Implementation of information security policies in public organizations:

Top management as a success factor

MASTER THESIS WITHIN: *Informatics*
NUMBER OF CREDITS: *30 Ects*
PROGRAMME OF STUDY: IT Management and Innovation
TUTOR: *May Wismen, Christina Keller*
JÖNKÖPING: May 2017

Abstract

The purpose of this thesis is to investigate potential success factors related to the implementation of an information security in organizations, with a specific focus on the role of top management in implementing information security policies in organizations. The following are the research questions: What are the factors related to the implementation of an information security in organization according to the literature and what is the organization's view of these factors? What is the role of the top management in implementing an information security policy in an organization according to the literature and what is the organization's view of the role? A case study approach was implemented in this study, collecting data from both primary and secondary sources by doing a literature review, and interviews. A document analysis was done as well as a field visit.

Based on the literature, the success factors related to the implementation of an information security in organization are: management support, security awareness and training, budget, information security policy enforcement, organization objectives and goals. Based on the interviews, both two organizations agree with those success factors found in the literature. Regarding the role of the top management in implementing an information security policy in organization, the two organizations have different views on that role. For one organization, the successful implementation of an information security policy does not need the involvement of the top management, and for the other one, in order to achieve a successful implementation of an information security policy, there must be involvement of the top management. Suggestions for further researcher are: Future researchers interested in this field may include to conduct a qualitative research in different public organizations, also including private organizations but for a longer period of time, so the researcher can make a comparison of the top management's role in implementing an information security policy between public and private organizations. The researcher can also try to find other success factors related to the implementation of an information security.

Key words: Information security, information security policy, top management

Acknowledgements

I would first like express my gratitude to my first supervisor, May Wismén and my second supervisor Christina Keller of the Jönköping International Business School at the Jönköping University, for their great support provided from the beginning of this study to the end.

I would also like to thank the two public organizations for giving me the opportunity for the thesis project, the participants who were involved in the interviews for this study that provided their precious time during the process of interviewing.

My greatest gratitude to my husband, handsome little boys and my beloved mom for giving me more support through my years of study and during the process of researching and writing the thesis.

Table of Contents

Figures

1. Introduction

This chapter introduces the research presented in this thesis. It starts with an explanation of the research background and the problem discussion. The chapter continues with the aim of the thesis and presentation of the research questions. The last two parts contain the delimitations and definitions.

1.1 Background

According to Gordon and Loeb (2006), *"Information security relates to an array of actions designed to protect information and information systems*" (p. 16). However, information security does not protect only the information, but also the whole infrastructure that makes its use easier. It covers hardware, software, and physical security. The more the number of applications, users and systems increase, the more the management of an organization's information security gets more complex and the vulnerability increases. In order to ensure a secure use of hardware and software in organization, the security awareness program as well as support of the top management should be raised (Dhillon, 1999).

All organizations need to secure the information. For example, many organizations have extensive and frequent customer contacts, and if customer database is lost, it may be difficult or even impossible for them to run a business. At the same time this means there is violation of the rules of Personal Data Act. Another example is the innovation company that may have sensitive research results, and if unauthorized persons manage to access them, the organization may suffer substantial financial losses in terms of time, maybe several years that had been used in developing new products. Information security has been regularly considered to be a technological problem with a technological solution. That is not correct because information security involves managing risk and managing risk consist of identifying and measuring threats to information assets in the organization and taking actions to address to those threats. When organizations fail to manage their information security, the organization's integrity will be compromised and loss of money may occur (Jones,2007).

Information in various forms is the most important asset for most organizations. It is crucial that both private and public sector work systematically and need to secure the information so that it is confidential, accurate and accessible. This work concerns the entire organization, not only the management (Andersson, H., Andersson, J., Björck, Eriksson, M., Eriksson, R., Lundberg, Patrickson& Starkerud, 2011). Hone and Eloff (2002) explain that information security policies are the primary concern of an organization's information security management. The information security policy is needed by organizations in order to protect the organization's critical information assets. The information security policy explains what an employee should do and should not do as well as employees' reasonable behavior in order to secure the information. Furthermore, Peltier (2005) states that an information security policy gives management direction and support for information security. Von Solms (1999), Canavan (2003), as well as Doherty and Fulford (2005) point out that the establishment of standards are a good starting point for creating the information security policy in order to enhance information security in organizations. The information security policy should be adapted to the needs of the organization.

Most security measures introduced in a business require systematic maintenance and constant supervision. There are very few security measures that may be introduced once and for all and then serve in perpetuity. A virus protection becomes for example quickly worthless if it is not updated, and an alarm system will be unreliable if the authentication notice is not current. Therefore, it is needed one or more processes to be sure that an introduced security measure continues to function effectively. In some cases, it is in fact the actual process that are the security measure. For example, incident management is considered as a security measure that is based on a number of documented activities. With process means a set of predefined, interconnected and documented activities corresponding to an established need. A security process applies here as a process that is dedicated to managing information security. If it is possible, organizations should instead strive to integrate security measures processes that are already in business. Some businesses, however, have no well-defined processes to start from, and then it will be still necessary to design specific security processes (Andersson et al., 2011).

Processes help to create flows that are important, they facilitate to function effectively the information security work. The processes are also an important starting point to regularly review the work. Moreover, processes facilitate to grasp how things affect each other or are interdependent and how they support business requirements and goals of information security work. To describe the process is to identify what must be done, and how, while clearly communicating what is being done. A clearly defined process facilitates the work in the next step when it is time to develop policy and regulatory documents. The security measures that will be implemented affect and are affected by a number of processes in the business. The purpose of designing security processes is to identify, map and update these business processes. The goal is to identify and document the necessary security processes with the included activities and responsible persons (Andersson et al., 2011).

The activity to establish security measures includes to document the technical or administrative security measures to be introduced. Some of these security measures consist of, or are dependent on, processes that must be in place to protect business information. For designing security processes, you need to first identify what processes the business needs, and map the business processes that already exist. Possibly it will be necessary to design new processes. The work covers both the specific security processes at the operational level, partly the general processes to govern and manage information security work at strategic and tactical levels. A general process that goes from the strategic to the operational level are, for example risk management and operational process can be changed (Andersson et al., 2011).

According to Andersson et al. (2011), an information security management system (ISMS) is the part of the management system, which controls the information security business. Other parts of the system, for example, may deal with environmental issues or quality. In order for the information security work to succeed and to be successful, it is important that LIS (ISMS) has to be integrated with other forms of governance. Just as in environmental and quality area, there are established international and national standards that support the work with information security management system. In order to get a working LIS (ISMS), management must be motivated and allocate resources to work. Everyone involved must also understand that the LIS work is an investment in the short term involves considerable costs.

1.2 Problem discussion

The implementation of information security policies in organizations can be difficult when organizations do not get any support from the top management regarding the information security, or the top management do not understand the need or importance of an information security policy. There might be a lack of security awareness training and education programs. These programs are important because they contain the details of the most important elements indicated in the security policy. Without top management's commitment and support, the implementation of an information security policy will fail (Hone & Eloff, 2002; Kwok & Longley 1999). This is considered as one of the reasons that can impede the successful implementation of an information security policy.

Lack of information security policy in organization puts the organization at risk. This means that the organization has a less understanding of its most sensitive data and information. This also implies that the organization does not have a strong awareness regarding possible exposures. Such gaps unfold the organization to cyberattacks and important security issues.

1.3 Purpose

The purpose of this thesis is to investigate potential success factors related to the implementation of an information security in organizations, with a specific focus on the role of top management in implementing information security policies in organizations.

1.4 Research questions

The undertaken study is proposed to answer two research questions, which are:

1. What are the factors related to the implementation of an information security in organization according to the literature and what is the organization's view of these factors?

2. What is the role of the top management in implementing an information security policy in an organization according to the literature and what is the organization's view of the role?

1.5 Delimitations

This study is performed in Sweden, in one Region County Council and one Municipality. This means that the study only includes public organizations. The study is also limited to the implementation of the information security policy, which is only one part of the overall information security work process.

1.6 Definitions

- **Information** is an asset, like other business assets which has value to an organization and that needs to be suitably protected (Doherty & Fulford, 2005).
- **Information security** protects the information from a variety of threats, risks. It also ensures the preservation of the confidentiality, integrity and availability of an information (Knapp et al,.2006).
- **Information security policy** is a set of instructions that define what users should do and should not do, pointing out reasonable behavior in order to secure the information and information assets (Hone & Eloff, 2002).
- **Security awareness program** is a formal process of educating employees about computer security (Brodie, 2008).
- **Vulnerability** is a weakness in the organization, network that can be exploited by a threat (Whitman & Mattord, 2011).
- **Risk assessment** is the analysis of the possible hazards that could occur within a workplace and finding a solution to reduce the risk. This is avoiding injury to an individuals and damage to property (Purser, 2004).
- **Top management**: high level management (Snedaker, 2013).
- **Committed champion**: A senior executive who promotes, support the project both financially and administratively at the highest level of the organization (Siponen, 2000).
- **Confidentiality**: Data or information prevented from the exposure to unauthorized individuals is labelled as confidential (Whitman & Mattord, 2014).
- **Integrity** is the quality of being whole, uncorrupted, complete (Whitman & Mattord, 2014).
- **Availability**: Enabling authorized users to access the information without obstruction (Whitman & Mattord, 2014).
- **Encryption:** the action of changing the information by using an algorithm to make it unreadable to anyone. It can be recovered only by the persons who have the key (persons having special knowledge) (Whitman & Mattord, 2011).
- **Incident management** is an area of the IT service management that help to restore service operation to normal as fast as can be done after an incident has occurred, and reduce the negative impact on business operations (Whitman & Mattord, 2011).
- **ISMS:** An information security management system (ISMS) is a tool that helps organizations to establish, implement, operate, monitor, review, maintain and improve the desired level of information security in the organization (Andersson et al., 2011).
- **Personal Data Act:** The Personal Data Act is based on Directive 95/46/EC, which has the purpose of protecting against violation of personal integrity of personal data (Andersson et al., 2011).

