access control, the physical security, the human resources security, the operation security and etc. Therefore, the manager can take measures to improve and modify the law or the policy of the organization according to the risk analysis.

Above chapters also provide the checklists sample and the information security sample for better understanding the process of the information security management. After doing the research of the information security controls, it is obvious that the information security management is significant in every organization. After reading this thesis, the readers will acquire the basic knowledge of the information security management in both theoretical and practical aspects.

REFERENCES

Andress, J. 2011. The Basic of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Massachusetts: Syngress.

Beal, V. 2007. Computer virus (virus).

Address: http://www.webopedia.com/TERM/V/virus.html

Accessed 20 November 2014.

Edwards, J. 2007. The Essential Guide to Firewalls. Address:

http://www.itsecurity.com/features/essential-guide-firewalls-061208/. Accessed 27 November 2014.

Edwards, J. 2008. The Essential Guide to Intrusion Detection and Prevention Systems. Address: http://www.itsecurity.com/features/essential-guide-idps-042408/. Accessed 29 November 2014.

Finnish Standards Association SFS. 2013. SFS-ISO/IEC 27001.

Goodwin, M. 2007. Introduction to Enterprise Network Firewalls. Address:

http://www.itsecurity.com/features/intro-enterprise-firewalls-012507/. Accessed 28 November 2014.

Harris, S. 2003. CISSP Certificate All-in-One Exam Guide. California: McGraw-Hill/ Osborne.

Honeynet Project. 2006. Know Your Enemy: Honeynets. Address: http://old.honeynet.org/papers/honeynet/. Accessed 5 December 2014.

ISO 27000. 2013. An Introduction To ISO 27001 (ISO27001). Address: http://www.27000.org/iso-27001.htm. Accessed 23 March 2014.

ISO/IEC 17799:2005(E) Information technology - Security techniques - Code of practice for information security management.

ITSecurity. 2007. Network Security Threats for SMBs. Address: http://www.itsecurity.com/features/network-security-threats-011707/. Accessed 20 November 2014.

Janssen, C. 2010. Network Security Protocols. Address: http://www.techopedia.com/definition/29036/network-security-protocols. Accessed 5 December 2014.

Kershaw, M. 2011. KISMET. Address: https://www.kismetwireless.net/index.shtml. Accessed 4 December 2014.

Layton, T.P. 2007. Information Security: Design, Implementation, Measurement, and Compliance. New York: Taylor & Francis Group.

Ministry of Finance. 2009. Security Instructions for Personnel. Address: http://www.vm.fi/vm/en/04_publications_and_document

s/01_publications/05_government_information_management/20090623Inform/information_NETTI_%2B_KANNET.pdf. Accessed 23 March 2014.

Moore, J. 2008. The Essential Guide to VPNs. Address: http://www.itsecurity.com/features/vpn-essential-guide-042108/. Accessed 5 December 2014.

Muhammad, W.R. 2013. Access Control. Address: http://www.slideshare.net/wajraj/access-control-presentation-23717821. Accessed 12 November 2014.

O'Donnell, A. 2014. What is a Packet Sniffer? Address: http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm. Accessed 4 December 2014.

Rouse, M. 2013. Application security. Address: http://searchsoftwarequality.techtarget.com/definition/application-security. Accessed 19 December 2014.

Rouse, M. 2014. Firewall. Address: http://searchsecurity.techtarget.com/definition/firewall. Accessed 27 November 2014.

Rouse, M. 2007a. Honeynet. Address: http://searchsecurity.techtarget.com/definition/honeynet. Accessed 5 December 2014.

Rouse, M. 2007b. Honey pot (honeypot). Address: http://searchsecurity.techtarget.com/definition/honey-pot. Accessed 5 December 2014.

Rouse, M. 2007c. Phishing. Address: http://searchsecurity.techtarget.com/definition/phishing. Accessed 25 November 2014.

Stewart, J-M. – Chapple, M. – Gibson, D. 2012. CISSP: Certified Information Systems Security Professional Study Guide (6th Edition).

TechFAQ. 2013. Computer Worms. Address: http://www.tech-faq.com/computer-worm.html. Accessed 20 November 2014.

Thigpen, A. 2010. Trojan Horse. Address: http://www.symantec.com/security_response/writeup.jsp?docid=2004-021914-2822-99. Accessed 20 November 2014.

University of Miami School of Medicine. 2006. Organization of information security (ISO). Address: http://privacy.med.miami.edu/glossary/xd_iso_org_info_sec.htm. Accessed 21 December 2014.

