Creating, Maintaining and Managing an Information Security Culture.

Alex Fagerström

Degree Thesis

Information and Media Technology

2013

EXAMENSARBETE	
Arcada	
Utbildningsprogram:	Informations- och medieteknik
Identifikationsnummer:	4361
Författare:	Alex Fagerström
Arbetets namn:	Att skapa, upprätthålla och administrera en informationssäkerhetskultur
Handledare (Arcada):	Göran Pulkkis
Uppdragsgivare:	KPMG Oy Ab

Sammandrag:

Under det senaste årtiondet har företagsledningen haft behov att skydda företagsinformation mot ett nytt hot: företagspersonalens misstag och illvilja har stigit till ett av de största hoten mot datasäkerheten i organisationer. Genom att skapa en stark informationssäkerhetskultur i organisationen kan detta hot minskas. Detta slutarbete utreder hur man skapar, upprätthåller och administrerar en informationssäkerhetskultur i en organisation. Litteraturanalys, intervjuer och empirisk forskning används för att bättre förstå grunderna och utmaningarna med att etablera och administrera en informationssäkerhetskultur. Detta slutarbete är skrivet för Information Protection and Business Resilience avdelningen på KPMG Finland Oy Ab.

Nyckelord:	Datasäkerhet, datasäkerhetskultur, företagskultur, datasäkerhetsadministration, KPMG
Sidantal:	37
Språk:	Engelska
Datum för godkännande:	

DEGREE THESIS	
Arcada	
Degree Programme:	Information and Media Technology
Identification number:	4361
Author:	Fagerström Alex
Title:	Creating, Maintaining and Managing an Information Security Culture
Supervisor (Arcada):	Pulkkis Göran
Commissioned by:	KPMG Oy Ab

Abstract:

In the last decade a new threat to information security within an organisation has risen: data loss by personnel mistakes or maliciousness now rank among the top threats to a company's data. By creating a strong information security culture, the management can reduce the risk of data loss. This thesis investigates how to create, maintain and manage an information security culture. Literature analysis, interviews with management members at KPMG, the company for which this thesis was written, and an empirical study are used to better understand the basics and challenges with establishing and managing an information security culture.

Keywords:	Information Security, Information Security Culture, Corporate Culture, Policy, KPMG, Information Security Management,
Number of pages:	37
Language:	English
Date of acceptance:	

INNEHÅLL / CONTENTS

Figures

1 INTRODUCTION

In today's corporate world business and operational information is among the most valuable resources a company has and it is essential for almost all operations (Glazer, 1993; McFadzean et al.,2006; Nadiminti et al., 1996; Van Wegen and deHoog, 1996). This vital information needs to be protected, ensuring its integrity, confidentiality and accessibility. The traditional approach to information security is protecting company information through a collection of technical information security procedures, usually comprising of firewalls, spam filters and access control (Glazer, 1993; Williams, 2008). While these measures improve information security by, usually, blocking unauthorized access to internal information, another, more severe, threat is often overlooked. This threat, only recognized recently, originates from within the company where the highly technical measures are inadequate. In recent years it has become evident that an organization's own personnel poses the greatest threat to its information security. Accidents while handling sensitive information ranks among the top threats in modern-world companies (TTLRY, 2007).

Even though senior management, and especially information security management, is aware of this threat, the most resources are still directed to the more technical processes, while the human factor is overlooked. Perhaps because information security is often perceived as a highly technical field, efforts have not been made to improve the more non-technical, "human", side of the company's information security. This human factor, or company culture, determines how the organization's personnel experiences and views the company. Information security culture includes individual beliefs, values and tacit knowledge about the company's information security. Because of its abstract nature it might be difficult to observe, and ever more difficult to quantify and measure, which can lead to that the senior management, perhaps even unconsciously, is neglecting it.

An information security culture is one of the corner stones for the general information security level of an organization. Technical measures, keeping the unauthorized people

outside, are useless if the threat to information security originates from inside the company.

Every organization has a corporate culture, even though its existence might not be recognized. This culture exists at both a conscious and unconscious level (Thomson, 2006). Corporate culture guides the activities of the organization and its employees (Beach, 1993) by both prescribing what the organization and its employees must do and by setting limitations concerning the activities and behavior of the employees. These limitations are especially important in information security since it relies to a large degree on employee actions and behavior. "Information security is far more than simply applying an assortment of physical and technical controls" (Thomson et al., 2006).

This thesis aims to investigate how to create, maintain and manage an information security culture. It is written to be used as a guideline when creating, maintaining and managing the information security culture at KPMG Finland Ab Oy**.** A company culture and an information security culture needs to be defined, along with what the differences, ~~if any~~, are. The current information security climate must be determined to provide a link to the real-world circumstances. Best practices, management tips and examples will be collected to help determine the best approach to creating, maintaining and managing an information security culture.

Literature analysis, interviews with company management and observation of best practices will be used in this thesis so that an educated and thoroughly researched conclusion can be made. As a case study for this thesis, the usage of ID-cards at the KPMG office in Helsinki was observed. KPMG uses the ID-cards for access control and to identify personnel at its offices around the country. The usage of these ID-cards will be tracked so that the development of information security awareness may be analyzed.

This thesis will only shortly describe and define information security, since it is expected that the reader possesses a basic knowledge of the topic. Information security culture will be presented, defined and described to provide a structured and easily readable guideline to its implementation. Examples of good practices and methods will be

presented briefly, to help the reader in understanding the fundamentals of an information security culture and how it works.

1.1 KPMG Finland Oy Ab

KPMG Finland is mainly an accounting firm, with business operations also in tax and management advisory. KPMG's headquarter is in Helsinki, KPMG operates in 17 different locations and employs almost 750 people in Finland alone.

Management wants to increase information security awareness by strengthening the information security culture. Due to its main focus being in accounting, some parts of the information security awareness within the company is relatively low. Except for the Information Protection and Business Reliance (IPBR) division of KPMG most users are not living up to the standards of a modern information security culture. This thesis and its findings will be used as a guideline when improving the information security culture.

Juha Purovesi, the Chief Operations Officer (COO) at KPMG Finland, and Antti Pirinen, the National IT Security Officer at KPMG Finland will be interviewed to provide additional viewpoints and establish a link to real-world information security applications.

1.2 Background

"Despite our intellect, we humans – you, me and everyone else – remain the most sever threat to each other's security" (Mitnick & Simon, 2002)

According to a study conducted by Tietotekniikan liitto ry (TTLRY), Symantec and Rittal in 2007 the employees pose the greatest information security risk for small and medium sized enterprises (SMEs) employing 20-250 persons. The study was conducted as an online survey, which focused on finding out the perceived information about security threats and about preparedness of SMEs in Finland. The survey received 220 re-

plies, with industry (31%), services (20%) and commerce (10%) being most active branches. IT companies only represented about 6% of the replies.