1.7 Disposition of the thesis

Introduction: This chapter introduces the research presented in this thesis. It starts with an explanation of the research background and the problem discussion. The chapter continues with the purpose of the thesis and presentation of the research questions. The last two parts contain the delimitations and definitions.

Theoretical framework: This chapter provides broad concepts like information security policy, and its frameworks. It also provides an overview of policies, standards and practices. The success factors related to the implementation of an information security in organizations are explained. It ends with a summary of different theories used in this study.

Methodology: This chapter explains the research methods that were used in this study. It starts with a research philosophy, and explain in details the research approach, Interviewees and research strategy. It followed with an explanation on data collection and data analysis. Moreover, validity and reliability of the research are discussed, and some ethical considerations are underlined.

Results: This chapter provides all the data that was collected using emails interviews

Analysis: This chapter provides the analysis of the findings. This chapter reviews the results against the theoretical framework.

Conclusion is the last chapter of this thesis. It concludes the research by answering the research questions. It also comprises a section on limitations and future research work.

2. Theoretical Framework

In this section, main theories that are related to this study are explained. First, an overview of the information security policy concept is presented. This is followed by the concept model of implementation of an information security policy in organization. Next, the governance of an information security is described. This is followed by already known success factors connected to the implementation of information security.

2.1 Information security policy

Hone and Eloff (2002) explain that an information security policy helps to identify the organization's important assets, with written instructions of what an employee should, and should not do, as well as reasonable behavior in order to ensure security of information. Fung, Kwok and Longley (2003) states that an information security policy is an important tool that most organizations need in order to manage a good and effective implementation of information security. An organization which does not have an information security policy is at risk. The information security policy's primary concern is to direct the information security efforts of the company. Starting to use an information security policy helps to reduce the risk of unacceptable use of any of the organization's information resources (Fung, Kwok & Longley, 2003). The information security policy points out the management's involvement and commitment for information security in organization and describe the role it plays in achieving the organization objectives and mission (Hone & Eloff, 2002). Information security policy documents differ from organizations to organizations. A typical policy document contains (Diver, 2006):

- the purpose of policies: defines the principal goals of the policy
- scope: a statement that describe the people affected by the policy, the infrastructure and information systems to which the policy applies (anyone who is a user of information or system covered by the policy)
- establishment of role and responsibilities, how the responsibilities of policy implementation are appointed (delegated) in the organization,
- sanctions and violations, which includes how policy violation should be reported, and what sanctions should be taken in case of policy violation
- history of revisions, which defines the person responsible for making updates and revisions, and how often they need to be done.
- definitions of any terms that are not known by the reader of the policy document

2.1.1 Types of information security policies

In order to create a complete information security policy, management need to describe three types of information security policy (Swanson & Guttman ,1996).

a. Enterprise Information Security Policy (EISP)
b. Issue-specific security policies (ISSP)
c. Systems specific security policies (SysSP)

a. Enterprise Information Security Policy(EISP)

An enterprise information security policy establishes the strategic direction, scope and tone for the organization's security effort, and gives responsibilities for different areas of information security. The EISP provides guidelines for the development, implementation and management prerequisite of the information security program (Whitman & Mattord, 2014).

b. Issue -specific security policies (ISSP)

Issue specific policies gives detailed instructions, and guidance to all members of the organization in the use of a resource, for example process or technology used by the organization. Every organization's ISSP should address specific technology based systems, and need to be updated frequently (Whitman & Mattord, 2014).

c. System specific security policies (SysSP)

System specific security policies do not resemble the other types of policies. They can often be made to function as standards or procedures that can be used when configuring or maintaining systems such as configuration and operation of a network firewall (Whitman & Mattord, 2014). System specific security policies can be divided into two groups:

- Management guidance SysSP: the managerial guidance SysSP document is made by the management, and contain guidance for the implementation and configuration of technology as well as a description of reasonable behavior that people in the organization should adopt in order to support security of information (Whitman & Mattord, 2014).
- Technical specifications SysSP: the managerial policy is created together with the manager and system administrator; the system administrator may need to make another kind of policy to implement the managerial policy. For example, if the ISSP may require that user passwords are modified quarterly, systems administrator can put a technical control within a particular application to enforce this policy (Whitman & Mattord, 2014).

2.1.2 Development of information security policy

The development of information security policy is composed by a two-part project:

In the first part, the policy is designed and developed and in the second part, management processes are created in order to ensure that the policy would continually be used within the company. The policy development projects should be well planned and funded, well managed and be finished on time and within budget (Whitman & Mattord, 2014).

The policy development projects can be guided by using the SecSDLC (Security Systems Development Life Cycle) process (Whitman & Mattord, 2014).

Investigation phase: In this phase, the policy development team should:

- Obtain support from senior management(CIO). If the project gets support from the senior management, it has a better chance of success. The more top management get involved, the easier the implementation will be.
- Express the goals of the project policy well
- Gain participation of the exact individuals who are affected by the recommended policies
- The team should be composed by representatives from the legal department, human resources department and the end users.
- Obtain a capable project manager to lead the project from the beginning to the end

Analyzing phase: In this phase, the following activities should be included:

- Make a new or recent risk assessment or IT audit recording the current information security needs of the organization
- Collecting of key reference materials, as well as existing policies

Design phase: This phase should include a plan for how policies should be distributed and how verification of distribution should be achieved. Members of the organization must acknowledge that they have received and read the policy.

Implementation phase: In this phase, the policy development team writes the policies. The team have to make sure that policies are enforceable as written documents, and distributed, read, understood by those to whom it applies.

Maintenance phase: In this phase, the policy development team maintains, and change the policy as needed, to make certain that it continues to be effective. The policy should be connected to a system via which problems related to it can be reported anonymously. It also should be reviewed regularly.

The development of an information security policy document will need a high level of commitment, not just from the information security groups but also from other information security personnel in the organization. In order to ensure that the project will get enough resources, management buy-in must be founded at the start of the policy development project. Management needs to be aware of the importance of the policy development project in order to allocate the resources in the later phases (Latham, 2013).

Latham (2013) state that, in order to make sure that the organization information security policy is useful, policy documents must be developed that fit the organization culture. It is important to involve and get support from all the important players in policy development such as senior management and legal, employees, system administrators.

According to Latham (2013), it is essential to communicate the need and the importance of information security policies to those who have to live by them, in order to achieve its successful implementation. Sometimes, employees think that policies are something which is going to stand in the way of their everyday work. An important part of policy development and to make sure the policies are put into practice and not refused by employees, is to communicate the information that policies are useful. This can be done by giving a framework within which employees can work, a reference for best practices and to make sure the employees obey the legal requirements. Once employees become aware that information security policy is something that is going to help them in their daily work, they would be much more willing to the information security policy document, and to ensure compliance. Similarly, when top management are willing to accept that policy is a tool they can benefit from in order to help assure devotion to legislative requirements and to an effective management of an information security, they might be more helpful and supportive in providing funding and other resources.

Top management can also support the information security policy document, implementation and maintenance process by defending the resulting policies throughout the organization and putting efforts in implementation process. Top management should also be ready to support projects that it is caused by policy to assure compliance. This support is important to the ongoing feasibility of the policy development (Latham,2013).

2.1.3 Approaches to the implementation of Information security policy

The implementation of information security policy can be achieved in two ways: the top-down approach and bottom up approach (Whitman & Mattord, 2014). The two approaches are presented in figure 1.

The bottom up approach is initiated by administrators and technicians. In this approach, systems administrators try to enhance their systems. Systems and network administrators have substantial knowledge that can help to enhance the information security in the organization. They know the risks that can be harmful to their systems, and they know what mechanisms, and policies are needed in order to secure their systems. This approach is rarely successful due to that the planning is not coordinated by the top management, such as coordination between departments and provision of sufficient budget (Whitman & Mattord, 2014).

In the top-down approach, there is coordinated planning which comes from the top management, and a committed champion who provide funding and propose implementation process. Top management provides sufficient resources, give directions, produce policies, procedures and processes (Whitman & Mattord, 2014).

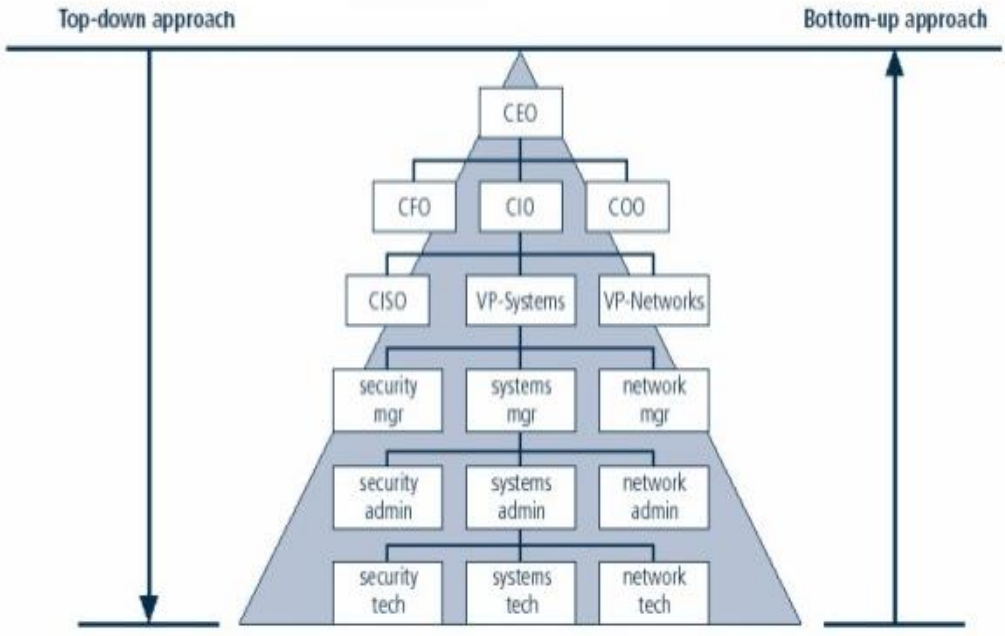

Figure 1: Top-down and Bottom-up approaches (Whitman & Mattord, 2014)

2.2 Policies, Standards and Practices

According to Peltier (2005), policies are a set of rules that prescribe acceptable and unacceptable behavior within an organization. Policies direct how technologies should be used. The information security policy is made up of high level statements connected to the protection of information across the organization, it should be created by senior management. The policy describes security roles and responsibilities, scope of information that need to be protected. They should not state exactly the proper operation of software or equipment. This kind of information should be stated in other documentation called standards, procedures, guidelines and practices. Figure 2 illustrates the relationship between policies, standards and practices.

