UNIVERSITY OF VAASA
FACULTY OF TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE

Kaisa Toivonen

INFORMATION SECURITY AWARENESS AT THE FINNISH OPEN UNIVERSITIES

Computer Science
Master's thesis

VAASA 2008

CONTENTS

ABBREVIATIONS

CD-R	Recordable compact disk
DDoS	Distributed Denial of Service
IM	Instant Messaging
IRC	Internet Relay Chat, a form of real-time Internet chat or synchronous conferencing
IS	Information Systems, an organization of data-processing persons, records and activities
key user	Key user's activities are critical to an organization and from personnel security point of view key user should be protected better than a normal user
PC	Personal Computer
P2P	Peer-to-Peer, a type of ad-hoc computer network
SIS	Student information system, also known as student information management system (SIMS, SIM), student records system (SRS) or student management system (SMS)

UNIVERSITY OF VAASA
Faculty of Technology
Author: Kaisa Toivonen
Topic of the Master's Thesis: Information Security Awareness at the Finnish Open Universities
Instructor: Jari Töyli
Degree: Master of Science in Economics and Business Administration
Department: Department of Computer Science
Major Subject: Computer Science
Year of Entering the University: 2002
Year of Completing the Master's Thesis: 2008 **Pages:** 81

ABSTRACT:

The principle research objective of the thesis is to survey the current reality of information security awareness among the personnel of the Finnish Open Universities in the light of recent theory. The thesis follows mainly the theoretic-empirical research method with an influence of a case-research method. The theory part of the thesis progresses from an abstract level towards more concrete issues. First we discuss the principles of information security and introduce privacy and legislation concerning the subject area of the thesis. Secondly, we examine the human factor in information security, the possible risks brought by the personnel and the preventive method, information security training.

The level of user's information security awareness is influenced by several interlocking organizational, technological and individual factors. User's awareness behavior and motivation are influenced by information security management, social norms and interactions at the work place as well as personal factors, such as knowledge, attitude and values. In addition, the level of information security awareness in an organization is greatly dependent on the extent of information security training. Training has to be continuous and originate from the top management.

The results of this thesis give reason to presume that the level of information security awareness among the personnel of Open Universities in Finland is fairly low. The two major possible security threats are trustfulness and carelessness of the employees. In addition, the foundation for information security awareness at the Finnish Open Universities is weak, as information security training is rarely provided for the personnel.

KEYWORDS: Information security, Open University, information security awareness

VAASAN YLIOPISTO
Teknillinen tiedekunta
Tekijä: Kaisa Toivonen
Tutkielman nimi: Information Security Awareness at the Finnish Open Universities
Ohjaajan nimi: Jari Töyli
Tutkinto: Kauppatieteiden maisteri
Laitos: Tietotekniikan laitos
Oppiaine: Tietotekniikka
Opintojen aloitusvuosi: 2002
Tutkielman valmistumisvuosi: 2008 **Sivumäärä:** 81

TIIVISTELMÄ:

Tutkielman päätavoitteena on tutkia avoimen yliopiston henkilöstön tietoturvan tietoisuuden tasoa viimeisimmän teorian pohjalta. Tutkielma perustuu pääasiallisesti teoreettis-empiirisen tutkimusmenetelmän käyttöön, mutta ottaa vaikutteita myös case-tutkimusmetodista. Tutkielman teoriaosa etenee abstraktilta tasolta konkreettisiin aiheisiin. Aluksi esittelemme tietoturvan periaatteet, tietosuojan sekä aihealuetta koskevaa lainsäädäntöä. Seuraavaksi tutkimme ihmisen vaikutusta tietoturvaan, henkilöstön aiheuttamia mahdollisia riskejä sekä ehkäisevää menetelmää, tietoturvakoulutusta.

Käyttäjän tietoturvan tietoisuuden tasoon vaikuttavat useat organisatoriset, teknologiset ja henkilökohtaiset tekijät, jotka ovat vuorovaikutuksessa toistensa kanssa. Käyttäjän tietoiseen käyttäytymiseen ja motivaatioon vaikuttavat tietoturvan johtaminen, sosiaaliset normit ja vuorovaikutukset työpaikalla, mutta myös henkilökohtaiset tekijät, kuten tiedot, asenne ja arvot. Lisäksi tietoturvan tietoisuuden tason organisaatiossa on merkittävästi riippuvainen tietoturvakoulutuksen laajuudesta. Koulutuksen on oltava jatkuvaa ja sen tulee juontaa juurensa johdon sitoutumisesta.

Tutkielman tulokset antavat aihetta olettaa, että tietoisuus tietoturvasta Suomen avoimen yliopistojen henkilöstön keskuudessa on melko alhainen. Kaksi suurinta mahdollista tietoturvauhkaa ovat työntekijöiden luottavaisuus ja ajattelemattomuus. Lisäksi perusta tietoturvallisuuden tietoisuudelle Suomen avoimissa yliopistoissa on heikko, sillä tietoturvakoulutusta tarjotaan henkilöstölle harvoin.

AVAINSANAT: tietoturva, avoin yliopisto, tietoturvan tietoisuus

1. INTRODUCTION

1.1. Background

Information security can not be bought. Money can only help you acquire technical devices, which can assist in increasing the level of information security. Besides external threats, internal abuse of information and risks of obstruction have increased in organizations. According to Järvinen (2002: 47) the real information security is composed of internal trust, correct operational practices, education and carefulness. An employee can intentionally or unintentionally damage an organization and nullify the effect of good security solutions.

The awareness of information security is often underestimated sector of information security management, because time of the people responsible for information security is mostly spent on controlling the security monitors, observing the attempts of breach and evaluating risks. People are often the weakest link in an organization's security chain because they for example have not received proper training and do not know what security means or they do not understand what results their however small actions may have.

1.2. Thesis' Scope and Objective

The study is directed at the administrative personnel of the Finnish Open Universities. The principle research objective is to survey the current reality of information security awareness among the research subjects in the light of recent theory. Our belief is that the level of information security awareness at the Finnish Open Universities is low. The thesis is made from a standpoint that Open Universities do not have trade secrets or confidential information of the

organization that would jeopardize the organizations existence if it leaked outside. Here the most valuable information stored at the Open Universities is considered to be the personal data of students and personnel as well as students' study records.

Information security is a vast subject area. It consists roughly speaking of risks involved with technical information processing and risks resulting from people using the system. The technical issues of information security, which are administered at most Open Universities by the mother Universities' IT departments, are not covered in this thesis. Our assumption is that the technical issues of information security are at the same level at all Open Universities. In this thesis we concentrate on users' individual information security behavior. The study is mainly considering the administrative aspects, and does not discuss users' views on technological security measures. Thus, the main focus is on the human factor of information security.