Most SMEs focus purely on technical information security, even though employee mistakes and ignorance is perceived as the greatest threat. The study concludes that you can divide the greatest perceived threats into three categories: traditional IT-security, physical security and end-users.

Most security solutions in SMEs try to address the traditional IT-security risks, which include network security, malware, spam and hacking over the network. Hardware and software problems are also included. Almost every company was using anti-virus software (99%), firewalls (98%), spam filtering (95%) and data backup (94%). About half (53%) of the companies also used intrusion prevention systems (IPS) and encryption (50%).

The second category, physical security, included threats that might damage information and hardware. Fire-, water- and smoke-damage, eavesdropping and theft were all perceived as high-risk scenarios. Most companies were satisfied with their physical security, and about half employed access management systems (55%), temperature (60%) or humidity (35%) control systems.

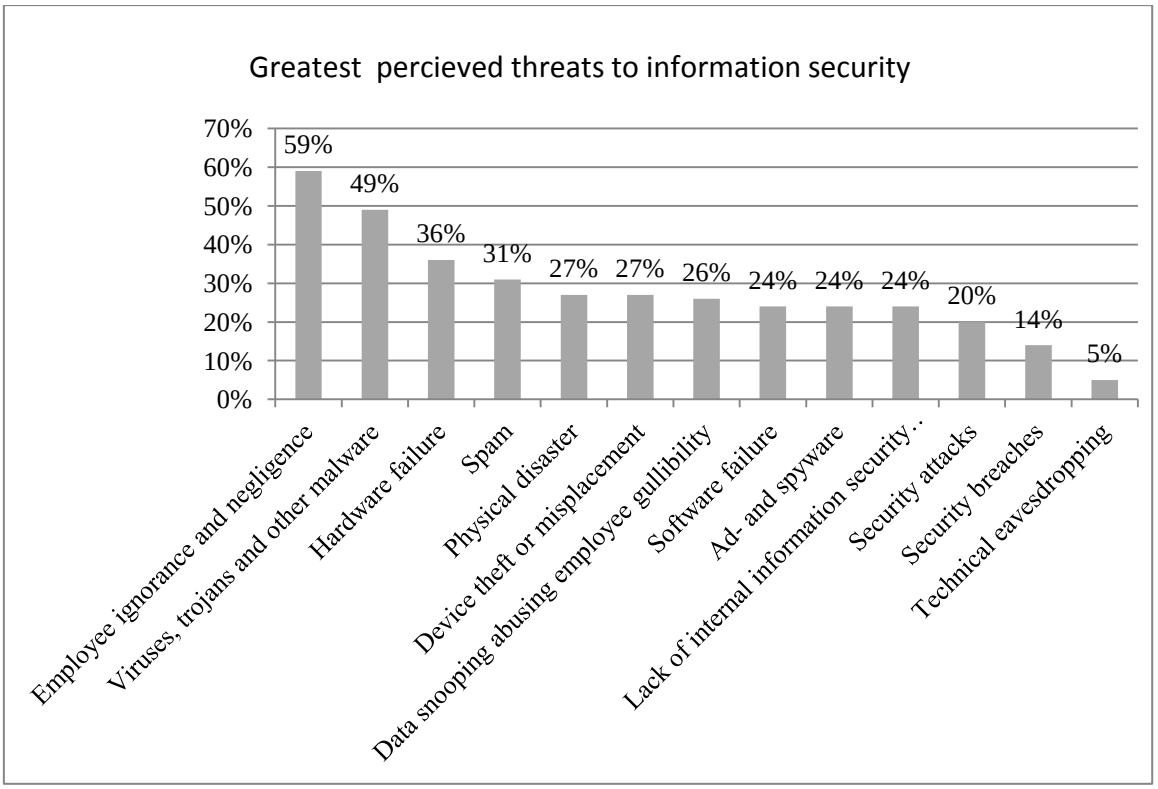

Figure 1: Greatest perceived threats to information security (TTLRY, 2007)

According to the study the greatest threat to information security is end-user ignorance and negligence. As Figure 1 illustrates, 59% of all the respondents classified the company employees the greatest threat to information security, with 26% nominating friendly spying and 24% lack of information security policies the greatest threat to information security. Information security level is greatly reduced by the employee's lack of knowledge (27%), budget limitations (14%), lack of time (13%) and the fact that the company management did not understand the importance of information security. The most common reason for data loss was reported as employee mistakes (53%), while data loss due maliciousness was only 3%. Hardware or system failures were perceived as the second greatest reason for data loss at 49% of the answers. Malware and physical breaches played only a minor role, with 10% and 14% respectively.

These findings are in line with other recent studies ranking end-users as the greatest threat to an organization's information. Despite this fact, most companies still focus al-

most purely on the technical aspect of information security, neglecting employee education and information security culture (Dhillon et al., 2001).

Information security can be seen as a competitive advantage, as long as it is properly implemented and maintained (Kosunen, 2011). The prerequisite for continuity increases when information security is integrated into every aspect of the organization's daily operations (Laaksonen et al., 2006). The employees can be encouraged to comply with management-set information security policies, by regularly educating and reminding them about the rules and regulations.

2 COMPANY AND INFORMATION SECURITY CULTURE

Every organization has a particular culture, comprised of the beliefs and values shared by its employees (Smit & Cronjé, 1992). Due to the nature of beliefs and values they cannot be measured accurately, which is why a company culture is often referred to as "just the way we do things around here" (Schein, 1999) or "that something" that contributes to the organization's success (Smit & Cronjé, 1992). A widely accepted way of thinking about company culture is to look at the different levels at which it exists. These levels are:

- **Level One: Artifacts**
  Artifacts are what can be seen, heard and felt, in an organization (Schein, 1999). These include processes and organizational structures. "Artifacts are what actually happens in an organization."(Van Niekerk & von Solms, 2010)

- **Level Two: Espoused Values**
  An organization's espoused values are the "reasons" an employee would give for why things in the organization are done in a certain way. These values are often expressed in the organization's documentation about the organization's vision, principles, ethics and values. Teamwork and the belief that everyone is important in the decision-making process are typical espoused values. They can be seen as the organization's management's "visible" contribution towards the cultural direction of the company: what the company *wants* to live up to (Van Niekerk & von Solms, 2010).

How the espoused values are interpreted and implemented depends heavily on the shared tacit assumptions of the employees. (Schein, 1999)

- **Level Three: Shared Tacit Assumptions**
  These are the beliefs, assumptions and values shared and taken for granted by the organization's employees and form the essence of that organization's culture. These under-the-skin-elements, such as rituals and routines, form an important part of the organizational culture. These tacit assumptions act as a filter when deciding how to interpret the company's espoused values: the policies and principles.