- Standards are detailed statement of what must be done in order to comply with policies (Whitman & Mattord, 2014). The standards support and facilitates the enforcement of an information security policy. They facilitate to make certain the security consistency in the organization, the standards usually describe the security controls connected to the implementation of particular technology, hardware or software.
- Practices, procedures and guidelines specify how employees will comply with policies (Whitman & Mattord, 2014).
- Guidelines are made up of recommended controls that support standards. According to Whitman (2014), guidelines should be seen as best practices that are recommended very much. For example, a standard may require passwords to be 10 characters and a supporting guideline may outline that it is best practice to also make sure that password will expire after 30 days.
- Procedures are step by step instructions that help to implement policies, standards and guidelines. For example, a procedure may state how to install securely Windows, by providing detailed steps that needs to be followed in order to secure the OS, so that it satisfies the relevant policy, standards and guidelines.

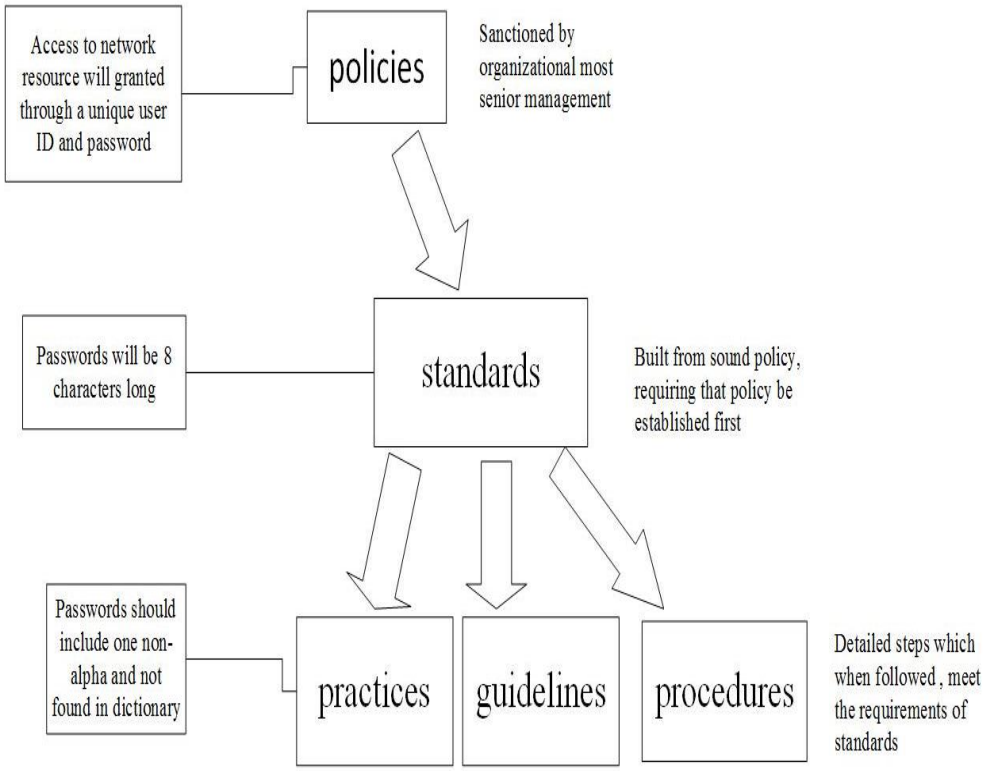

Figure 2: Policies, standards and practices (Whitman &Mattord,2014)

2.3 Governance of information security

According to Posthumus and Von Solms (2004), information security governance is defined as a series of actions on how information security can be dealt with at an executive level. The information security which involves protecting the confidentiality, integrity, and availability of organizational information, helps to reduce the different risks that can be harmful to business information by applying appropriate security controls. In order for organizations to implement a suitable set of controls and manage the information security effectively, there are various security requirements and guidelines that need to be considered. These security requirements and guidelines originate from sources both internal and external to an organization.

It is important to address both internal and external security requirements in order to suitably manage information security and prevent possible consequences of any negligence in information security. These security requirements contain requirements to secure the IT infrastructure, legal, regulatory and statutory requirements, requirements for information confidentiality, integrity and availability as recognized by the organization. These requirements together with the guidance of accepted security standards, such as BS 7799 and other best practices, create the base of an effective approach to information security (Posthumus & Von Solms, 2004).

Regarding external requirements and guidelines, the information security standards and best practices are crucial as they served to inspire global information security principles and help to develop relationships between organizations and its stakeholders. BS 7799 is an example of such a standard that gives guidance on how organizations can deal with information security, by providing information security advice based on 10 wide security control categories. The standard is considered as a starting point for organizations to start an effective information security strategy. Governments all over the world have decided to create numerous statutory and legislative requirements in order to motivate, encourage and improve corporate information security efforts. There are different kind of legal requirements that organizations are supposed to comply with. These contain different discipline specific and also country specific statutes and laws (Veiga & Eloff, 2007).

Concerning internal requirements, IT infrastructure issues connected with information security help to describe requirements in order to secure the crucial infrastructure that constitute the information backbone. Business information issues connected with information security help to define those requirements that are relevant in terms of protecting the confidentiality, integrity and availability of the sensitive business information assets. These issues are addressed by making a risk analysis which intends to identify and evaluate different risks. Next, a process of risk management is done, in which appropriate security controls are chosen and implemented with the aim to mitigate these possible risks (Veiga & Eloff, 2007).

There are two important sides to information security governance that help to achieve an effective strategy for addressing business information threat at a corporate governance level. First, there is a governance side, which includes executive management and the board. They are required to set the information security direction and strategy, controlling the information security efforts in their organization. By directing an organization's information security efforts, executive management and the board should create a corporate information security policy that demonstrate that they are committed to information security and supports the organizational mission, goals and information security strategy. In controlling an organization's information security efforts, executive management and the board must have periodic reports from different organizational department managers in order to carefully examine and review their strategies and policies so that these can be checked against rules or laws and improved if necessary. Second, there is management side which involves on how the management and the implementation of an organization security strategy will be. This includes how different department chefs and other managers are committed to the implementation of the corporate information security policy with help of conventional security codes of practices. An example of code of practice is BS 7799, which provides suitable security controls that can protect the confidentiality, integrity and availability of business information and help to integrate information security in everyday activities and functions of an organization (Von Solms, 2005).

The certification of ISO 27001 gives extra security to the existing information security system, without changing the structure of information security processes. ISO 27001 preserve the confidentiality, availability and integrity as the important principles in its standards. The application of ISO 27001 standards can be very helpful to organizations, it can facilitate to establish a rigorous framework that provides security to the organization and the information assets. The standard ISO 27001 can help to evaluate, implement and maintain an information security management system (Abu Talib et al., 2012).

In general, the implementation of a new standard cost a lot of money. But seeking ISO 27001 certification for organizations will help to reduce the money spent in IT security operations, it will also help to improve the security processes, which means the dependency on third-party services will be decreased or even removed. Furthermore, organizations can increase its benefit if its stakeholders understand the need of an information security management system.

Seeking the certification of ISO 27001 by organizations can also be very helpful because it can help the top management to improve the way it deals with information security within the organization. The standard contains controls objectives and controls that the management needs to follow in order to achieve an effective management of the information system (Abu Talib et al., 2012).

2.4 Success factors

The adoption of an information security policy can not only make an organization secure or minimize the risks of unacceptable use of any the organization's information resources. There are some factors that are required to control, guide the successful implementation of an information security (Dhillon, 1999). There are number of necessary factors that play an important role in improving an information security in organization. Those necessary factors are awareness and training, management support, budget, information security policy enforcement, and organizational mission. These factors are described in more detail below.

2.4.1 Awareness and Training

The information security in organizations can be easily achieved by increasing the awareness and giving training to all employees. The security training and awareness are the information and instructions given to all members of the organization in order to facilitate for them to accomplish their duties securely (Canavan, 2003).

According to Dhillon (1999), training is to teach users what they should or should not do, and also how they should do it. Security awareness refers to a state where all employees in an organization are aware of or involved in their security objectives and mission (Siponen, 2000). Security awareness help employees to be aware of potential threats and risks threatening the organizations information's assets, how those threats can occur, and how to handle organization's information securely.

Many organizations deal with many security issues which arise from their own employees (employees' errors). This is known as insider threat damage. The security training must be designed according to the users' needs (Al-Awadi & Renaud, 2007).

According to Whitman and Mattord (2014) training for users can be customized, depending on the functional background. This method include training for general users, training for managerial users, and training for technical users.

Training for general users: The best way to make sure that the general users read and understand the policies, is by giving training on those policies. This training permits the users to ask questions and they can also get guidance. These general users also get training on how they can perform their duties securely, for example regarding good security practice and password management.

Training for managerial users: Managers require a more personal type of training, in small groups and including more interaction and discussion.

Training for technical users: This is technical training for IT staff, which means that the training may require hiring a consultant or outside training organizations.

2.4.2 Management support

Management support plays a crucial role in successful implementation of information security (Al-Awadi & Renaud ,2007). However, in many organizations, the need for security is evoked by the IT department or the person responsible for information security.

Top management often are of the opinion that everything regarding information security is the responsibility of the IT department (Fung & Jordan,2002). This is due to that the top management often has a lack of knowledge regarding information security, and does not understand the need of information security in organization.