APPENDICES

Appendix 1. A sample checklist for information security auditing

Administrative information security	Yes	No	For us irrelevant
1. Does the organization have written the data security policy			
2. Does the organization have the IT security management team			
3. Does the organization have a written IT security plan			
4. Does the organization have the systematic assessment method			
5. Do all staffs receive education in the IT security			
6. Does the organization have a clearly written IT security manual			
7. Is the security manual maintained and updated regularly			
8. Is there a clear procedure for reporting security problems			
9. Are security events reported regularly to the leadership			
10. Does the company assign employees in charge of security			

Data assets security	Yes	No	For us irrelevant
1. Does the owner of data assets know his responsibilities			
2. Are there clear rules for protecting and handling the data			
3. Is there risk analysis for data			
4. Does the personnel know how to deal with the classified data			
5. Is there clear method for labeling the classified data			
6. Can the personnel recognize the important data assets			
7. Is there safety physical location of the classified data			
8. Does the personnel return all the sensitive data after termination of the employment			

9. Do the third parties, the partners or the customers know the rules of handling the classified data

10. Do the data assets all have the named owners

Physical security	Yes	No	For us irrelevant
1. Are the construction of company premises strong enough to prevent accidents			
2. Do the premises have electronic access control system			
3. Are there some separate locations for storing backup tapes			
4. Do the premises have emergency alarm system			
5. Do the negotiation rooms have the sound isolation to protect the sensitive information			
6. Do the premises have reserve power system when the emergency accident happens			
7. Does the organization have the security officer and the security plan			
8. Are there some security controls when other company's workers or visitors go to the premises			
9. Is there a system for managing and keeping the traditional keys			
10. Do the premises have the first-aid equipment such as the fire extinguishers and the gas masks when the natural disaster happens			

Human security	Yes	No	For us irrelevant
1. Do the new employees get adequate information security education			
2. Do the employees have adequate education of handling rules to classify the data			
3. Does the organization has procedure for dealing with the security			

problems

4. Do the whole personnel know the responsibilities of the information security

5. Can the personnel recognize different information security risks

6. Do the employees know how and where to report the security problems

7. Does the organization have the information security plan and the instructions

8. Do the employees know the meaning of the nondisclosure agreement and the responsibilities to secure the sensitive information

9. Do the superiors cancel all the rights immediately during the termination of the employment

10. Do the employees return all the information assets and the property after the termination of employment

Operation security	Yes	No	For us irrelevant
1. Are system updated properly			
2. Are there instructions for handling daily tasks			
3. Do the personnel know how to use network, email, and own computer in a secure way			
4. Are there instruction for where and how to save confidential information			
5. Are performance, capacity and failures of systems observed and measured immediately			
6. Does the employee check the recipient before sending the email containing sensitive information			
7. Is data backupped, and ensure the backup contains all important data			
8. Are there descriptions of processes in the organization			

9. Do the own workers and workers of subcontractor follow the handling instructions

10. Are system developer authorized before accessing to the data

Privacy laws and legal issues	Yes	No	For us irrelevant
1. Does the organization has the knowledge of laws and regulations			
2. Does the organization follow the laws when handling the information			
3. Does the organization use the legal software that meet the license requirements			
4. Does the personnel know the consequence of using illegal software			
5. Are there instructions how to purchase new software for organization			
6. Are copyrights monitored in the organization			
7. Is there regular monitoring of information security			
8. Are private keys of RSA encryption protected properly			
9. Does the organization follow the standards in the software development			
10. Is the information security requirement definition done before buying the new software			

Appendix 2. LAPIN AMK information security policy

The objective of the information security policy is to present the LAPIN AMK's management of determining the goals, the responsibilities and the methods. The IT security work concerns every employee and student in the university and it is regarded as part of the quality work.

Target state and goals

1. The goal of the LAPIN AMK's IT security work is to protect uninterrupted operation of information systems and networks
2. Prevent the unauthorized use of systems, intentional or unintentional destruction of destruction of information
3. Take measures to avoid the threats and the exceptional situations in advance
4. Protect the LAPIN AMK's information systems and the services in normal and exceptional conditions by using administrative and technical methods
5. The IT security functions in LAPIN AMK's can meet different needs of different departments
6. The IT security of LAPIN AMK is in good national and international level

IT security definitions

IT security is based on the principles of confidentiality, integrity and availability of information, access control and non-repudiation

1. The confidentiality means that only the authorized people have access to the information

2. The integrity means that the information is correct, reliable, and it will not change by the hardware or the software faults, the nature disaster or the unauthorized human actions
3. The availability means that only authorized users are available to the information and the IT systems in a reasonable time
4. The access control means to avoid the unauthorized use of the IT systems
5. The non-repudiation means creating evidence to make sure that no party will deny participation in the actions

The IT security work includes the technologies of securing information, equipment, and economical resources. The LAPIN AMK's security system is based on the national and the international laws and follows the instructions given by the Finnish government.

Responsibilities

The IT security is part of the organizational security of LAPIN AMK, the president of the LAPIN AMK has the highest responsibility. The manager of the LAPIN AMK has the responsibility to do the security development plan and supervise the measures with the authorization given by the president. The manager also need to provide the budget resources for the LAPIN AMK's faculties and departments in order to maintain and develop the IT security in their own condition. Every employee and user has his own part of the responsibility for using, handling, and maintaining the information systems.

Methods of implementation of security measures

The implementation of security measures are based on the security policy document. All the employees, students and users of information system must know about those security measures. The manager should analysis the IT security risks of the LAPIN AMK. And then the IT security development plan is created based on the risk analysis. This plan must be updated periodically. Furthermore, the information and systems must be classified according to the

information systems. Each information system should assign a system administrator. And the required security level and the security measures must be decided for each confidentiality class.

Monitoring IT security and dealing with security problems

The president can authorize the IT manager and the IT security employee to monitor the security level. And every user has the responsibility to follow the security instructions and the rules. The users and the maintainers must report the faults and misuse to the IT employee, and then the IT security employee or the IT manager will response the reports and handle the issues accordingly.