1.3. Research Methods

The thesis follows mainly the theoretic-empirical research method where theoretic research findings are confirmed with an empirical research. However, the research does have influence also from the case-research method, which is used to examine a single-case.

Theoretic-empirical research means that the research is based on a particular theory. Hypotheses are derived from the theory and their fidelity is tested. Testing is constructed in a form of a questionnaire. The use of a questionnaire as a research method is opportune to situations where the number of questions is few and the number of respondents is large (Järvinen & Järvinen, 2000: 155). A request email to fill in the online questionnaire was sent to 238 administrative personnel at the Open Universities in Finland.

Case-research can be conducted by using questionnaires, interviews, observation and archived material. Thus, the information collected can be either quantitative or qualitative. The nature of case-research can be descriptive, theory-testing or theory-creating research. (Järvinen & Järvinen, 2000: 78.) Open University, if looked at as an undivided institution could be classified a single-case. The discussion of the results of the thesis will be influenced by the fact that the student works at an Open University and has observed the habits of the employees for over a two year period. Therefore, it could be argued that the thesis follows in addition the case-research method.

The research material was collected through an online questionnaire. A request email to fill in a questionnaire was sent to all administrative personnel of 19 Finnish Open Universities. Some of the questions were adapted from questionnaires by Ministry of Finance and by PK-RH project (Valtiovarainministeriö 2006: 102–103, 108–109 and 160; Räsänen 1998: 1–2). Most of the questions are measured using a five-point Likert scale (strongly disagree – strongly agree). In rest of the questions a selection of answers was provided in order to assist the analysis phase. Since the questions were made specifically for this research, we saw the need to test the questions. Therefore, the web-based questionnaire was piloted with administrative personnel of the University of Vaasa Open University. Based on the received feedback, the readability of the questions was improved.

Research questions were designed to support the purpose of the thesis. In the beginning of the questionnaire were background questions, which were used to group the results in the analysis phase. In addition, to aid the analysis of the answers, some questions were asked to find out the access rights of the employees.

With primary research questions, the objective was to map out the security behavior of the employees of Open University and to find out the major black spots and challenges for realizing information security. These aspects were tracked down by asking how employees protect the information handled at work, what is their established practice of password usage, how employees use email and the

Internet, as well as how they perceive their own know-how, attitude, motivation and atmosphere at work community. Finally, employees were asked how the personnel is trained on information security and about security guidelines at work, if there was any.

The research subjects were found through Open University websites, from the personnel section. Some of the respondents represent Managers of Open University, some Planners and Heads of Study Affairs, and some administrative staff. The enquiry was conducted in February – March 2008.

1.4. Previous Studies

The awareness of information security at the Finnish Open University has not been studied previously. Most research on information security in general has focused on technological rather than human issues. Further, most research on human issues take an organizational or managerial perspective rather than a perspective of an end-user. When an end-user is researched, the research is mainly theoretical and seldom empirical. This research paper aims to add to the empirical research conducted on the end-user.

Research publications related to this research topic are presented below shortly. The first publication presented is related to the research topic on a general level and looks at different dimensions of information security awareness. The next two publications are based on studies in the university setting. The fourth publication presents the findings of a general study of end-users' views of information security and the last one talks about employees' IS security policy compliance.

Dimensions of Information Security Awareness (Siponen, Mikko T. & Jorma Kajava 1997)

In their research paper Siponen & Kajava enlarge upon people's level of information security awareness. They argue that people progress upwards or regress downwards on three stages of information security awareness according to their success or failure in IT security awareness. The three stages of information security awareness according to Siponen & Kajava (1997: 6) are:

1. drawing people's attention to security issues
2. getting user acceptance
3. getting users to learn and internalize the necessary information security activities.

Researchers argue that awareness is an aspect whose proportions are not discerned holistically enough (Siponen et. al. 1997: 7). They divide IT security awareness into five borderless dimensions, which are organizational, general public, socio-political, computer ethics and institutional education dimensions. Within the dimensions different target groups should have access only to information relevant to their needs. Thus, information needs to be classified to relevant or irrelevant for each target group. On the whole, researchers emphasize prevention.

Incorporating Information Security into University Infrastructure (Kajava, Jorma & Rauno Varonen 2003)

In their research paper Kajava & Varonen discuss information security at universities. They explain what security awareness program entails and conclude that security awareness should be seen as a key function in our society, that all security solutions include compromises and that instead of always using imperatives in information security, discussion between different user and management groups is needed. They stress that the security programs are needed also at universities, not only in companies.

Data Protection in the University Setting: Employee Perceptions of Student Privacy (Earp, Julia B & Fay C. Payton 2001)

Julia B. Earp and Fay C. Payton from North Carolina State University have studied university employees' perceptions of student privacy. Their findings suggest that university employees are concerned about organizational practices that may result in improper access and unauthorized use of student data. They state that organizational policies that require prescribed level of performance do not always accord with the experience of workers in the collection, access and use of personally identifiable data. They accentuate that worker roles and responsibilities should be clearly defined and integrated with organizational policies.

A Qualitative Study of Users' View on Information Security (Albrechtsen, Eirik 2007)

In his study, Eirik Albrechtsen aims to provide knowledge of users' experience of information security and their individual security role in daily work. Albrechtsen found in his qualitative study that even though users declare to be motivated for information security work, they do not perform many individual security actions. In addition, according to his study, information security assignments generate a conflict of interest between functionality and information security. He found also that instead of general awareness campaigns, users consider a user-involving approach to be much more effective for influencing user awareness and behavior.

Emploees' Behavior towards IS Security Policy Compliance (Pahnila, Seppo, Mikko Siponen & Adam Mahmood 2007)

Researchers have proposed a theoretical model, which contains factors that explain employees' IS security policy compliance. They found that information quality has a substantial effect on actual IS security policy compliance. In addition, they discovered that intention to comply with IS security policies depends greatly on attitude, normative beliefs and habits. Researchers found also that sanction and reward system in the studied organization did not have an effect on attitude towards complying.

1.5. Results

The results of this thesis have given reason to presume that the level of information security awareness among the personnel of Open Universities in Finland is fairly low. The two major possible security threats are trustfulness and carelessness of the employees. In addition, over half of the respondents either did not respond or responded "never" to the question on how often they are given information security training. Over 40 % of the respondents had received information security training less frequently than once a year or only once over their working time at the Open University. Therefore, we can say that the foundation for information security awareness is weak at the Finnish Open Universities.