The top management needs to be convinced in order to understand the importance of information security in organizations, hence they will provide a sufficient budget and try to enforce the information security policy (Von Solms,1999). The management support is very important because if the top management do really understand the need of information security in organization, they will put efforts into enforcing it and employees will be more involved (Hone & Eloff ,2002).

2.4.3 Budget

The budget is also important when implementing an information security in organizations. Organizations need sufficient budget to realize an effective information security (Doherty & Fulford, 2005). According to Bjorck (2002), a budget can be defined as a financial facility that can estimate the costs and evaluate the access needed to the resources to accomplish successful implementation of information security. A budget can include technical costs and educational cost. The technical cost covers all the necessary material to ensure the computers security, for example antivirus that provide protection against viruses, online attacks; a firewall that protect the network connections. Educational cost covers all the money used to prepare the security education for the employees for example. The security education may require hiring an external expert or outside training organizations

2.4.4 Information Security Policy Enforcement

The information security policy helps to identify the organization's important assets. It also helps organizations to reach a successful performance. It is important that the policy should be straightforward, easy to understand and clear. The policy often needs to be reviewed and updated (Hone & Eloff ,2002).

According to Madigan, Petrulich and Motuk (2004), in order to enforce the policy in organizations it is necessary to make sure that all employees understand the policies, can verify if the policies are being violated**,** and have some procedural guidelines to address incidents in case of policy violation. Canavan (2003) clarifies that the information security policy can only be enforced by the method of conscious implementation. When an organization decide to implement an information security policy, employees are asked to follow the rules and are required to be aware of their rights and responsibilities (Hone & Eloff, 2002).

2.4.5 Organizational Mission

It is significant for every organization to set goals and objectives, because they will help to the successful implementation of information security (Al-Awadi & Renaud,2007). According to McKay (2003), if the organization's goals and objectives are not addressed, the organization will continue to have difficulties to protect its information and employees will not be concerned and will not follow guidelines in the information security policy.

2.5 Summary of theories and models used in this study

Figure 3 outline different theories that are used in this study and the connection between them. The theoretical framework helps to make interview questions which can be found in Appendix A. The interview questions are made before the empirical phase of data collection.

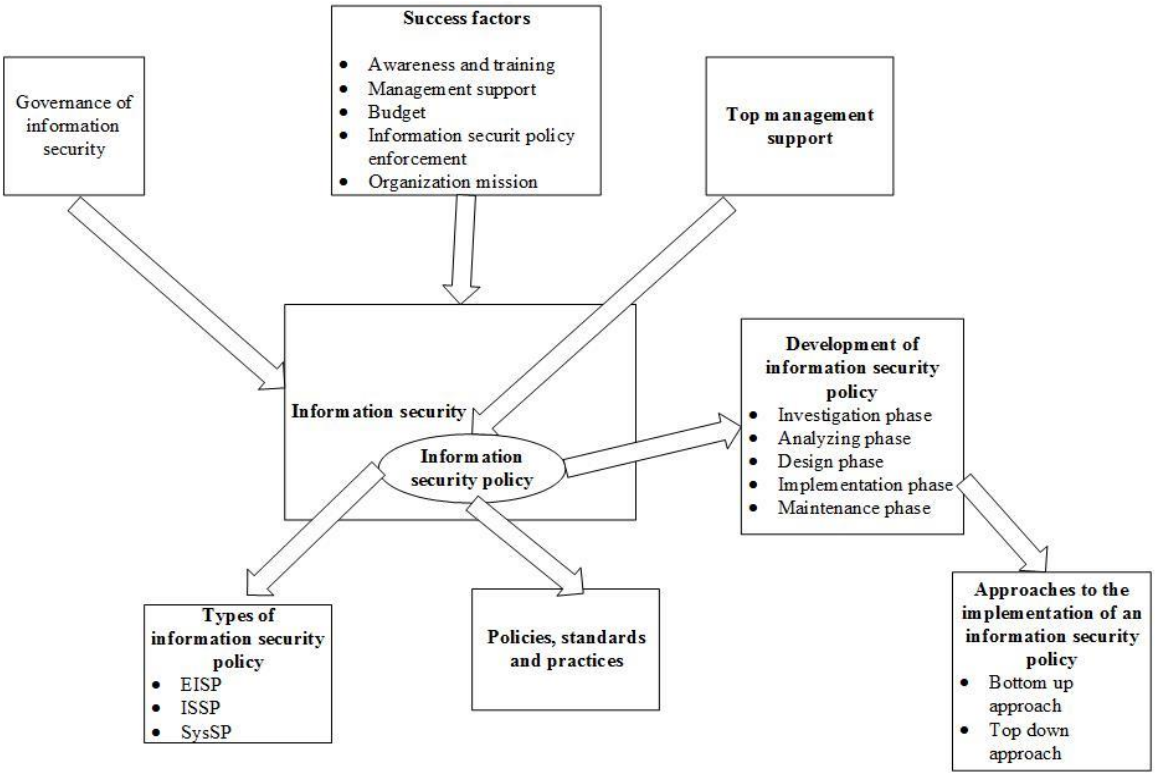

Figure 3: Summary of the theories and models used in the thesis

In order for the organization to guide a successful implementation of an information security, some specific factors like as awareness and training, management support, budget, information security policy enforcement, organizational mission must be in place (Knapp, Marshall, Kelly Rainer & Nelson Ford, 2006). Those factors help to enhance the information security within the organization. Governance of information security is needed in the organization and helps to manage effectively the information security at executive level. Organizations can effectively manage the information security by considering some security requirements and guidelines. According to Posthumus and Von Solms (2004), the top management has the responsibility of making sure that their organization comply with laws, regulations and code of practices**.** A policy is an important foundation of an effective information security program. A good and effective management of an information security can be achieved by using information security policy in organization.

The information security policies are composed by three types which are EISP, ISSP, and SysSP. The success of an information security program is based on the development of an information security policy which is performed in different phases: investigation phase, analyzing phase, design phase, implementation phase and maintenance phase. Once information security policies are developed, they need to be implemented, and this is can be done by using the bottom up or top down approaches.

Standards and practices help to enforce and support the information security policy. In this study, the focus is on top management because information security and information security policy needs support, commitment, and involvement of the top management. Top management involvement is needed when an organization wants to create an information security policy. If the organization gets more support from the top management in policy development project, this implies that the project will succeed. The implementation of an information security policy also needs support and involvement of the top management. Regarding the governance of information security, Top management is required to establish the information security direction and strategy. By achieving that top management should produce a corporate information security policy that shows that top management is committed to information security and supports the organizational goals and information security strategy (Posthumus and Von Solms, 2004).

3. Methodology

3.1 Research philosophy

Chua (1986), Myers (1997), Orlikowski and Baroudi (1991), classify the research epistemologies into three types: interpretive, positivist and critical. According to Myers (1997), the qualitative research can be interpretive, positivist and critical. In interpretive research people make and associate their own subjective and intersubjective meanings about the world they live in, and the researchers try to comprehend the phenomena while investigating them from the viewpoint of the people that are related with these phenomena (Orlikowski & Baroudi ,1991).

Klein and Myers (1999) emphasize that interpretive research is important in the field of information systems research, as it facilitates to investigate and comprehend how people think and behave in social and organizational contexts. According to Walsham (1993) as well as Klein and Myers (1999), interpretive research in the information systems field pinpoints the understanding of the context of the information system and the ways information system influences and is affected by the context. The information system research is considered as interpretive if it is founded on the fact that understanding of reality is gained through social constructions such as language, consciousness, shared meanings, documents and other artifacts. (Klein & Myers, 1999).

The philosophical worldview behind this interpretive study relies on the investigation of the participant's social context and the relations between the social structure and the reality of the employees. The investigation between people, their social environment and the other external factors that affect their everyday life help to understand human behavior. The aim is to achieve a better understanding of top management's role in implementing an information security policy in organizations by interviewing employees in those organizations.

This thesis adopts an interpretivist worldview, because I believe it will help me to answer the questions posed and to examine and understand the interviewees' thoughts in their organizational context. This will help me to understand what happened in the organizations, how employees think about the implementation of an information security policy in organization, and the role that top managers play when implementing information security policy in the organization.

3.2 Research approach

The case study is one of several strategies that can be used in social science research. Other strategies are experiments, surveys, histories and the analysis of archival information. Each strategy present advantages and disadvantages depending on three conditions which are the type of research question posed; the extent of control an investigator has over actual behavior events; and the focus on contemporary as opposed to historical phenomena. (Yin, 2003).

This research uses a case study approach which facilitates to investigate and identify potential success factors that are connected to the implementation of information security with specific focus on the role of the top management in implementing an information security policy in organization. There are different ways of collecting data in case study: surveys, interviews, documentation review, observation and collection of physical artifacts. According to Yin (2014, p. 43), *"a case study is an empirical inquiry that investigates a contemporary phenomenon in depth and within real world context, especially when the boundaries between phenomenon and context may not be clearly evident."*

The research is conducted in two public organizations, by making emails interviews with employees in order to find qualitative results. A document analysis is done; this helps to examine existing documents. I also did a visit in the field.

3.3 Research Setting

The research setting for this research is two public organizations: one Municipality and one Region County Council. The Municipality is governed by politicians, who decide for various activities in the municipal council and committees. IT has different divisions to govern their activities. Those divisions are:

City council: it is considered as the municipality's highest decision making body, the parliament. Political parties(members) that will be represented in the city council are elected every four years.

Municipal: The Municipal government is the Municipality's government and is responsible for the Municipal administration and supervise other committees and boards' activities. All suggestions and opinions from other committees and boards are handled in municipal government before they are presented to the city council.

Administrations and Boards: the administrative manager's is responsible for the administration's work.

The Region County Council has two main missions: Public health, medical and dental care Regional development and growth. The Region is responsible for the county's residents; it ensures that they have access to equitable and dental care of high quality, public transport is working well, organize cultural activities. The members that will be in the Region County Council are elected every four years, they are given the authority to pursue regional development work and coordinate development efforts in areas such as infrastructure, industry and labor market. The region development project is about bringing together agencies such as universities and professional organizations, in a regional development strategy, organize work, create communities and networks, and assume responsibility for monitoring work development.