These three levels form the corporate culture in any organization. As can be seen in Figure 2, the information security culture requires and additional level to function properly:

- **Level Four: Knowledge (Information Security Only)**
  When defining the "normal" corporate culture the regular employee's job-related knowledge might be ignored since it does not benefit the culture. However, in an information security culture knowledge might not be needed to perform "normal" job functions but to be able to act according to set information security rules and policies. Employees need to have the required knowledge to perform their everyday tasks securely. Also, unless an employee knows why a certain control or action is necessary, complying with it might not seem reasonable or necessary. (Van Niekerk & von Solms, 2010)

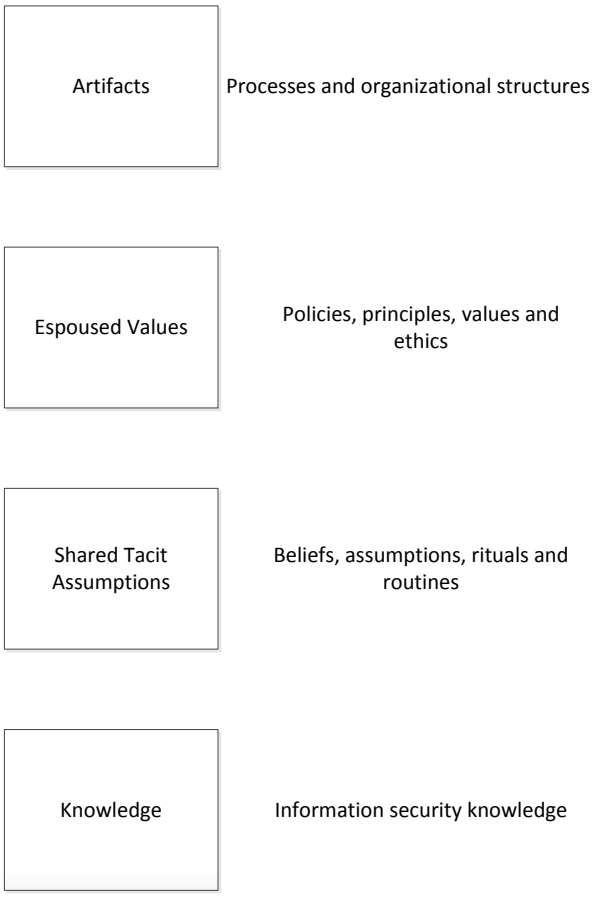

Figure 2: Levels of information security culture. Adapted from Van Niekerk & von Solms (2010)

3 CREATING AN INFORMATION SECURITY CULTURE

Beach (1993) states that the corporate culture guides the activities of the organization and its employees and not only places constraints upon the activities and behavior of employees, it also describes what the organization and its employees must do. A change in the current corporate culture requires, in practice, the unlearning, or modifying, of the organization's employee's current beliefs. Due to human nature this change might lead to resistance among the workers (Schein, 1999). The most influential factor on employee beliefs and attitudes is the working environment, which is why the change of culture has to originate from the senior management (Drennan, 1992)

The implementation of information security should start with the top management and continue downwards in the hierarchy. Schlienger and Teufel (2003) suggest a four-staged approach: commitment of the management, communication with organizational members, educating organizational members and commitment of the employees. Management education also plays an important role, since if the management does not understand the need and requirements for an information security culture then the management cannot fully support it (Laaksonen et al., 2006).

3.1 Policies and Guidelines

When companies reach a certain size, communication between the management and the employees shifts from a largely direct and verbal interaction to a more indirect kind of interaction. The sheer number of employees and the size of the middle-management level makes it harder for the top management to convey orders and wishes to the workers. This is when different guidelines and policies are introduced.

Policies are communication documents used by the management to communicate directions, rules and regulations to employees, business partners and other various parties. The Guidelines for Information Security Management standard BS7799 states that the purpose of an information security policy is "to provide the management direction and support information security (BS7799, 1999). ISO 27001, which is discussed later, is the modernized version of BS7799-2. A policy can be defined as "a course of action, guiding principle, or procedure considered expedient" (von Solms et al., 2003). Through policies the management's expectations of how employees should act is conveyed, however, everyone using them should agree that they do not interfere with personal beliefs and that they are beneficial to the organization.

Management expresses its vision and desired direction of the company through policies. This ensures that the actions and creations of the employees, and possible other parties, are in line with the senior management's vision. Policies also help to establish a company culture - although "knowing the policies is only half of the equation, staff needs to know how they should comply, from a procedural perspective" (RUsecure, 2002).

Mattia and Dhillon (2003) assign the lack of information security policy compliance to the policy's inability to reflect current practices, but stakeholder resistance also plays a key role.

A good information security policy requires structured and systematic management. The policy should be maintained, reviewed and updated when necessary. It should be well-structured, and preferably split into several sub-documents, for example on email usage and on data handling.

A well thought-out information security policy usually addresses:

- The goals of the policy, and the actions related to them.
- The roles and responsibilities of the personnel.
- Information security education.
- Protected data processing.
- Disaster preparedness and recovery.
- Repercussions from neglecting the policy.

There is no universal information security policy template since every company has individual needs and the policy must be adapted to reflect the motivations and goals of the company. (Laaksonen et al., 2006)

3.2 The "Moses Model"

Von Solms' (2004) have created a model, the Moses Model (Fig. 3), which is based on the educational structure of the Torah, the first five books in the Old Testament, which defines the rules of worshipping the Christian and Judaic God. This model could be used for creating an information security culture and it outlines what the senior management should do to influence employee behavior and increase information security compliance within the organization. These methods, including policies and procedures, are designed to provide a framework for establishing and maintaining a sustainable and easily managed information security culture.

To ensure credibility, and maximize compliance, the executive level policies should be issued, and especially endorsed, by the company's CEO (Laaksonen et al., 2006).These policies, like the Information Security policy, should not be too specific or technical, but rather conceptual and fairly static over time. It should avoid addressing regularly changing details and concentrate more on conveying the principles the management has decided upon.