1.6. Structure of the Thesis

The thesis is divided into five parts: Introduction, theory, results, discussion and conclusions. Theory part progresses from an abstract level towards more concrete issues. First, we discuss the principles of information security and introduce privacy and legislation concerning the subject area of the thesis. Secondly, we examine the human factor in information security by going through what is meant by information security awareness. We discuss the personnel risks in an organization and their prevention method, information security training.

In the results part, we first present the research subjects, go through the techniques used to analyze the data and finally, we present the results. In the sixth chapter we discuss the results in the light of recent theory. The last chapter of the thesis is the conclusion.

2. INFORMATION SECURITY AND PRIVACY

The Ministry of Finance produces guidelines and recommendations on information security for the public administration in Finland. The Ministry of Finance (2005: 7) defines information security as follows: "Information security is an extensive operational entity, and its foundation is formed by the security culture of the organisation and by human actions."

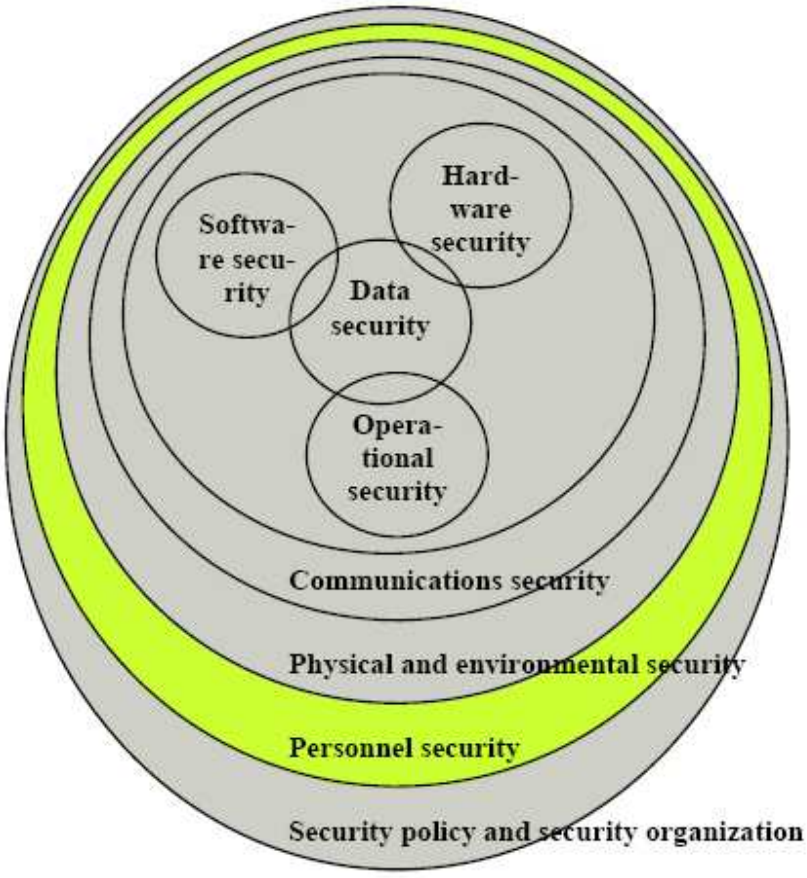

Figure 1. Information security consists of layers.

Information security is presented in a form of a structure diagram in Figure 1. The diagram consists of different layers, which interact with each other in various ways. The layers together constitute the wholeness of security. Layers are presented in more detail in the next three paragraphs.

Data security stands for protection of information, that is, the files within the system. It is the means of ensuring that data is kept confidential, available when needed and safe from corruption and that access to the data is protected (integrity). Thus, data security helps to protect privacy. The three principles of information security: confidentiality, integrity and availability are presented in more detail in the chapter 2.1.

Software security means maintenance of software licenses, protection of programs used within the system and forbiddance of unauthorized use of the programs. Hardware security stands for protection of system devices, such as computers, routers and firewalls. Operational security means that the system is used in a secure manner. Operational security has a direct connection with personnel security, as careless use of the system or use, which doesn't follow guidelines, diminishes operational security. (Ruohonen 2002: 4–5.)

Communications security stands for protection of communications within the system. This means protection of messages within the system network as well as messages travelling in networks outside the system. Physical and environmental security means protection of the physical space where the system resides. Personnel security means protection of the system from threats from the user. Unintentional damages caused by the users can be reduced with sufficient guidance. Intentional damages can be brought down by giving users only the access rights they require and by verifying backgrounds of the key users. The outer layer in Figure 1 contains security policy and security organization, which stand for management of different areas of system security. (Ruohonen 2002: 4–5.)

2.1. The Principles of Information Security

The aim of information security is to protect important information. Therefore, it is necessary to know which and what kind of information is important. In order to protect the information, we need to know the threats and risks that it is faced with. Only then it is possible to find correct protection measures. As information security does not only consider information systems and applications or information in electronic form, orchestration of information security should not be administered only by the IT department, but directly by the management of the organization and thereby management of each sector of the organization. The main factor of information security is not technology, but people management.

According to Kajava (2003b: 6) information security is in some issues almost entirely a technical question, in others mostly a legislative one. Kajava considers both aspects important, but he also points out that the main focus should be on the social and ethical levels of information security.

Information security can be understood as a target state, where information processing fills the following criteria: Confidentiality, integrity and availability. The three factors form the classic definition of information security, a definition, which is based on the value of the information. Information has to stay confidential and available only for the people permitted to access it. It has to stay intact and therefore be protected from illegal changes and additions. In addition, it has to be available when it is needed. (Paananen 2005: 387–388.)

2.1.1. Confidentiality

In order to keep up the confidentiality of information we ensure the privacy of sensitive information by protecting systems with user names and passwords and other access control methods. The information can be available only to those who have a right to access it (Hakala, Vainio & Vuorinen 2006: 4). The purpose is to

prevent intentional or unintentional exposure of information. Confidentiality can be lost in several ways, for instance by unintentionally vouchsafing private information of an organization or as a result of a misuse of access rights for a network. (Krutz, Ronald L. & Russell Dean Vines 2003: 3.)

In order to identify the authorized users, their identity needs to be verified. For the verification process to stay protected, encryption is required. When transferred or saved information is encrypted with a safe enough method, it is not exposed even if someone managed to eavesdrop on the information transfer connection. (Järvinen 2002: 22.)