The political parties in the Region, that are democratically elected, are those that decides how the tax money should be distributed in the Region and gives the overall direction for the business. After that, the Director of the Region and the other top managers must execute this decision.

3.4 Research strategy

A qualitative methodology was used and semi structured interviews were conducted in the study (Creswell, 2009). An interview guide was developed containing open questions. The interview questions were based on theoretical framework about information security and information security policy presented in chapter 2. The interview guide is presented in Appendix 1.

I organized a meeting with the interviewees in order to explain the theoretical framework and I also sent a short explanation of the theories by email. Accordingly, those explanations would enhance their possibility if giving adequate answers. The next step was to send the interview questions to the security coordinator, the employees from other departments of the Municipality, and to the information security manager of the Region County Council to gather the empirical data.

3.5 Data collection

Secondary and primary data sources have been used for the data collection.

3.5.1 Literature review (secondary data source)

A review of previous research is necessary in any academic study. It helps to establish a solid background for advancing knowledge. It helps theory development, and identifies areas where a large amount of research exists and where research is needed (Webster &Watson, 2002).

According to my research questions, a literature reviews about potential success factors related to the implementation of an information security and the role of top management in implementing an information security policy was performed. In order to collect information connected to the topic, I used Jönköping University database Primo, journal databases of Emerald and ACM, Wolverhampton database summon, with three keywords: information security policy, success factors connected to the implementation of an information security in organization, policies, standards and practices. The literature types were books, journals, articles, conference proceedings, white papers. The literature review identified the theoretical framework used in the data collection and data analysis.

3.5.2 Interviews (primary data source)

There are different methods that can be used for the collection of data in a qualitative research, for example interviews, observation and letters, reports, newspapers articles can be utilized as sources in a written form (Myers ,1997).

Semi structured interviews were used in this study. I chose to perform email interviews because the interviewees told me that they are more comfortable in writing than speaking English. The

disadvantage of making emails interviews, is that the answers are not deep. For the Municipality, I first sent questions to the security coordinator who works in IT department, also questions were sent to other employees of the other departments, but I got answers from one employee of the other department and the security coordinator. In the Region County Council, I sent questions to the administrative manager.

This section outlines the advantages and disadvantages of using emails interviews.

Advantages:

- Emails interviews compared to interviews face to face do not need travel, or require to dress up. They can include different participants from different locations. Participants can answer the emails interviews at any time that is appropriate for them. The researcher does not need to find a time when participant is ready and available for the interview (Burns,2010). The emails interviews do not require any cost; they facilitate to ask more details or explanation for prior comments.
- Email interviews provide the interviewee time to create an answer to a particular question. The interviewee has a time to think and reflect before writing the answers.
- Emails interviews also give participants more time to consider and think about their answers, and they can also review their answers before sending them, this facilitate them to be engaged in careful communication (Burns,2010)
- Emails interviews give participants flexibility when they answer to questions, participants do need to respond to questions immediately as in face to face interview (James & Busher, 2006).
- The emails interviews are easy to transcribe, copy and paste.
- Email interviews facilitate the researcher to interview multiple participants at the same time.

Disadvantages

- The emails interviews do not provide body language and other contextual signals for the interview.
- Missing nonverbal cues may cause complications on the social aspect of communication and may bring about emotional misunderstanding without difficulty (Reid, Petocz & Gordon, 2008).
- Lack the spontaneity and richness (Reid, Petocz & Gordon, 2008).
- Emails interviews could extend over months, with gaps between questions and responses
- The gaps between responses create discontinuous responses, for example a participant can forget what had been said before (previous thoughts), it can also be hard for participant to get clarification of meaning of questions (interpret email questions) (James & Busher,2006)
- Providing the email questions one at a time may bring on: loss of coherence and flow of thought (James & Busher,2006).
- Distractions and disturbances of every/day life may bring on: unfocused responses, loss of threads of what the email interview was talking about and getting more from face-to-face interviews, quick answers (James & Busher, 2006)

As I performed email interviews, I did not need to travel to the locations of the interviewees. As a result, the interviews did not require any travel costs. The interviewees could choose to respond to the questions at any time and place that were suitable to them. When participants sent me answers that I could not understand, I could ask them afterwards to give me more details or explanations of prior comments.

The email interviews facilitated for me to interview multiple participants at the same time. They

also were easy to transcribe. At the same time, there was a lack of richness in the answers I got from the participants. It also was not easy for participants to get clarification of meaning of questions, is the reason why I sent them a short explanation of the theories by email. Those explanations would improve their possibility if giving suitable answers.

3.5.3 Interviewees

The interviewees were categorized into two groups: In Municipality, the first group was employees of IT department. Interviews was conducted with Information security coordinator. He was among those who leads the work of IT by proposing and creating the strategy of the work of IT department, and participated in the creation and enforcement of information security policies. Furthermore, he made decision on how information security awareness and training can be carried out, what platforms can be used within the organization, he organized the overall work of IT, and on new software and hardware.

A second group of interviewees were employees who work in other departments. The interview was conducted with a responsible of social administration, who worked in the Education Department. He used computer during his day at work, was interested about security of information. Sometimes, he got in contacts with IT service desk and asked them questions and got answers from them.

The interviews were also conducted with a local security coordinator, who also worked with ensuring security of information. As long as the responsible of social administration and local and safety coordinator were preoccupied with information security, their responsibility was to attend the security training and awareness program, following the rules and guidelines which were in information security policy document.

An interview was also conducted with the information security manager of Region County Council. She belonged to the top-level managers of the Region County Council. She was involved in information security policies creation, in implementation and enforcement of information security policies. She also decided on how security education should be performed and awareness should be created.

These interviewees had different job positions and different backgrounds. The purpose was to get different point of views and thoughts from different employees.

3.6 Data analysis

The written interview material was analyzed by comparing the findings with the different theories and models presented in the study. Those theories that have been used in this study are connected to each other. The focus is on top management because a good and effective implementation of information security policy needs support, involvement of the top management, and successful management of information security can be done by using an information security policy in organization. How to analyze the data relates to which type of the research that is performed (Baxter & Jack,2008).

3.7 Construct Validity

According to Yin (2003), the problem of construct validity can be addressed because multiple sources of evidence provide multiple measures of the same phenomenon. Two sources of evidence, interviews and documents analysis are used to identify the role that plays top management in implementing an information security policy in organization and how organizations' views about that. According to Yin (2003), in a case study, the use of documents helps to corroborate and increase evidence from other sources.

3.8 Reliability

According to Yin (2003) reliability involves demonstrating that all procedures for example data collection procedures can be replicated with the same results. The description of all procedures that have been used in this study from the research approach to the data collection procedures is given.

3.9 Ethical consideration

In order to validate ethically this research, there are some components that have been considered (Callahan & Hobbs, 1998).

- Disclosure: interviewees have been told about the aim of this research, and the procedures that have been used. I have read a document that defines procedures in place in order to protect the confidentiality and anonymity of the interviewees**.** The statement describes clearly the person to communicate with questions about the research and the rights of the interviewees.
- Understanding: make certain that all interviewees understand all the information that have been given to them and they could also ask questions
- Voluntariness: to participate in the research has been voluntary
- Consent: interviewees have all agreed to participate in interviews and visit in the field.

4. Results

4.1 Results for Municipality

The study has found that the municipality has an information security policy**,** and it helps the organisation to the successful management of information security. The Municipality agrees that the information security policy is an important tool that organizations should have with the purpose of managing a good implementation of an information security.

One of the interviewee stated: *"In the public sector we handle a great deal of delicate information about citizens whom we must guarantee a safe handling*".

The information security policy is deployed during an awareness session and is explained to the top management and chiefs of every section. After the session, every chief of each section has the responsibility to communicate and disseminate all the information concerning the information security policy to the end users within each section.

The municipality uses one type of information security policy, that helps to protect the information in general. One interviewee explained: "*We have only one information security policy covering information in general. No matter what form of information, we advocate the same protection level.*"

The information security policy document of the municipality is understandable, means that the employees can understand the content of the policy. One of the interviewees explained that "*The information security policy of our organization is written to be understood by everyone in order to follow the meaning of the policy*. It is also placed on a very easy available place on the net, internal (the intranet) as well as external (website).

The person responsible of creating the information security policy is the security manager with support from the IT department. The Municipality uses the standards of ISO 27001 and ISO 27002 as guidance in their work. The organization gives a lot of importance to information security policy by starting from the top management and reaching to the end users. One of the interviewee stated that: "*The top management in our organization understands the need, the importance of having information security policy, they approve and apply the ongoing process of its implementation."*

The top management's perception regarding the implementation of an information security is that: "*It is a process that takes time to implement in such a big workplace",* commented one of the interviewee. Thus, the top management of the municipality understands the need of an information security.

The information security policy is the principal of the documents that were aimed to the organization. The organizations should have a structure and procedures on which policies should exist and how these are developed, organization should take this into account. What one chooses to call policy? For example, operational policy (which probably also includes other than security related to information), security policy (which deal with security issues), or information security policy is up to each organization. The important thing is that management should show its intentions regarding the information security. The methodological support provided by the Swedish Civil Contingencies Agency deal only with information security and there are also some recommendations for what should be included in information security policy (Andersson et al., 2011).

The policy should not contain some concrete rules of conduct without expressing management' intentions and thus frame the other governing documents. A policy should be brief and accessible to all. More information and explanations can be presented on the internal web for example. The policy expresses management's overall intentions. When it comes to information security policy can be called information security policy or security policy if it applies to all security work. The policy should be developed at an early stage, before or at the same time as the activities determine the safety and designing security processes. It is important to identify all existing policy documents to know what material you have to work from. This gives an idea of the work required to prepare the regulatory documents required and to bring order among policy documents. The working group can then update and write policy documents in the order that fits the information security needs of the organization, general way is to first regulate the protection of the most sensitive information in the areas where the risks are greatest (Andersson et al., 2011).