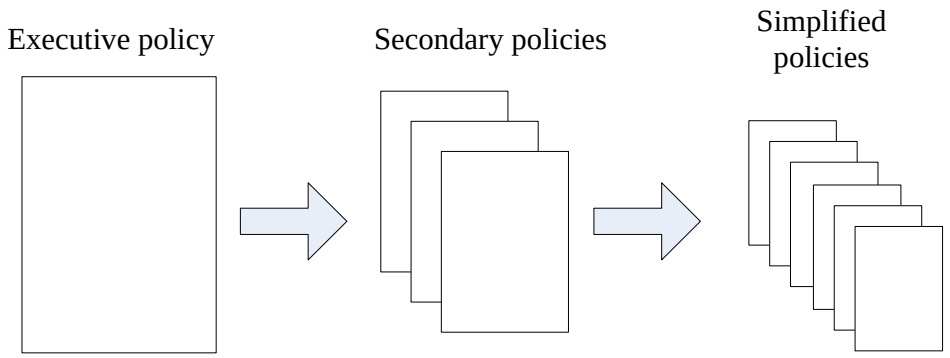

Figure 3: The Moses Model

The executive policies should be explained in more detail by secondary policies, like Internet or network policies, that account for and change depending on economical, business and technological changes happening in the organization. These secondary policies should be dynamic and quite detailed, covering all the technical directives and regulations concerning the IT-infrastructure.

To increase employee compliance and collaboration a series of simplified procedures, based on the executive level and secondary policies, should be used. These procedures should reflect the higher level policies in a non-technical and easily understandable way to facilitate an information secure way of working. Examples of simplified procedures are proposed actions for end-users or third party consultants.

Unless procedures and policies are followed, either due to the lack of communication or education, the chance of cultivating an information security culture is minimal. This is why everyone in the organization should be properly educated on the management-set

policies and procedures. The employees must also constantly be reminded about the policies and procedures and their knowledge about the subject refreshed. Solms recommends a continuous information security awareness program to ensure initial education and regular updates and reminders.

A proper framework should be used to embed the management's general principles and ideas in logical, non-technical and well-structured documents. These policies should then, through education and reminders, be distributed to the employees.

3.3 Educating Personnel

“Properly trained and diligent employees can become the strongest link in an organization’s security infrastructure “ (Thomson et al., 2006).

All personnel should be educated about information security, but everyone does not need a formal education or certificate (Whitman & Mattord, 2003). The goal with information security education for employees is to make them act according to the management’s wishes, so that the company information is properly protected. The employees do not need to know everything about information security, but they should be knowledgeable about the risks with their work and how to minimize them (Kauppinen, 2009). The technical aspects of information security should not be visible to the users (Laaksonen et al., 2006).

The education should primarily be based on the information security policy and procedures. Process descriptions and information security flaws discovered in either internal or external audits should also be used when planning employee education. The information security education should consider the impact of different motives on the learning experience. Individual motivation also plays an important role in the education’s effectiveness (Laaksonen et al., 2006).

Information security education should in general be made more usable and less technically advanced and time consuming (Herley, 2009). Policies and procedures should be

explained with the help of practical examples relating the employee's job. Using practical examples are supposed to spark conversation between the employees about policies and their practical deployment. Essentially the employees need to understand how to act and why. Presentations should focus on demonstrations, instead of listing things the employees are not allowed to do. Unless practical examples are used, the desired level of information security will not be reached (Laaksonen et al., 2006).

3.4 Employee Compliance

Employee compliance plays an important role when creating an information security culture. The general approach to information security is to issue policies, rules and regulations to control employee behavior. These instructions are often neglected and dismissed for being overly technical and difficult to understand. The employees need to understand, internalize and follow policies, procedures and processes set by senior management. Without proper understanding of what the policies, procedures and processes include and control an employee will not be able to follow set standards. (Laaksonen et al., 2006)

As studies suggest, the employees pose the greatest threat to an organizations information security. Through either mistakes or malicious actions they might disclose confidential and potentially harmful information to outside parties (TTLRY, 2007). To counter this, the company's employees need to be educated about the information security policies, procedures and processes. They also need to follow them. In some cases, even though policies and regulations are in place, end-users still breach information security. One common argument is that users are inherently stupid and lazy for not following simple rules, Herley (2009) presents an interesting idea: that user behavior is dependant of a simple economic equation. Herley claims that users, perhaps unconsciously, weigh the advantages and disadvantages of complying with information security rules, and conclude that the cost / gain ratio is not good enough to warrant secure behavior. The main problem is that information security promoters are unable to present scientific data to demonstrate that information security compliance is worth investing

time in. There is no data for how many intrusion attempts were stopped because of strong passwords, or how many victims a spam campaign creates.(Herley, 2009)

4 MAINTAINING AN INFORMATION SECURITY CULTURE

4.1 The PDCA model

The ISO 27001 standard, which was published in 2005 and replaces the old BS7799-2 standard, is a specification for an Information Security Management System (ISMS). The objective of the standard is to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS". The ISO 27001 standard covers management responsibility, internal audits and ISMS improvements. It also presents and defines a set of objectives and controls to be used when improving information security.(ISO 27001)

ISO 27001 is often implemented to address information security issues. By complying with the ISO 27001 standard the company can ensure these issues are being addressed in a consistent, repeatable and auditable manner. The ISO 27001 certificate reassures internal and external stakeholders that information security issues are being addressed in a standardized manner. (Ashenden, 2008)

The standard employs the Plan-Do-Check-Act model (PDCA) to structure the process approach, which is defined as "The application of a system of processes within an organization, together with the identification and interactions of these processes and their management". Essentially it defines a way of working within an organization, a framework for continuously improving information security. As can be seen in Figure 4, the PDCA model promotes a continuous cycle of Planning, Doing, Checking and Acting. (ISO 27001)

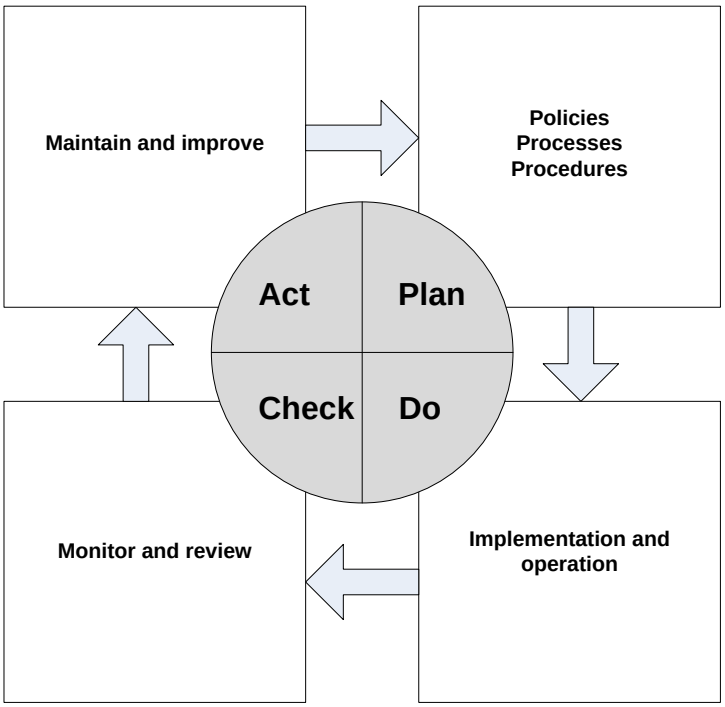

Figure 4: The PDCA model

The Planning-phase, or the establishing of the ISMS, includes creating policies, objectives, processes and procedures to help manage the risk and improving information security. These regulations should be in line with the organization's general objectives and policies. (ISO 27001)

In the Do-phase, the IT-management implements and operates the Information Security Management Systems policies, processes, procedures and controls (ISO 27001).