2.1.2. Integrity

Integrity of information means that no external party is able to change the content of information without permission. External party can be a malfunctioning application or a user, who intentionally or unintentionally makes a mistake. Changing the content of information consists of deletion of files or adding impertinent information to the files. Hakala et al. (2006: 5) state that integrity is pursued mainly by programming solutions. Applications have various input restrictions and verifications such as checksums, log files, information transfer protocols and various internal check-ups built within. These preventive solutions ensure that non-authorized people or processes do not change information, that authorized people or processes make only permitted changes and that internal and external information is consistent. (Järvinen 2002: 22–23; Krutz et al. 2003: 3.)

Integrity of information is important when archiving information. For example the log files connected to the organizations financial information and security systems have to be archived in a manner disabling anyone to change them later. This can be assured by storing the log files into a storage medium, which can be written on only once, for instance a CD-R disc. (Järvinen 2002: 24.)

2.1.3. Availability

Availability is assured by ensuring that systems work accurately, the machines are effective enough and that the software is the best possible choice for processing the saved data (Hakala et al. 2006: 4). In addition, the service should never be refused from authorized users (Caelli, Longley & Shain 1991: 5; Krutz et al. 2003: 3). Here service includes security services, which should be always available for those in need of them.

Availability of a service can be disturbed by intentionally overloading the system. The attacker does not attempt to break in to the system (confidentiality), nor does s/he try to mix up anything (integrity), but by disturbing the system s/he prevents the normal operation of the system. (Järvinen 2002: 24.)

Availability differs from usability, which is presented later in this chapter. Usability can be prevented even if the information is available, if for example a new application can not open an old file format.

2.1.4. Extended Definition of Information Security

According to Hakala et al. (2006: 5) the classic definition of information security is insufficient as it does not consider the identity of the producer, the owner of information or the value of hardware and software. Järvinen (2002: 24–27) presents three additional factors, which are to be fulfilled to achieve information security. Confidentiality requires *authentication* of an entity, which can be a user, a machine or a source of information, internet service or a piece of programming code downloaded from the Internet. Authentication requires the entity to have a certain unique quality, which other similar entities do not possess. Users are usually authenticated by the use of passwords. The use of password is based on assumption that the password is known only to the right person. Authentication is inadequate unless an entity is also authorized to use, for example an IS. Authorization is given by the owner of an IS.

The second additional factor to be fulfilled is *access control*. It is necessary to control that only the authenticated people have access to the information stored in the system. Access control is looked after by the operating system and the application. Access control is in connection with auditing. A system forms an audit trail of users' behavior within the system. It shows who has opened and rewritten files, who has used which programs or in general signed in or out of the system. (Järvinen 2002: 27.)

The final principle of information security according to Järvinen (2002) is *non-repudiation* of performed actions. This is needed especially with electronic commerce where typical phases of a purchase: placing an order, receiving an order and sending an order have to be possible to prove.

Miettinen (1999: 25) complements the definition of information security with *possession*. Possession considers the ability of an individual to process information owned by an organization. He includes also *authenticity* (1999: 27), which means that information is original and has not been falsified, and *usability* (1999: 28), which stands for the fact that information needed within an organization is in a format, which can be opened and used with ease.

Security's weakest point is usually connected with the usability and efficiency of a system. Usability and efficiency require that a customer can use the system as easily as possible. Therefore, usability and security are to some degree mutually exclusive attributes. (Mäkinen 2006: 110.)

2.2. Privacy

Privacy and information security are not mutually exclusive but complementary to each other. According to Miettinen (1999: 23) privacy is a sector of information security, which considers the protection of personal details of people connected to

organization's activities. In short, privacy is a legal term, which means protection and use of personal data.

According to Lantto (1999: 42) privacy consists of those ethical and legal terms under which personally identifiable information that has not been publicly documented can be kept and processed. She continues (1999: 43) that when considering the requirements privacy imposes on processing of personal data, it should be remembered that it is really the case of protecting the privacy of a physical person as a basic right that s/he owns.

The viewpoint on privacy differs between administrative law and law concerning individuals. According to Lantto (1999: 43) this is because privacy has to be matched with the principle of publicity. Thus, the starting point is under public law. On one hand public authorities, for example Universities, have to provide other authorities and outsiders information they are according to the law entitled to receive. On the other hand they have to be able to protect the privacy of customers and prevent exposure of information, which is to be kept secret.

2.2.1. Special Characteristics of Privacy in Electronic Services

Protecting privacy online is a challenging task. Protecting the privacy of a person using electronic services includes confidentiality of electronic communication, secrecy of communication in electronic communications and appropriate processing and protection of information connected to the person. In electronic services one has to take into consideration all aspects of privacy, which are protection of personality, protection of intimacy, and privacy. (Lantto 1999: 44.)

Lantto (1999: 44) states that open information network environment with its information security problems does not justify deviation from privacy protection, but implementation of electronic services has to be postponed until protection of privacy can be ensured in authorities' information systems and in electronic data transfer. Implementation of privacy protection may be different depending on

whether the system contains sensitive personal data or information, which is publicly available such as name and address.

2.2.2. Information Security Risks in Electronic Services

Electronic services of public administration contain all the same privacy risks as traditional services. In addition to those, privacy is directed with specific risks when personal data is transferred in open information networks and stored in information systems that are in connection with open information networks. (Lantto 1999: 44–45.)

If the personnel processing private information are not familiar with regulations concerning handling of personally identifiable information or with operational principles of technical systems, which are implemented to protect privacy, the expensive information security systems are useless. Imperfections in the control of information usage and undefined personally identifiable information processing responsibilities are also threats for privacy protection. (Lantto 1999: 45.)

2.2.3. The Acts Defining Privacy

The main Act, which defines privacy is the Personal Data Act (Henkilötietolaki 01.06.1999/523), which enacts of mechanical processing of personal data. The purpose of the Act is to protect private life and civil rights connected to it, when personal details are handled, as well as to promote development and compliance of good mannered information processing. The Act concerns predominantly mechanical information processing, but also processing and maintenance of information in other means, when the information comprises a person register or a part of one. (Järvinen 2002: 411.)

In practice this means that before an organization collects personal details and forms person registers, it has to clearly specify why information is collected and how it is stored and protected. The document where this is declared is called

person file description. An organization has to determine sources for the information and rules on how the information can be passed on. The main principle of the Act is that the collected information can be used solely for the purpose it was collected for. (Järvinen 2002: 412–413; Miettinen 1999: 249.)