An information security policy should contain:

- Management's intentions, why it is important to have information security.
- Short description of how these intentions will be achieved
- Short description of responsibilities) within information security
- An explanation of important concepts
- a statement of who is responsible for the policy and how it is reviewed and revised

The management should actively be involved in creating policy. It is after all, the management who sends the message and it is important that it feels responsible for the policy. In practice, however the person responsible of information security or LIS group leaders who are responsible for policy development. Although the management owns the document, experts in information security should create the information security policy so that it suits with the intentions in information security work. Once the policy is complete, the organization should organize security education and dissemination of knowledge in order to inform all employees about policy and how important it is for the organization.

Those who should design policies and above all the other governing documents must know the process to develop and establish the regulatory documents in organization. Most organizations have some sort of formalized process with such a defined policy document hierarchy, internal preparations and referrals and established templates for how policy documents should look like. The organization's legal expertise should be involved in developing papers. Examples of information security policies are found in the methodological support documents (Andersson et al., 2011).

The organizations need to protect the organization's information in a way that suits their business. It is necessary for them to achieve business objectives and to customers, clients, partners, the public and employees to feel confidence in them. Therefore, they work actively with information so that all their information should always be confidential, accurate and accessible. They have chosen a common and structured way of working with information that is based on the Swedish and international standard (LIS management information security). With the support of LIS, the organizations get the right level of information security while their employees receive support in their daily working.

Work on information security should be long term and continuously, covering all aspects of their business and all of the information assets they own or manage. Staff should receive continuous training to understand how information security works.

Everyone has a responsibility for the security function. Whoever discovers deficiencies in information security, must pay attention to their manager or security feature on it. All employees must also report events that may cause our information assets are exposed to risks.

Responsibility for information security is operational responsibility.

Definitions (based on definitions taken from "Terminology Information, SIS HB550 Issue 3, SIS publishing):

• Information Assets are anything that contains information and carrying information.

• Information security is the security in respect of information concerning assets, the ability to maintain the required confidentiality, integrity and availability.

• Confidential information may not be accessed by or disclosed to any unauthorized person.

In most cases the content of an information access but sometimes also asset existence secret.

• Accurate information means that the information cannot be changed without authorization;

not by mistake and not because of a malfunction.

• Available information allows information to be utilized by authorized users when needed and as much as necessary.

• An information security management system (ISMS) is a tool that helps organizations to establish, implement, operate, monitor, review, maintain and improve the desired level of information security in the organization.

Each year, the head of security review and possibly revise the information security policy. To comply with the regulations and guidelines on the right way you can have a guide. Guides can also be written in areas where there is no regulations or guidelines. Procedure descriptions and instructions indicating how the work should be carried out in detail. Such procedures may, for example, specify how and when to make backups or how to monitor and manage event logs (Andersson, et al., 2011).

4.2 Results for Region County Council

Also the Region County Council had an information security policy. It is very critical for the organization to have an information security policy with the purpose to manage a good implementation of information security. One of the interviewees commented: *"It is very important with the policy; the organization needs to know the strategic direction"*.

The Region County Council also think that the information security policy is an important tool that the organization should have with the purpose of managing a good implementation of an information security, one of the interviewees commented:

"Yes, it is important tool. It shows the organizations desired intensions, strategic. It should be valid for the whole organizations and therefore it must be quite overall, not detailed. More specific instructions, guidelines are the next level and they are more directed to different parts of the organization. Then further detailed instructions for different working tasks are described in routine descriptions. It is important that these different levels of descriptions (policy-guidelines-routine descriptions) are not contradictory. The information security policy should be written in a way that it is valid for several years. Guidelines can be revised more often and routine description even more often."

The information security policy will be revised soon, guidelines and rules will be revised after the policy. In the Region County Council, an information security policy is created by one of the top managers who is an information security manager for the whole organization, with support of other three information security specialists and one jurist consult. They create a first draft and the information security responsible present the draft to the Director of the Region. The draft needs to be approved by the Director before it is presented to the political organization that makes the final decision.

The top management of the Region County Council understands and gives high importance to the information security policy and information security. Top management is responsible for the information security policy work, assess the policy draft and approve it. It is also involved in the implementation and maintenance of the information security policy. A top down approach is used in the Region County Council in the implementation of the information security policy.

One of the interviewee commented: "*It is important that the policy implementation is managed from the top. All professions in the operative organization want to do their best and sometimes there is a risk that information security will be overlooked. Therefore, steering mechanisms is needed as help for the employees to do things in the right way. There are also often good ideas innovations, coming up from personnel at different levels. There must be regulations from the management that says what can be done and what not can be done. Except the policy, that are so overall, specific program management groups are created for infrastructure and eHealth*

services. In these groups, top management is represented and when they look at new ideas they keep an eye at information security and strategic issues".

The Region county council has one type of information security policy and some guidelines. One of the interviewees stated: "*Guidelines are more detailed and subject-specific. For example, there is guideline for procurement of new IT systems. In the future, maybe there can be even more overall security policy, i.e. maybe cover all security, not just information (but that are not the plan right now)*". Its information security policy document is easy to understand, which is one of the goals of the policy work. One interviewee stated: "*we try to make our policies understandable*".

The Region County Council runs a policy development project and they use a PDSA wheel. It is a continuous quality improvement model (concept) formed by a systematic series of steps for acquiring valuable knowledge and learning for continuous improvement of a product or process. The PDSA wheel starts with the Plan step: This step consists of identifying a goal or purpose, planning a theory describing success metrics and putting a plan into action. This is followed by the Do step: This step consists of implementing all elements of the plan. Next comes the Study step, where the results are checked to test the validity of the plan for signs of advancement and success, or problems and areas that need to be improved. The last step is Act, it consists of integrating the learning created by the whole process, which can be used to modify the goal, modify methods or even reformulate a theory altogether. These four steps are repeated over and over, the cycle is never ended, it is a continuous improvement model. (Deming institute,2016)

One interviewee stated: "*When we have projects we used the PDSA wheel. It has four phases and the whole organization is comfortable with this development model."*

This study also has found that during the policy development project, different activities are scheduled, the information security manager with support of other three information security specialists and the Jurist will review and evaluate the old information security policy document that they have right now. They will see what parts they can reuse and what parts that must be updated. They will also in this phase, look through other related documents like strategic plans and existing guidelines. Then a draft of a new policy will be written. If needed ideas and suggestions can be tested in the operational workplaces via some selected IT contact persons. Then the approval process will begin (first the Director of the Region and then the politicians). There can be some adjustments that must be handled before the final approval by the politicians.

When the policy is approved, the next phase is to make a communication plan for the policy – how the IT contact persons shall be informed and educated and how the policy can be spread in other channels. For example, they can use different meetings that continually are arranged (like groups for physician managers, unit managers, and management teams for different units in the Region). When the policy is approved the guidelines also must be revised and after the guidelines working routines should be adjusted, but the working routines is mainly handled at clinic or department level because they are detailed descriptions for the daily work. In the work with the guidelines different other specialists must be involved. For example, when the guidelines are about employment issues, HR department is involved and for guidelines concerning the electronic medical record system, specialists on that must be involved. The maintenance phase after implementation is more about further revisions of guidelines if needed. Of course, the policy also must be reviewed, but the ambition is that it should not need to be updated in a couple of years.

A new specific risk assessment is not planned for the information security policy work, but risk assessments is continually done in the organization. Problems with information security is in the organization are reported in the same way as other problems. They have a specific electronic system for that and in the system, problems are grouped by subject. Information regarding different kind of problems is collected and there are persons in charge for the evaluation of all reported problems. In cases when patients have been injured in the health care process (independent reason) there is a national self-reporting system called Lex Maria and all cases that are reported there will be thoroughly examined. Top management is involved in these cases. Several standards are used in the Region, such as ISO 27001 series and SWEDAC.

One of the interviewee stated: "*The information security in Region County has a near collaboration with a neighbor Region and they exchange experiences and valuable*

information. The Region also has dialogue with the County Administrative Board, that have a more overall responsibility for the security for the citizens, like preparedness for different crisis in the society. They also working with the same standard and with management system for security"

Regarding the role of the top management when implementing an information security policy in organization, one interviewee commented: "*The role of the top management is to confirm and sign information security policy"* and also added: "*The purpose of information security policy is to secure the organization's information."*

"Good Information security is seen as a basic condition for the organization. Information security should be a natural part of all work and the policy that describe the organizations intensions is a base for that". Added one of the interviewee

The employees in the Region county council follow the security guidelines, the interviewee stated: "*Yes, we follow the guidelines, but it is hard to remember them all."*

The Region educate and makes aware its employees of security of information by using different channels: through the organization-net, and classroom education. The organization will create a new website where employees can read the information regarding the information security and information security policy. This study has found that, in 2015 information security was an important issue in the county council. A few years before 2015, The information security manager for the whole organization made some changes in information security in organization. Before the information security in Region County Council was decentralized. Each department had its own information security responsible (Health care, public transport, culture, regional growth and infrastructure).

The organization decides to centralize the information security responsibility and overall work, Now the information security management is very naturally a part of the top management in the Region. Now there are more changes ongoing and instead of having several information security administrators that working part time, the Region County Council is recruiting three full time information security specialists. These are going to work close to the information security manager for the whole organization. There is also one jurist, called "personuppgiftsombud" in Swedish, every Region/County Council should have jurist. The role of the jurist is to ensure that all personal data is handled in a proper and in legal way and do internal revisions.

Thus, the information security responsibility is on this top management level in the Region. There is also one person responsible for the IT security and he is working at the IT department, but is connected to the information security manager and the other information security persons in a working group. The information security is a very important area for the Region and the top management is very aware of that. The highest managers in the Region (Director of the Region) are supporting the information security. The overall responsibility for information security is always on the top management, they cannot delegate that to someone else.

In the different parts of the organization (like the different health care clinics, development departments, administration departments and so on) there are one or several (depending on the size of the departments/clinics) IT contact persons appointed. These are often administrators that get special education and training for IT related issues that must be handled. They are also a kind of bridge between the end users and IT support i.e. they can do a first assessment of IT problems, sometimes they can solve the problem, but if not they can direct to the right instance.