Monitoring and reviewing the ISMS should be done in the Check-phase. The process performances should be assessed, and preferably measured, against the set policies and objectives. The results should then be compiled and reported to the management for review, and to be used in the next phase. (ISO 27001)

The Act-phase consists of maintaining and improving the ISMS. The results from the Check-phase are used to determine the improvements that should be made to achieve a continuous improvement of the ISMS. (ISO 27001)

These phases are designed to be continuously used as a never-ending cycle to ensure that the organization's information security is kept up to date and improved (ISO 27001). "It's a cycle of evaluation and change of maintenance" (Schlienger & Teufel, 2003).

ISO 27001 also includes chapters on management responsibility, resourcing and personnel education. It also describes the requirements, functions and development of an information security management system. (ISO 27001)

4.2 Measuring Information Security

To be able to ensure that implementation of information security policies and procedures, and employee education, is benefiting the organization their effect must be measured. Schlienger and Teufel (2003) suggest a mix of methods for evaluating the different layers of information security culture: artifacts, espoused values and shared tacit assumptions. (Schlienger & Teufel, 2003)

The analysis of information security documents, such as policies and procedures, evaluates the artifacts and official, espoused, values while being unable to grasp the true values of the employees. Having everyone fill in a questionnaire about the company's information security policies helps map the true values of the employees, while also making it possible to compare them to the official documents. Interviews should be conducted, especially with the Chief Security Office to get an overview of all three layers; artifacts, official and true values. Artifacts should also be examined through audits, where the visible part of the information security culture is studied.(Schlienger et al, 2003)

5 MANAGING AN INFORMATION SECURITY CULTURE

An organization's information security culture generally reflects the management's view on information security (Ruighaver et al., 2007).

"Knowledge and experience, information relating to incidents and vulnerabilities, risk analysis and management, strategy and planning, policy and standards, processes and procedures, methodologies and frameworks, awareness and training, audits and contracts and outsourcing are all important parts of information security management." (Purser, 2004)

5.1 Managing Principles

Managing an information security culture is the responsibility of the senior management. While senior management members might not draft the policies and procedures themselves, they need to appoint someone to do it. They also need to give their full support to information security processes, by endorsing and signing them. Without the support of the senior management it is impossible to establish and maintain an information security culture. (Laaksonen et al., 2006)

Information security often neglects the human challenges, and focus is on the "locks and keys" of information security. Even though policies and procedures play an important role in information security management, human behavior needs to be considered when establishing and maintaining a balanced and structured information security culture.

When conventions and traditions are challenged by new security rules and regulations being implemented, it has the potential to cause value conflicts. These value conflicts easily manifest themselves as misinterpretations of new policies and procedures. Research suggests that this conflict and resistance is unavoidable, but through the use of for example icons, rituals and language, change can be given a new meaning. This makes it appear rational, legitimate and even desirable. (Kolkowska & Dhillon, 2013)

Information security is no longer only about the holy trinity: confidentiality, integrity and availability. The focus has shifted towards being able to provide real business benefits by both protecting and facilitating the controlled sharing of information, and managing the risks associated. However, the management must also realize that information security is about individuals, and when managing their behavior both their specific job-related roles and their personal and social identities must be considered. (Ashenden, 2008)

One of the greatest challenges in information security management is to balance resources. This is done by implementing a management system which is based on information security policies, processes and practices. The goal will be to make sure that employees follow these principles consistently. The employee's behavior might seem confusing and unpredictable because their individual beliefs and values are often overlooked. This needs to be taken into account when planning and creating an organizational culture. (Ashenden, 2008) Dhillon and Backhouse (2001) claim that information security is about "more than just locks and keys and must relate to the social grouping and behavior [of the employees]".

Interviews with information security managers reveal that they often neglect listening to the end-users, and instead focus on reinforcing their ideas through presentations. Instead of listening to the end user's perspective, the information security managers often rely on their own, often biased, view of how they think the end-user experiences information security. (Ashenden, 2008)

According to Adam and Sasse (1999) a lack of communication with end-users causes them to create their own, very often flawed, view on information security, its importance and threats.

6 RESULTS

6.1 Case Study

KPMG is one of the Big Four accounting firms, with divisions also tax and management advisory. With about 750 employees and 17 locations around Finland KPMG Finland Oy Ab can be classified as a large enterprise. The company has its headquarters in Helsinki, where most of the company's employees work on a daily basis.

KPMG uses photo ID-cards to identify employees at the offices and to control access rights to different parts of the building. General security requires everyone within the offices to be identifiable, which is why wearing an ID-card is mandatory. Everyone, from senior management to trainees is required to wear an ID-card when on premises. However, this rule has proved difficult to enforce, which is why the company's management decided to launch a campaign to promote the usage of ID-cards.

The campaign time was 8.4.-21.4.2013 and was named "Bongaa Partneri –kampanja" ("Spot the Partner"). The idea was that if an employee was able to spot a partner or the National IT Security Officer (NITSO) without and ID-card they would be able to claim a reward. However, the employee itself had to be wearing his/her ID-card, otherwise they would not be eligible for the rewards.

Employees often think of information security as something boring with a lot of technical instructions, which is why the campaign was designed to encourage ID-card usage through a more fun and relaxed way.

The campaign ran for two weeks in April 2013, and was promoted through the KPMG intranet and screensavers on computer lock-screens displaying campaign posters. The intranet promotion was done two weeks in advance to spark interest and so that everyone missing an ID-card could get a new one or anyone with a broken one could get a replacement card. The screensaver poster was also aired during that time, but it was more cryptic, aiming to intrigue the employees and spark a conversation.

In order to evaluate the success of the campaign its results needed to be measured. This was done in three phases: before the campaign, during the campaign and after the campaign. ID-card usage was estimated by counting the percent of employees wearing their ID-card in the office. To increase the accuracy and credibility of the observations, they were conducted in the same place and at around the same time every time. The observations were made at three different dates to gain and reference points in order to assess the effectiveness of the campaign. The observations were made two weeks prior to the campaign, once during the campaign and one week after the campaign ended. The average sample size (N), i.e. the amount of people observed, was 54.