Open University does not collect information on students' health status, political or religious beliefs, sexual orientation or criminal background, which are included within the scope of the Personal Data Act. One piece of information that is within the scope of the Act and collected by the Open University is the personal identity number. According to the Personal Data Act 1999/523 "personal identity number may be processed on the unambiguous consent of the data subject or where so provided in an Act. A personal identity number may also be processed if it is necessary to unambiguously identify the data subject". Personal identity number is an extraordinary piece of personal information as it is the key piece of information for several registers and it enables connecting personal data from different registers (Koskinen, Alapuranen, Heino & Salli 2005: 101).

The second Act presented is the Act on the Protection of Privacy in Electronic Communications (Sähköisen viestinnän tietosuojalaki 16.6.2004/516), whose aim is to protect the confidentiality of communication and privacy protection in electronic communications and to promote information security in electronic communications and development of services in electronic communications. The Act aims to clarify the processing rules of confidential identification information. Its objective is also to clarify the possibilities of execution of information security and it gives rules for the use of cookies and processing of geographic information.

The last Act presented is the Act on Electronic Services and Communication in the Public Sector (Laki sähköisestä asioinnista viranomaistoiminnassa 16.10.2003/13), whose aim is "to improve smoothness and rapidity of services and communication as well as information security in the administration, in the courts and other judicial organs and in the enforcement authorities by promoting the use of electronic data transmission". The Act contains provisions on the rights, duties and

responsibilities of the authorities and their customers in the context of electronic services and communication.

3. HUMAN FACTOR IN INFORMATION SECURITY

Ministry of Finance (2005: 11) states that information security is not only limited to technical solutions, but "it also includes the development of services and the attitudes, knowledge and skills of the users of information technology". Thus, Ministry of Finance emphasizes the importance of human factor in information security. In the following chapters we present the information security awareness, the risks that the personnel may pose on an organization and information security training, which can assist in diminishing the risks.

3.1. Information Security Awareness

Being security aware means understanding that there is a potential for some people to deliberately or accidentally steal, damage, or misuse the data that is stored within organization's computer systems and throughout the organization. According to Krutz et. al. (2003: 25) security awareness means that the personnel of an organization have a general, collective and common awareness of the importance of security and aspects of security control mechanisms. Siponen & Kajava (1998: 327) define information security awareness as a preventive measure, which is aimed at securely constituting correct security procedures and security principles in the minds of all employees.

It has been said that awareness is the best counteractive measure against the biggest weakness in all systems: the human factor. Information security awareness requires always full commitment and example of the top management in order for it to succeed. In addition, building awareness has to be consistent and training for awareness has to be delivered through different means.

Information security awareness consists of three stages. The first stage is arresting people's attention to security issues and trying to get people interested in them.

The second stage involves acquiring user approval. If an organization succeeds in the second stage, it is important to get user's approval also for organization's information security policy. The third stage comprises of getting the users to learn and internalize the necessity of information security measures. (Kajava 2000: 172.)

3.2. Personnel Risks in an Organization

"A chain is only as strong as its weakest link."

According to Bailey (1983: 81) from a system designer's point of view, users' personal factors, such as traits, characteristics or conditions, contribute most, namely 35 %, to the number of errors in data systems. While organizations spend a great deal of time and money fortifying their networks from an outsider threat, they may neglect the threat from within. The fact is that some of the most devastating threats to computer security have come from individuals who were considered trusted insiders. While the full-time employees may be the most obvious insiders, those employees make up a fraction of the individuals organizations should be concerned about. Anyone who has physical or electronic access to the organization poses a potential security risk. In addition to the employees, organizations should consider all of the people who can get past the possible security guard and into the office. These include contract workers, temporary workers, visitors, and service, support and maintenance people. Once they are inside the office walls, they have access to unlocked workstations, paper files, and any passwords or other sensitive data that could be left out in the open. (Coe 2004a.)

The security policies of the organization may not be familiar for the employee. A common problem is employees being ignorant and lacking understanding of general safe computing practices and information system use. However, while employees may be aware of security policies and procedures, all too often they are careless and do not consider how their actions would breach the rules. Their motivation usually is not to exploit, attack or otherwise adversely affect

organization's system, but it could end up badly regardless of motive. A disgruntled employee, or any employee who deliberately intends to cause damage, destroy, or compromise the organization's information, for financial gain, or simply for personal satisfaction, is behaving maliciously. (Coe 2004a.)
A gap in information security may also arise simply from employee's insufficient information technology know-how or a trusting person can be tricked by convincing behavior (Kajava 2003a: 4–5).

Some insiders who pose a threat do not necessarily have physical access to the office. Often it is the *key holders*, those who have access to organizations' internal systems through contract or partnership arrangements with the organization, who can cause the most harm. In order to conduct business with these key holders, they have to have access to the network and are given authorization to be there. (Coe 2004a.)

In order to diminish the threat from employees, organizations should establish strict security policies and develop internal processes to enforce these policies. Through training each user should understand how important it is to follow given guidelines. Training is required also to maintain the achieved level of information security awareness.

3.2.1. Motivation and Attitude

Employee's performance depends on ability, motivation and working conditions. These factors are in continuous interaction with each other. Thus, even if a person is motivated to perform a task, if s/he lacks the ability, performance level will not reach high and vice versa. Motivation tends to be dynamic and last from minutes to weeks while attitude is more static, built-in factor, lasting from months to years. Attitude correlates mainly to the quality of actions, whereas motivation is connected with activity levels. (Siponen & Kajava 1998: 328.)

Siponen & Kajava (1998: 328) divide motivation into external and intrinsic motivation. When considering security guidelines, people often seem to be externally motivated. In the case of intrinsic motivation, people have to feel free to make their own choices concerning their behavior. They need to justify their actions in the light of internal reasons, for example their own ambitions. Fundamentally, the primary deciding factor determining whether someone is intrinsically or externally motivated is self-determination. (Siponen & Kajava 1998: 328.)

An organization is dependent on the attitudes of its employees and their beliefs that the information, which they use, is important and in need of protection (Kajava 2003b: 4). The value of the security software and policies organizations have in place will decrease if employees do not understand their role in maintaining a secure organization. With that in mind, the main reasons behind internal security breaches according to Coe (2004a) are ignorance, carelessness, disregard for security policies and maliciousness. When users are held accountable for the security of information, they are more likely to adhere to the policies and procedures that have been set down (Kajava 2003b: 4).