Information security is a strategic issue for the Region. The citizens in the region assumes that the organization can handle information that often is confidential in a proper way. For example, today, quite many patients that have been using health care service read their medical records and critical reviews information (log files) about who have opened the records. Therefore, it is very important that all personnel knew what they are allowed to do and not to do. Citizens also assume that the Region is updated with new technical innovations and can secure information that is transferred in for example mobile apps.

Regarding the success factors connected to the implementation of an information security, the interviewees for both the Municipality and the Region County Council all agreed with the success factors find in the literature.

Management support

The Municipality and the Region County Council all agree that a good implementation of an information security needs management support. Their Management know and understand the importance of protecting the information to the survival of the organization. The organizations need to preserve the confidentiality, integrity and availability of the information. According to Von solms (2003) Ensuring confidentiality involves protecting sensitive information to unauthorized people (users who don't have access). In order to maintain the confidentiality of information assets they need to be kept secret. Sensitive information should not be left accessible to anyone who wish to gain access to it (Posthumus & Von Solms,2004).

Thompson and Von Solms (2003) state that the confidentiality of information may be maintained by using two approaches. These contain limiting access to confidential information or encrypting sensitive information.

Integrity of the information involves protect the accuracy and comprehensiveness of the information (Von Solms, 2003). There is a mechanism that is used to preserve the integrity of the information, is to attach a simple message digest to a message before transmission so that this identifier can be used to calculate if the message sent has been changed (Thompson & Von Solms, 2003). Availability of the information involves ensuring that authorized users have access to the information. The effectiveness of an information security needs the involvement and buy in from the management.

Security awareness and training

The Municipality and the Region County Council all agree that Security awareness and education is important in implementing an information security in organization. They make aware and educate their employees about information security and information security policy during the security sessions. "*It is important to continuously inform and educate employees about information security"*, Commented one interviewee of the Region County Council. The Municipality's and Region's information security is effective, because their employees have given all the necessary information to protect the organization resources.

The Region County Council use different methods to disseminate that information in the organization: through the organization-net, and classroom education

"*When an organization do not organize the security awareness and education, it is exposed to attacks against organizational information resources* "commented one interviewee of the Region County Council. In Region County Council, the first information/education about information security to employees is performed in the introduction program. All new employees must participate in such a program.

Budget

The Municipality and the Region County Council all agree that budget also plays an important role when implementing an information security policy. Those two organizations plan for information security accordingly to the budget. These organizations get a proper budget in order to ensure an information security in organizations. They get the money to buy new software, consultants, hardware.

Information security policy enforcement

The Municipality and the Region County Council all agree that the information security policy is one of the most critical controls needed by organizations to realize a good implementation and effectiveness of an information security. The content of policy documents for the Municipality and the Region County Council is understood by their employees. Those two organizations ensure that their employees understand the content, by organizing the security awareness and training sessions. These security sessions help the Municipality and the Region County Council to achieve an effective enforcement of an information security policy.

Organization mission

The Municipality and the Region County Council all agree that the organization's goals and objectives are critical in implementing an information security. The Municipality's and Region's mission is to achieve a good implementation of an information security; they could achieve that because they understand the need of information security in their organizations.

One of the interviewee in the Region County Council commented*: "There is overall objectives and goals, but also more specific that are different at different units. The organization is consisted of so many areas, like health care in one hand and culture and public transportation in the other hand. There must be adjusted goals at different levels. But all units have and handle information that must be secured. The aim is that the top management built and secure a structure for information security that then can be adjusted to the specific requirements in guidelines and routine descriptions. Also, education and training must be adjusted to the specific areas. A good structure should make it easy for the personnel in the organization to work in the right way*"

5. Analysis

In this phase, I have analyzed the data by searching for similar patterns in the interviews. The headings in this section represents the most important keywords obtained from the interviews.

5.1 Information security policy

According to Whitman and Mattord (2014), for the purpose of making a complete information security policy, management have to define three types of information security policy which are enterprise information security policies, issue specific security policies and systems specific security policies. The analysis of the interviews, shows that the Municipality uses only one type of information security policy which covers all information without exception, whether if the information is handled in cyberspace, in computers, in a phone call or on paper. It is the same for the Region County Council.

Also, according to Whitman and Mattord (2014), the development of a policy project has two parts. In the first part, the policy is developed and created and in the second part management processes are created in order to perpetuate the policy within the organization. According to the interviews, the municipality does not have a policy development project. Instead, the information security policy is made by the security manager with support of the IT department. The IT department's task is to make sure that the organization has an information security policy, and that employees read and understand the content of the information security policy.

The Region County Council has a policy development project. This project is organized by one of the top managers with support of other information security specialists and one jurist consult. As previously mentioned, the top manager who organize the project is the information security responsible for the whole organization.

During the project, different activities will be scheduled and the whole project will have a time limit. The information security responsible gives a structure for the work. She also appoints the project members (the information security specialists and the jurist) and then they organize the work. When the policy is approved, the specialists will continue to work with implementation, together with the information security responsible, they create a communication plan and plan the education of other employees.

As stated by Whitman and Mattord (2014), the implementation of an information security policy can be done by using two types of approaches: a top-down approach and a bottom up approach. From the interviews, it is evident that the municipality uses the bottom up approach to implement the information security policy. The security manager has the professional role and knowledge about how to improve the information security in the organization and thus he creates the policy. On the contrary, the Region County council use the top down approach to implement the information security policy, as everything is coordinated by top managers, such as planning, implementation process, and the policy creation. According to the interviews, the employees take the information security policy seriously, because they see that top managers are concerned.

5.2 Success factors

Management support

According to Barman (2002), top management involvement in the creation of information security policies shows that top management supports the security program. He also emphasizes that top management support is always important, because employees will take policies more seriously. For that reason, without support of upper management, security programs are certain to fail before even the writing of the policy is finished. In the municipality, the information

security policy was created by the security manager with support of the IT department. The top management did not participate in the creation of information security policy.

The Region County Council agreed that management support is crucial in creation of information security policy. In the Region County council, top management was involved in creation of information security policy, with help from three information security specialists.

Security awareness and training

Peltier (2005) states that security awareness and training are crucial to the implementation of effective information security. From the interviews, it was clear that the municipality agreed that security awareness and training are important for the successful implementation of information security. The organization often organize security awareness and training session where the top management and chiefs of every section are invited and get information regarding information security, information security policy, guidelines. In their turn, they have the responsibility to forward the knowledge obtained from the security session to the employees of each section.

The Region County Council also agreed that security awareness and training are important to a successful implementation of information security. After their information security policy is developed and created, this is followed by creation of communication and education plan of other employees. This communication and education plan will help to make aware and educate employees about the information security policy.

Budget

When organizations plan for information security, they need enough budget to realize the implementation of information security. Thus, having a budget is a crucial aspect to the implementation of information security (Dinnie,1999). The interviewees agreed on the importance of budget in organizations, when they want to reach an effective information security. The level of protection they have in their organization depend on the money they can provide for it (Dinnie, 1999). The municipality gets a proper budget to the implementation of the information security. They handle a lot of sensitive information, that needs to be well protected.

The Region County Council agreed that budget is important for an effective implementation of information security. According to the interviews, the Region County Council gets enough budget for their policy development project, the implementation of an information security and information security policy.

Information security policy enforcement

Jon (2002) explains that if organizations want to realize an effective enforcement of a security policy, they have to make sure that the end users understand the content of policy documents, often verify if the policies are not violated and describe some procedural guidelines to address incidents of policy violation. The best way to know if the policies are understood by end users is by organizing security awareness (Madigan et al., 2004). The information security policy document of the municipality is understood by the end users. During the security session, the chiefs of every section explain the policy to the employees and employees can ask questions regarding those policies.

The information security policy document of the Region County Council is understood by its employees. It is also during the communication and education session, where the employees get information about policy and an opportunity to ask questions. Those security session or communication and education session also help to know if end users understand the content of information security policy document, and all information regarding information security. Information about both policy and guidelines is also published on the intranet.

Organizational objectives and goals

Sometimes organizations do not pay attention on information security, until something goes wrong, but when a data breach happens, they suddenly pay attention and a lot of effort is needed in order to recover from the situation. (Siponen,2000). This happen because organizations do not understand the need of an information security and when they do not understand that need, they cannot set objectives and goals.

Siponen (2000) explains that organizations need to set goals and objectives in order to make a successful implementation of information security. For the municipality, they know what they want to achieve, define what they want to reach by establishing goals and objectives. This is the same for the Region County Council, they know what they want to do, what they want to accomplish in order to make better their information security. For those two organizations, they understand the need of information security, they handle a lot of sensitive information that needs to be secured. Their objectives and goals are to ensure an effective implementation of an information security and information security policy in their organizations. They plan for their information security, by organizing the security awareness and training, in order to give information regarding information security and information security policy to all their employees.

6. Conclusion

This thesis has dealt with success factors related to the implementation of an information security in organization with focus on top management's role in implementing an information security policy in organizations. It was accomplished as a case study in two public organizations. In this chapter, I aim to answer the research questions, which are:

RQ1. What are the success factors related to the implementation of an information security in organization according to the literature and what is organization's view of these factors?

Those success factors are management support, security awareness and training, budget, information security policy enforcement, organization objectives and goals.

In the organizations where I have conducted the interviews all agree with those success factors found in the literature and they also add that those success factors are very important in a successful implementation of an information security.

RQ2.What is the role of the top management in implementing an information security policy in organization according to the literature and what is organization's view of the role?

The role that top management plays in implementing an information security policy within the organization is to be involved in the creation of information security policy, in the process of its implementation, and providing sufficient financial resources. This means, for example, funding that can be used to educate employees about information security policy, or to buy computer systems in which all problems connected to information security policy can be reported. Funding is also needed to implement a standard. A good and effective implementation of an information security policy needs a sufficient budget.

The organization's view of that role is different for the two studied organizations. For the municipality, there is no involvement of top management in creation of information security policy, in process of its implementation. Top management approve the process of information security policy implementation. For the Municipality, the successful implementation of an information security policy does not need the involvement of top management.