6.1.1 Campaign Results

The information security awareness campaign aimed at increasing ID-card usage ran for two weeks in April 2013. It was promoted in the KPMG intranet and through emails and lock-screen images. The measuring was done prior to, during, and after the campaign so that its effectiveness could be estimated.

The results from the campaign were not expected. While the average sample size was N=54, the average amount of people using their ID-cards was only 13,33.

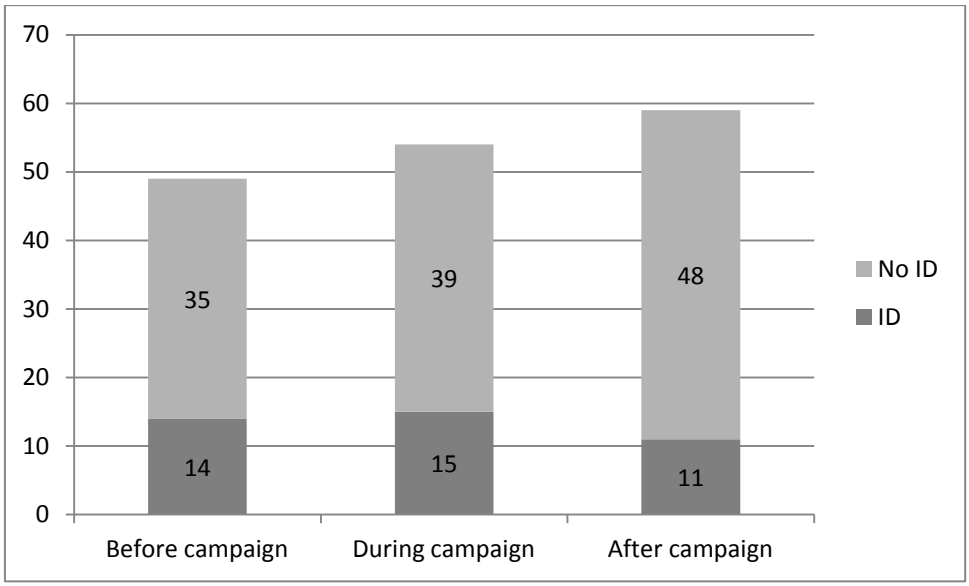

Figure 5: ID-card tracking results

As Figure 5 illustrates the ID-card usage dropped for an unknown reason directly after the campaign. Figure 6 shows that before the campaign launch the ID-card usage was at 28,6%, during the campaign it was at 27,8% and after the campaign it dropped to 18,7%.

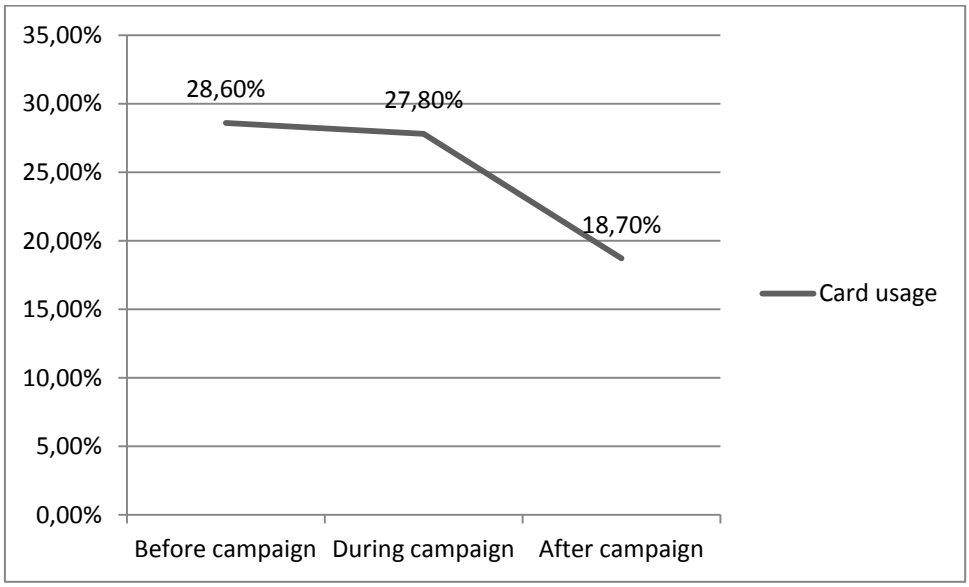

Figure 6: ID-card usage

These results show that even the best practices of information security culture maintenance might not always be effective. It is also a proof that maintaining an information security culture is an on-going process, and employee behavior cannot be easily changed. These findings might also result from employee resistance towards the management-set rules. This might be due to the inconvenience of wearing and keeping track of the ID-cards, but also because the employees do not understand the reasoning behind the rule. Since an information security culture relies heavily on the management's example, it would have been interesting to be able to measure the ID-card usage among the senior management members. Unfortunately this was not possible due to time constraints.

Only 4 partners were spotted not using their ID-cards during the campaign, and both the COO, Juha Purovesi, and Antti Pirinen, the National IT Security Officer, felt that the information security awareness among the partners had increased as a result of the campaign.

6.2 Interviews with KPMG Management

KPMG Management was interviewed to provide both a picture of the current view of the management on information security and information security culture maintenance. The interviews will also be used to find possible misconceptions and oversights regarding information security and information security culture. Juha Purovesi (JP), the Chief Operations Officer of KPMG Finland, and the National IT Security Officer (NITSO) Antti Pirinen (AP) were interviewed to provide two aspects; one of senior management and one of security management.

1. **How is the organization culture developed at KPMG? What is the vision of it?**

   Both interviewees agreed that the current organizational culture originates from the brand attributes and company vision that the senior management members have agreed on.

2. **What are the biggest threats to information security at KPMG?**

   While JP placed complete trust in the current technical countermeasures, AP was a bit more hesitant to completely disregard the risk of hacking or other intrusions. AP also did not consider internal data loss to be such a big risk, but if it would happen the consequences could be terrible.

3. **How would you describe the information security culture at KPMG?**

   "There's always room for improvement" is a commonly used phrase when discussing the information security culture. Both JP and AP considered the current information security culture level to be intermediate. AP stressed that while most employees know, and act according to, the confidentiality rules, the more basic regulations, like ID-card usage and locking the workstation when not using it, are often forgotten. JP also pointed out that since KPMG has not had any major information security breaches, many people may not consider it as a realistic risk.

4. **What are the greatest challenges with instituting an information security culture at KPMG? How is the information security culture maintained at KPMG?**

   Yearly, and initial, information security education, awareness campaigns and information security bulletins are used to maintain the information security culture at KPMG. AP divided the challenges into two parts; educating personnel and identifying current and future information security needs.