In addition to motivation and attitude, the behavior of individual end-users also depends on their values, view of life and on a host of social phenomena such as team spirit as well as atmosphere and culture of the organization. Good leadership skills and a healthy organizational culture tend to be important and essential factors when creating basic security awareness. Working conditions play a significant part in this respect. Labour dissatisfaction, for example, can produce immoral behavior among employees and may eventually generate various kinds of security threats. (Siponen & Kajava 1998: 329.)

3.2.2. Social Engineering Methods

Attackers are changing techniques and beginning to manipulate people by appealing to their human nature. They exploit regular characteristics of people,

such as trusting others, laziness, overlooking small discrepancies, assuming someone knows more than they actually do, being willing to help others and the fear of getting in trouble. These techniques are known as social engineering. With just a small amount of truth or facts, an intelligent person can often extract more information from a person or get him or her to perform an activity s/he shouldn't.

Kajava (2003a: 7) divides social engineering into two types. He states that social engineering can be connected to the intruder knowing exactly the structure of the organization and using the information to his/her benefit. It can also be connected to the employees' insufficient knowledge of information technology or information security.

Social engineering methods can take many different forms. Every method is intended to tempt unsuspected users into helping the attacker in to the organization's system – whether it is by opening attachments that will unleash a virus or providing the attacker with sensitive information that will help their efforts. Common social engineering methods according to Coe (2004b) include breach through email attachments, exploiting file sharing or instant messaging. Attackers may also simply request information over the phone.

If an employee opens unsolicited email attachments or does not scan attached documents for a virus before opening them, the organization is vulnerable to virus attacks. In addition, attackers often take advantage of people's trust in file sharing. Several P2P programs today contain "spyware". Spyware allows the author of the program, and other network users, to see what the employee is doing. It enables the program author to observe the employees actions on the Internet, and even use the employee's computer's resources without their knowledge. (Coe 2004b.)

Employees who use IRC and IM services may be lured into downloading and executing malicious software that would allow an intruder to use the systems as attack platforms for launching distributed DDoS attacks. Sometimes attackers also try to make contact with the organization insiders over the phone or in person. An attacker might call an insider and try to get crucial information out of the user by

imitating someone in a position of authority or relevance with an urgent need for the information. (Coe 2004b.)
The only protection against social engineering attacks is to educate and train the personnel.

3.2.3. Data Protection

Today, most critical and personally identifiable information is stored in electronic format. From an operational perspective, storing such information electronically makes it possible to provide quick and efficient services to students by being able to look up and uniquely identify them. However, given that such data is easily accessible, there exists an elevated risk for it to be exposed, either by accident or by a malicious party. (Penido 2007.)

Electronic data is a collection of information particles that is intended to be accessible, with the possibility for it to be modified, duplicated, and deleted by one or many people. Without proper security controls, data can potentially be exposed at any time. This risk can occur as it traverses computer networks, gets input into databases, is modified in SIS, or is printed out on paper. (Penido 2007.)

Data security is particularly important when the data contains financial, health, or personally identifiable information (Penido 2007). If personally identifiable information stored by Open University was to be exposed to a malicious individual, it could lead to identity theft, create unnecessary distress for the data exposure victim, and present a serious problem to the institution that leaked the information.

3.2.4. Passwords

Sometimes employees act in ways that they knowingly go against the security policy. Often this is an effort by employees to make their day-to-day tasks easier. For instance, when employees keep passwords on a piece of paper attached to their

monitors, they are not directly trying to cause harm, but they also know that they are going against policy and their actions could lead to compromise of information. (Coe 2004a.)

Schneier (2000: 136) states that "the whole notion of passwords is based on an oxymoron". The idea of a password is an easily memorable random string. The problem is how to come up with such a construct. If a password is easy to remember, it is something non-random such as "Juuso". If it is random, it is something like "K5d+2w6C", and not easy to remember. If people are forced to use stronger passwords, they feel the need to write them down on a piece of paper simply to remember them. If an average Internet user has about 25 accounts requiring a password (Florêncio & Herley 2007), remembering all of them may prove to be difficult.

According to a study by Dinei Florêncio and Cormac Herley (2007) around 70 percent of all passwords regardless of the length consist of only lower-case letters. Around 20 percent of passwords are purely numeric. According to the study people do not use uppercase and special characters in their passwords almost at all.

3.2.5. Email and Internet

Even though an email message has a protection, which could be related to secrecy of correspondence, abuse has often taken place. It has been proven that even messages containing fairly small amount of information can be useful for an outsider, because it contains email addresses. (Kajava 2000: 164.)

Interception of email addresses has become big business in the world and packets containing hundreds of thousands of email addresses are traded on the cheap (Kajava 2003a: 9). Open Universities should use blind carbon copy address field when sending bulk mail to students in order to protect students' email addresses.

When a user uses the Internet, s/he leaves tracks of his/her actions in the network, to both ends of the chain as well as to all of the servers, which s/he has travelled through, obliviously or knowingly. Even modestly skilled person can find out the tracks of a user in a network and even discover messages.

It is vital for the organization's information security that each employee understands the possibilities of the Internet, but also the threats that come with its use. Preparedness of the personnel should be increased through continuous training. (Kajava 2003a: 9.)

3.3. Information Security Training

> "It must be considered that there is nothing more difficult to carry out, nor more doubtful of success, nor more dangerous to handle, than to initiate a new order of things. For the reformer has enemies in all those who profit by the old order, and only lukewarm defenders in all those who would profit by the new order, this lukewarmness arising partly from fear of their adversaries, who have the laws in their favour; and partly from the incredulity of mankind, who do not truly believe in anything new until they have had the actual experience of it."
>
> Niccolò Machiavelli (1469—1527)

Marcia Layton Turner (2007) presents in her article three types of security training that are generally given at an educational institution. The first type is a general user awareness program that is designed to promote internet safety and security and includes information on how to protect personally identifiable information and prevent identity theft. The focus of the first type of training is on the user's role in protecting a computer system and personally identifiable information. The second type of training is general employee training regarding safe computing and employee responsibility that includes for example effective password development and protection. The third type of training given at educational institutions is specialized training in how to use a specific system at the university.

According to Anttila, Kajava & Miettinen (2003: 8) some researchers claim that knowledge can be divided into two categories, which are data and information (5 %) and tacit knowledge (95 %) (Figure 2.). Explicit information includes printed and electronic material. Tacit information, however, consists of all other forms of information imprinted in human thinking, competence, knowledge, will and wisdom. These aspects have a major influence in all activities within an organization and should be considered when making plans for organization's security. (Anttila et. al. 2003: 8–9.)