In the Region County council, there is an active involvement of top management in the information security policy creation, as well as in process of its implementation. As a result, involvement of top management is needed for a successful policy implementation.

7. Limitations and suggestions for future research

This study is focused on to management's role in implementing an information security policy in organizations. It depends on having access to people to interview such as high level managers, employees from different department in organizations such as public and private organizations, even international organization, but the access was limited for some organizations, even denied for others, because some of high level managers do not know their role when it comes of implementing an information security policy in organizations, means that they do not understand the role of having an information security and information security policy in their organization; for others they know about the information security policy but they are not involved in creating the policy. The case where the access was denied, is for those who did not want to give their information regarding the information security or information security policy because of the sensitivity of the information. This is why this study did have a high number of interviewees and did focus only on two kind of public organizations. It did not talk about international businesses.

A limitation of this study is that organizations do not reveal much information of this topic because of the sensitivity of the information**.**

Yin (2003) states that there are three elements that are required when constructing validity. Concerning the sources of evidence, this study was lacking a questionnaire in the data collection. This lack of questionnaire is this study, decreased the validity of the data.

Another limitation of this study was the language. As I said before this study was conducted in two public organizations. The employees, high level managers have English as their second language, means they are more comfortable in Swedish than in English, this is the reason why they preferred to make emails interviews, and the limitation of this emails is that the respondents could not give deep answers to the interviews questions.

Future researchers interested in this field may include:

- to conduct a qualitative research in different public organizations, also including private organizations but for a longer period of time, so the researcher can make a comparison of the top management's role in implementing an information security policy between public and private organizations. The researcher can also try to find other success factors related to the implementation of an information security.
- to conduct a mixed research study, by using both interviews with certain managers and employees and also questionnaire with employees who are randomly selected. In this case, the researcher can compare the findings from the qualitative and quantitative research, if they are similar, this would put more validity of the data.

8. References

Abu Talib, M. ; Khelifi, A. ; El Barachi, M. & Ormandjieva, O. (2012) Guide to ISO 27001: UAE Case Study. *Issues in Informing Science & Information Technology,* 9 (19), p. 331-349.

Al-Awadi, M. & Renaud, K. (2007) *Success factors in information security implementation in organizations*. Retrieved February 26, 2016, from: http://www.dcs.gla.ac.uk/~karen/Papers/sucessFactors2.pdf

Andersson, H., Andersson, J., Björck, F., Eriksson, M., Eriksson, R., Lundberg, R., Patrickson, M.. & Starkerud, K. (2011) *Designing policies and control documents*. Retrieved December 15,2011, from: https://www.informationssakerhet.se/siteassets/metodstod-for-lis/3.-utforma/utforma-policy-och-styrdokument.pdf

Andersson, H. Andersson, J. Björck, F. Eriksson, M. Eriksson, Lundberg, R. Patrickson, M.& Starkerud, K. (2011) *Designing policies and control documents*. Retrieved December 15,2011, from:https://www.informationssakerhet.se/siteassets/metodstod-for-lis/1.-forbereda/introduktion-till-metodstodet.pdf

Baxter, P. & Jack, S., (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report*, 13(4), 544-559.

Brodie, C (2008) *The importance of security awareness*. Retrieved March 16, 2016 from:https://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013

Burns, E. (2010) Developing email interview practices in qualitative research. *Sociological research online,* 15(4), 8.

Callahan, T.C. and Hobbs, R. (1998). *Research Ethics*. Retrieved March 16, 2016 from: http://depts.washington.edu/bioethx/topics/resrch.html

Canavan, S. (2003). *An Information Security Policy Development Guide for Large Companies*. Retrieved March 16, 2016, from: https://www.giac.org/paper/gsec/3475/information-security-policy-development-guide-large-companies/105682

Chua, W. (1986). Radical Developments in Accounting Thought. The Accounting Review, 61(4), 601-632.

Cresswell, J.W. (2009*.) Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (3rd ed.). Los Angeles: Sage Publications.

Deming institute. (2016). *The PDSA Cycle*. Retrieved 2016, from: https://www.deming.org/theman/theories/pdsacycle

Dinnie, G. (1999). The Second Annual Global Information Security Survey. *Information Management & computer security*, 7(3), 112-120.

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security*, *7*(4), 171-175.

Doherty, N. & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches. *Information Resources Management Journal*, *18*(4),21-39.

Fung, P. & Jordan,E.(2002). *Implementation of Information Security: A Knowledge-based Approach*. Retrieved March 16, 2016, from: http://www.pacis-net.org/file/2002/069.pdf

Fung, P., Kwok, L. & Longley, D. (2003). Electronic Information Security Documentation. *Australian Computer society, (21)*, 25-31.

Golafshani, N. (2003). Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*,*8*(4), 600-604.

Gordon, L. and Loeb, M. (2006). Budgeting process for information security expenditures. *Communications of the ACM*, *49*(1), 121-125.

Hinde, S. (2002). Security surveys spring crop. *Computers & Security*, *21*(4), 310-321.

Hone, K. & Eloff, J. (2002). What Makes an Effective Information Security Policy? *Network Security*, *2*(6), 14-16.

James, N. & Busher, H. (2006). Credibility, authenticity and voice: dilemmas in online interviewing. *Qualitative Research*, 6 (3), 403-420

Jon, D. (2002). Policy enforcement in the workplace. *Computers & Security, 21*(6), 506-513.

Jones, A. (2007). A framework for the management of information security risks. *BT Technology Journal*, 25(1), 30-36.

Knapp, K., Marshall, T., Kelly Rainer, R. & Nelson Ford, F. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security*, *14*(1), 24-36.

Knapp, K., Marshall, T., Rainer, R. & Morrow, D. (2006). The Top Information Security Issues Facing Organizations: What Can Government Do to Help? *Information Systems Security*, *15*(4),51-58.

Klein, H. & Myers, M. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, *23*(1), 67-93.

Kwok, L. & Longley, D. (1999). Information security management and modelling. *Information Management & Computer Security, 7(1),30-40.*

Latham, R. (2013) *Information Management Advice 35: Implementing Information Security*. Retrieved November 2013, from: https://www.informationstrategy.tas.gov.au/Records-Management-Principles/Document%20Library%20%20Tools/Advice%2035%20Implementing%20Information%20Security%20Part%204%20-%20IS%20Policy.pdf

Madigan, E. M., Petrulich, C. & Motuk, K. (2004). *The Cost of Non-Compliance – When Policies Fail*. Retrieved March 16 ,2016, from: http://130.18.86.27/faculty/warkentin/SecurityPapers/Robert/Others/MadiganPetrulichMotuk2004_SIGUCCS_NonCompliance.pdf

McKay, J. (2003). *Pitching the Policy: implementing IT Security Policy through awareness*. Retrieved March 16, 2016, from: https://www.giac.org/paper/gsec/3223/pitching-policy-implementing-security-policy-awareness/105199

Myers, M., (1997). Qualitative Research in Information Systems. *MISQ Quarterly, 21*(2), 241-242.

Orlikowski, W. & Baroudi, J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*, *2*(1), 1-28.

Peltier, T. (2005). Implementing an Information Security Awareness Program. *Information Systems Security*, *14*(2), 37-49.

Posthumus, S. & Von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 23(8), 638-646.

Reid, N., Petocz, P.& Gordon, S. (2008). Research interviews in cyberspace. *Qualitative Research Journal*, 8(1), 47.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

Snedaker, S. (2013). *Business continuity and disaster recovery planning for IT professionals*. USA: Elsevier Inc.

Stake, R. (1995). *The art of case study research*. London: Sage Publications.

Swanson M. and Guttman B. (1996). *Generally Accepted Principles and Practices for Securing Information Technology Systems*. Retrieved April 16 ,2016, from: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Veiga, A. & Eloff, J. (2007). An Information Governance Framework. *Information Systems Management,* 24(4) ,361-372.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security,* 24(2), 99-104.

Von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*, *7*(1), 50-58.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, *15*(3), 320-330.

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii – xxiii.

Whitman, M. & Mattord, H. (2011). *Principles of information security*. USA: South-Western Cengage Learning.

Whitman, M. & Mattord, H. (2014). *Management of information security*. Boston: Course Technology Cengage Learning.

Yin, R. K. (2003). *Case Study Research* (3rd edition). SAGE Publications Inc.

Yin, R. K. (2014). *Case Study Research*: *Design and Methods* (5th edition). SAGE Publications Inc.

Appendix A

Information security policy and approach to the implementation of an information security policy

1. Does your company have an information security policy?
2. Do you think the information security policy is an important tool that your organization should have with the purpose of managing a good implementation of information security?
3. What types of information security policies do you have in your company?
4. Do you read the information security policy document? If yes, is it understandable?
5. Who create the information security policy in your company?
6. Does the company have any policy development project? If yes? Explain how is it managed?
7. Do you think the information security policy is an important tool that your organization should have with the purpose of managing a good implementation of an information security? If yes? Why? if no? why?
8. Who organize the policy development project in your company?
9. Who creates the policy development in your company?
10. How many phases do the policy development project have?
11. Does your company use any standard? which standard does your company use?
12. What importance does the top management of your organization put on information security policy?
13. How do you see that top management in your organization understand the need on an information security policy in your organization?
14. Does your company use a bottom up or a top down approach when implementing the information security policy?
15. What is the purpose of information security policies?
16. Do you follow all security guidelines? Do you think it is hard to remember all guidelines?
17. What is the role of policy in an information security program?
18. Which approach does your company use when implementing an information security policy? (bottom up or top down approach)
19. What is the role of top management, when implementing an information security policy in your organization?

Success factors

1. What do you think are the success factors connected to the success implementation of an information security?
2. How does your organization educate and making aware its employees of security of information?
3. How do you ensure that employees read and understand the content of security policies?
4. What are the top management's perceptions of the implementation of information security?
5. Does top management in your organization understand the need of an information security? Explain how?
6. What importance does the top management of your organization put on information security?
7. What does an information security mean to you?
8. Does your organization get sufficient resources in order to realize an effective information security?
9. Does your organization set objectives and goals?