5. **Detailed observations of current state:**

    a. **Employee compliance: Which are harder to convince to follow the policies and regulations: management or the employees? Why?**

    JP stated that both groups, management and the employees, follow the policies and procedures equally well. AP agreed, but pointed out that while most of the senior management members understand their responsibility, persuading the ones that don't understand, to comply with defined policies is a great challenge.

    b. **What are the reasons for the poor ID-card usage? And the drop in usage after the campaign?**

    Both interviewees agree that the drop in ID-card usage was probably a statistical error or a coincidence. AP also pointed out that the awareness campaigns also focus a lot on just keeping the personnel aware of information security, so that it becomes a natural part of the office environment.

6. **How is information security measured at KPMG?**

    AP stressed more the ground-level measures taken; spam and malware filtering and monitoring, incident handling and risk estimation. JP focused on the management-side by discussing threats with the Risk Management Committee and Risk Management Partner, while also stressing the advantages of having an organizationally independent National IT Security Officer which monitors and reports on the current information security level.

7. **Information security culture's future challenges?**

    AP nominated understanding the big picture and controlling and balancing the risks and the new business models as the greatest challenges. Since the number of service providers increase, compatibility and data transferability are likely to become major issues in the future. JP stressed the possible vulnerability and stability issues larger platforms might present. The greatest concern was the increased dependence on information and information systems, since system fail-

ures could cripple the organization for an undetermined period of time. Continuous education and information about information security were perceived as the best ways to maintain the current level of information security and on information security culture.

While Juha Purovesi focused more on the management-side of the information security issues and culture, he and Antti Pirinen shared the same view on almost everything. The question about current threats ended up being the most controversial, with AP stressing the importance of considering the current climate and environment before making risk assessments.

6.3 Establishing an Information Security Culture

If one were introduced to a company without an information security culture with the objective of creating one, what are the main things to consider? Building on what has been discussed in this paper it should be done in several consecutive, perhaps overlapping, steps to ensure the effectiveness and success of the process. These steps could be as follows:

1. **Establish ground level**

The current situation must be defined. This should be done by measuring the personnel's knowledge and education, but the company's management's education and knowledge might play even a bigger role. Changing an information security culture is not possible without the support of the management, and if management members are not knowledgeable about information security issues they cannot support them fully. Technical testing should also be used to gain raw data about vulnerabilities, both to be corrected and to be used to motivate and inform the management.

2. **Educate management**

Educating management should be done as soon as possible so that the management's insights regarding information security issues can be used when defining the scope. Educating management members also helps to ensure their support for the coming changes. This should be done simultaneously with defining the scope.

3. **Define vision and objective**

Secondly the desired level of information security, and thus the information security culture, must be defined. Depending on the company's field and partners the required information security level might vary significantly. The vision and objective should be aligned with the other aspects of the business, so that information security becomes a part of every process and not just a separate, often disregarded, process. The company's future plans should also be determined, so that information security can be incorporated from the start of future computer systems and processes.

4. **Create policies, procedures and regulations**

Policies, procedures and regulations should be created based on the required level of information security. These instructions should be endorsed and followed by the management. Leading by example plays a major role when establishing an information security culture.

5. **Educate personnel**

The personnel should be educated about the policies, procedures and regulations. To spark conversation and help link them to real life scenarios the instructions should be explained using examples and personal experiences. The reasoning behind the policies and regulations should also be explained, so that the employees are able to understand why these should be followed. Workshops, where the employees can communicate with the information security team, express concerns and ask questions, should be favored over the usual lecture-like education. One reoccurring problem with employee education is the time requirement proper education poses. Especially in larger companies the logistics of education might present a greater challenge than the education itself. To solve this problem online education, lectures or video-conferencing could be used. Edu-

cation should also be made mandatory, and sanctions put in place in case employees are unable to acquire the required education.

6. Audits

Depending on the company's size and resources available internal audits should be made regularly. The personnel's knowledge and education should be audited within a year after the initial information security education. Questionnaires, campaigns and polls can be used to gain a better understanding of the knowledge and atmosphere. Also raw data should be used to assess the current level of information security, since employee viewpoints and knowledge does not always translate well into practice. The IT department could for example gather a list of all software installed on company machines, and check that list towards allowed and forbidden software. The results from these different measurements should be used to pin-point problem areas and to find possible paths to improvement.

7. Develop

The management and maintenance of the information security culture should be developed based on the results from the audit. User education should be tailored to meet the changing environment and specific security concerns. Processes should be developed towards a more information secure way of working.

8. Maintain

The achieved information security culture should be maintained according to the PDCA model, where you Plan, Do, Check and Act. Awareness campaigns, competitions and continuous education are some of the recommended ways to maintain an information security culture at an appropriate level.

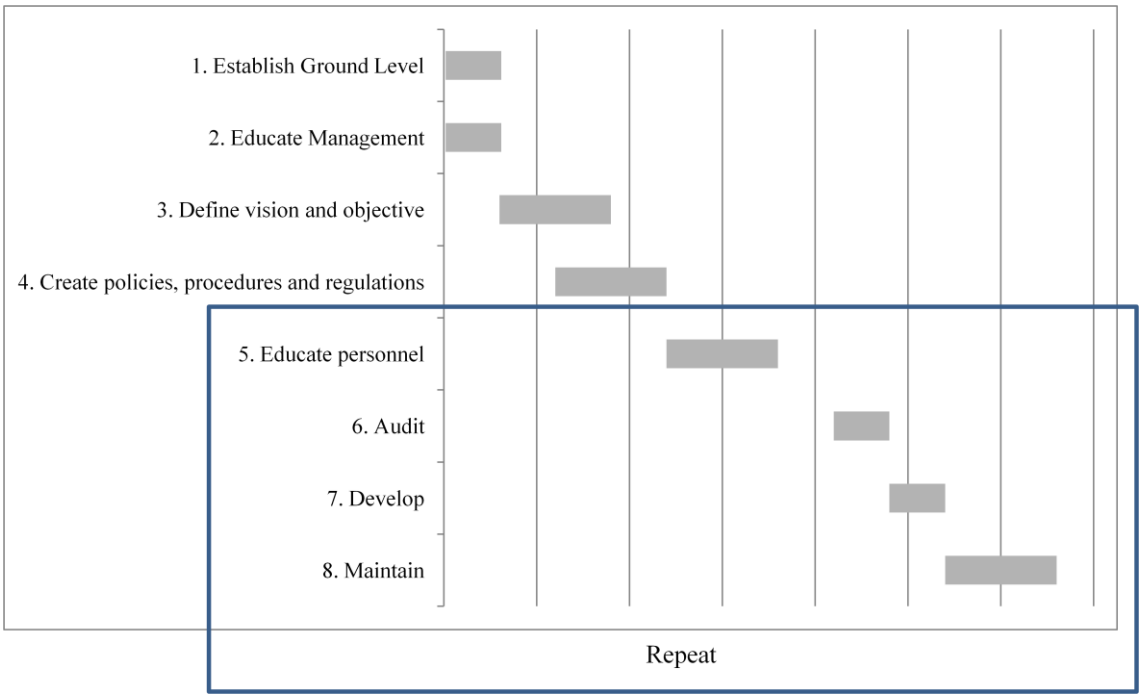

Figure 7: GANT-chart with a suggested time frame for implementing an information security culture.