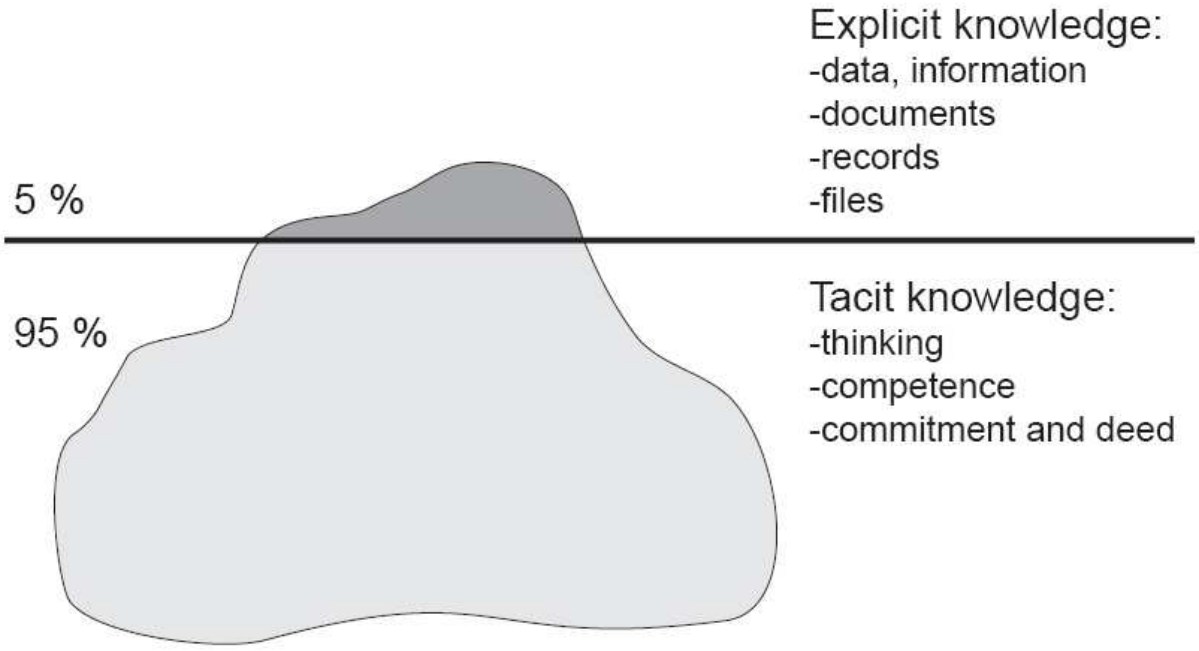

Figure 2. The information to be secured consists of explicit and tacit information (Anttila et. al. 2003: 11).

Information security education is going through a change from technical details to a focus on human factor. Anttila et. al. (2003: 9) believe that in the future, information security awareness will expand in importance and information security education will be mainly based on tacit knowledge. For an organization,

this means stronger co-operation between organizations and a culture that should begin with security education. (Anttila et. al. 2003: 9.)

Anttila et. al. (2003: 11) state that only a small part of information security education consists of teaching new skills and technologies. More vital is to make people understand the importance of the following factors:

- *learning new principles in order to understand operational realities*
- *learning new tools and methodologies*
- *learning new possibilities for constructing innovative infrastructures to get the new ideas implemented* (Anttila et. al. 2003: 11.)

Education and training are simple expedients of directing people's attention to information security issues and gradually, to act accordingly. Therefore, the emphasis in security education should be redirected from mostly technical issues to containing a strong human factor. This can be achieved by raising end-user's awareness level, by increasing their security skills, by respecting the end-user and by considering them more often. (Anttila et. al. 2003: 13.)

Kajava (2000, 159) states that it sometimes seems that information security solutions retard working and in some cases make it bothersome. He continues on to say that if the deeper meaning of the security solutions has not been understood, an employee may think of a way to bypass the security solution and as a result s/he makes the biggest security threats possible. Therefore, user acceptance and internalization should be considered as gradual processes and long-term goals (Siponen & Kajava 1998: 329).

In practice, information security threats resulted from personnel or aimed at it can be controlled by definition of job descriptions and access rights as well as by use of security training and monitoring. Organizations have to define policies in regards to permanent and temporary personnel. That includes job transfers, substitutions and situations when employment commences and finishes. (Kajava 2003a: 4.)

It is also important that training is provided for everyone in the personnel, so that everybody understands at least the basics of information security and its effect on the operational reality of the organization (Miettinen 1999: 158). According to Miettinen (1999: 159) each employee should have a possibility to attend information security training at least every couple of years. This is not always feasible in a large organization but he continues on to say that today with modern technology it is possible to execute a training package online and thereby provide training for all the employees. Kajava (2000: 167) adds that from the end-user's point of view it is important that there are several different information security guidelines, for example one guideline for the use of a computer and another for how to prevent viruses.

4. SUMMARY OF THE FRAMEWORK OF ANALYSIS

The topic of the thesis is information security awareness at the Finnish Open Universities. The topic has been approached by looking into information security and its characteristics through its definitions and going through the legislation, which touches upon the area of the thesis. As another entity we reviewed human factor in information security.

Previous research in the field emphasizes clear definition of user roles and responsibilities and access rights. User involvement in the security work is also stressed. This includes user involvement in both planning of information security in an organization and in the information security training. This is backed up by the fact that even though users declare to be motivated for information security work, they do not behave accordingly. This may be due to the reality that usability and information security are contradictory to each other.

The level of user's information security awareness is influenced by several interlocking organizational, technological and individual factors. User's awareness, behavior and motivation are influenced by information security management, social norms and interactions at the work place as well as personal factors, such as knowledge, attitude and values. Legislation gives guidelines as to what personally identifiable information needs to be protected if it is stored by an organization. It is then another matter whether the guidelines are followed or not.

The level of information security awareness in an organization is greatly dependent on the extent of information security training. Training has to be continuous and originate from the commitment of top management. In addition, user's personal factors such as attitude, motivation and skills have a strong influence on the level of awareness. Atmosphere at the work place has also a significant influence to the level of information security awareness.

As the focus of the thesis is theoretic-empirical with an influence of case-research method, the empirical section is based on the theoretic research. The questionnaire is based on the theoretical findings on human factor in information security and the discussion of the findings is influenced by the theoretical background presented in the thesis as well as by descriptive research, which is common in the case-research method.