These steps should preferably be done in this order, but as Figure 7 illustrates some of them may overlap. The timeframe depends on the organization's size and the resources available. This should not be seen as a definitive guide, but more of general guidelines of how an information security culture could be instituted in a company.

7 CONCLUSIONS

In recent years more and more companies have realized that a significant part of the threats to information security comes from inside the company. Employee mistakes and maliciousness account for a growing part of breaches in information security and data loss. This problem is hard to counter with hardware or software, and has to be dealt with more delicately. An information security culture, where the focus is on the individual's knowledge and perception on information security, needs to be established and maintained to ensure the safety of the company's data.

An information security culture should be based on management-set and endorsed policies, procedures and regulations. These should be divided into more general, executive level, policies, more technical and extensive secondary policies and simple, easy-to-follow instructions aimed at the regular employees. These policies need to be readily available to the personnel, and continuously updated. A good information security policy requires systematic and structured management, and it should address topics such as the roles and responsibilities of the personnel, protected data handling, and disaster preparedness and recovery.

The information security culture should then be maintained and improved using for example the PDCA model, which defines a continuous cycle of measurement and improvement. Both the management and the employees should be educated regularly, preferably yearly, about the basics and the changes in company policies, while the management should also be kept up to date on the progress of both external and internal information security issues. The education should be practical and non-technical and based on real life scenarios and examples to improve learning and understanding. Reasons for problems in compliance should be investigated and resolved. The information security level should also be measured, by performing internal or external audits, where problem areas and security issues are pin-pointed. These issues should then be investigated and corrected according the company information security policy.

To ensure information security in an organization, different frameworks can be used as references. For example ISO 27001 is an information security management framework which defines certain management principles and controls to improve organizational information security.

As the results from the ID-card usage tracking suggest, managing an information security culture is a continuous process and changes rarely happen overnight. The senior management members should lead by example, since if they do not follow the policies they have instituted themselves, the chance that the regular employees would follow these policies is minimal. The interviews conducted with KPMG management members suggests that the management should be educated on the current information security threats by for example a Risk Management Committee, which investigates possible threats and complications both within and outside the organization. Also instituting an Information Security Officer of some sort is advisable. The role should be organizationally independent to minimize the risk for bias.

Information security awareness campaigns and bulletins should be used both to increase awareness and to make information security a natural part of the organization.

REFERENCES

1 Adam, A., Sasse M. Angela, 1999. Users are not the enemy. Communications of the ACM 42 (1999), 40-6.

2 Ashenden, D., 2008. Information security management: a human challenge. Information Security Technical Report 13 (2008), 195-201.

3 Beach, L.R., 1993. Making the right decision. Organizational culture, vision and planning. Eaglewood Cliffs, New Jersey: Prentice Hall

4 BS 7799, 1999. Code of practice for the information security management. British Standards Institute, United Kingdom, 1999.

5 Drennan, D., 1992. Transforming company culture. Berkshire, England: MacGraw-Hill.

6 Glazer, M., 1993. Measuring the value of information: the information intensive organisation. IBM Systems Journal 32 (1), 99-110.

7 Herley, C., 2009. So Long, and no thanks for the externalities: the rational rejection of security advice by users. Microsoft Research, Redmond, WA, USA.

8 ISO 27001 standard. http://www.27000.org/iso-27001.htm. Accessed 23.4.2013.

9 Kauppinen, J., 2009. Tietoturvatietoisuuden lisääminen organisaatiossa. Case Normet Group Oy. Bsc. Thesis (in Finnish). Degree in Business and Management, Savonia University of Applied Sciences.

10 Kosunen, P., 2011. Yrityksen henkilöstö – merkittävä tietoturvauhka. Bsc. Thesis (in Finnish). Information Technology, Haaga-Helia University of Applied Sciences, Helsinki.

11 Kolkowska, E., Dhillon, G., 2013. Organizational power and information security rule compliance. Computers & Security 33 (2013), 3-11.

12 McFadzean, E., Ezingeard J.-N., Birchall, D., 2006. Anchoring information security governance research: sociological groundings and future directions. Journal of Information System Security 2 (3).

13 Mitnick, K.D., Simon, W.L., 2002. The art of deception – controlling the human element of security. Indianapolis, Indiana: Wiley Publishing, Inc.

14 Nadiminti, R., Mukhopadhyay, T., Kriebel, C., 1996. Risk aversion and the value of information. Decision Support Systems. 16 (3), 241-254.

15 Purser, S., 2004. A practical guide to managing Information Security. Artech House.

16 RUsecure information security policies**.** http://www.information-security-policies.com/policies.htm. Accessed 23.4.2013.

17 Ruighaver, A.B., Maynard, S.B., Chang, S., 2007. Organisational security culture: Extending the end-user perspective. Computers & Security 26 (2007) 56-62. Department of Information Systems, University of Melbourne, Australia.

18 Schein, EH., 1999. The corporate culture survival guide. Jossey-Bass Inc.

19 Schlienger, T., Teufel, S., 2003. Information security culture – from analysis to change. South African Computer Journal, 2003.

20 Smit PJ., Cronjé GJ de J., 1992. Management principles: a contemporary South African edition. JUTA.

21 Thomson, K.-L., von Solms, R., Louw, L., 2006. Cultivating an organizational information security culture. Centre for Information Security Studies, Nelson Mandela Metropolitan University, South Africa.

22 Tietotekniikan liitto Ry (TTLRY), 2007. Tietoturvatutkimus PK-yritykset. https://ssl.ttlry.fi/tutkimus/pk-tietoturvatutkimus. Accessed 23.4.2013.

23 Van Niekerk, J.F., von Solms, R., 2010. Information Security culture: A management perspective. Computers & Security 29 (476-486).

24 Van Wegen, B., deHoog, R., 1996. Measuring the economical value of information systems. Journal of Information Technology 11 (3), 247-260.

25 Von Solms, R., von Solms, B., 2004. From policies to culture. Computers & Security (2004), 275-279.

26 Whitman, M. & Mattord, H. 2003. Principles of Information Security. Boston: Thomson Course Technology.

27 Williams, P., 2008. In a “trusting” environment, everyone is responsible for information security. Information Security Technical Report 13 (2008), 207-215.