5. RESULTS OF THE RESEARCH

The aim of the research was to present the level of information security awareness among the administrative personnel of Open Universities in Finland. The results are intended for the use of Open Universities in Finland and for anyone interested in the subject area. The following chapters will present the results acquired with the use of a questionnaire, which is presented in Finnish in the Appendix 1 and in English in the Appendix 2.

5.1. Research Subjects

The questionnaire was directed to the administrative personnel of 19 Finnish Open Universities. It was answered by 113 respondents, out of which most were females and only one sixth were males (Figure 3.). Response rate was 47,5 %, which is discussed in detail in the chapter 6. The age of the respondents varied with the smallest respondent group being the under 29-year-olds. Age groups of 30–39-year-olds, 40–49-year-olds and 50–65-year-olds had each around 29 % of the respondents (Figure 3.). Descriptive statistics of the respondents are presented in more detail in the Appendix 3. Over half of the respondents were Planners and Heads of Study Affairs, third were Secretaries, Study Advisors and Tutors, 8 % were Managers and one response came from IT personnel (Figure 4.).

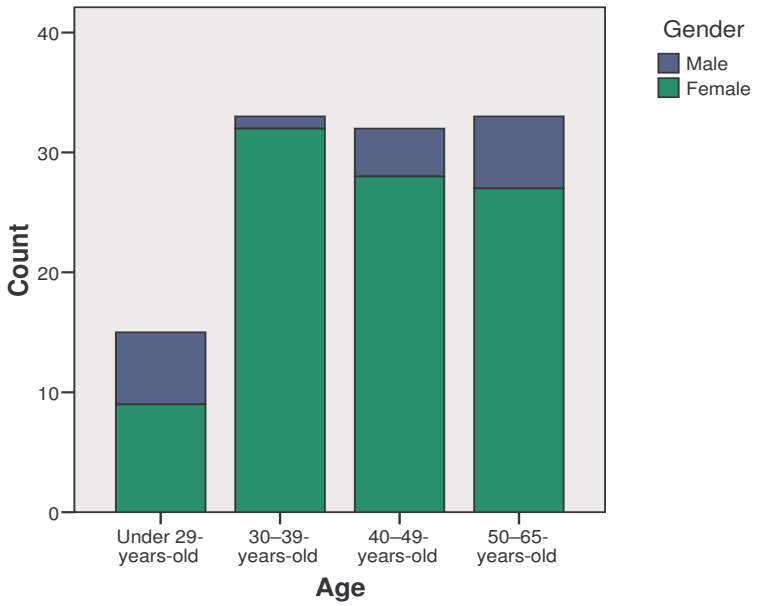

Figure 3. Age and gender of the respondents.

Open Universities were classified as large, medium or small according to the number of administrative employees they had. The personnel of each Open University were looked up through Open Universities' websites. Half of the respondents were from medium-size Open Universities. Little over third were from large Open Universities and 11,5 % from small Open Universities (Figure 4.). Almost all of the respondents had worked at Open University for over a year, out of which three fourths for over three years and one sixth for one to three years. Only about 9 % had worked at Open University for less than a year (Figure 5.). Majority of the respondents were permanent staff (Figure 5.) and 22 % of the respondents were not able to share their duties with anyone (Figure 6.).

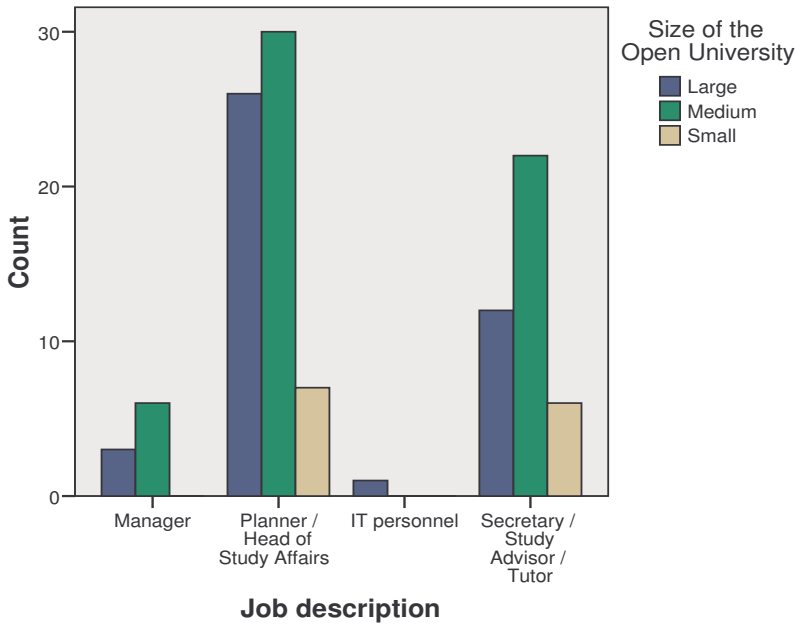

Figure 4. Job descriptions and distribution of respondents according to the size of the Open University.

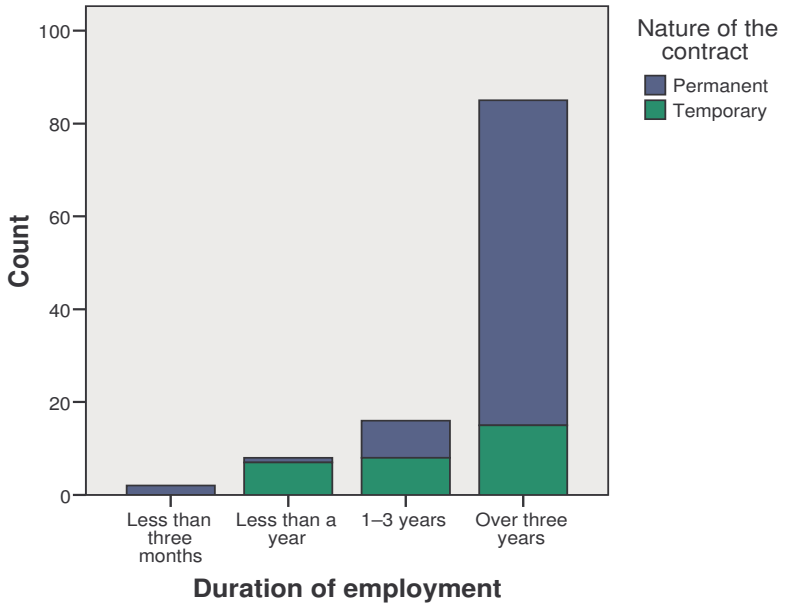

Figure 5. Nature of contract and duration of employment.

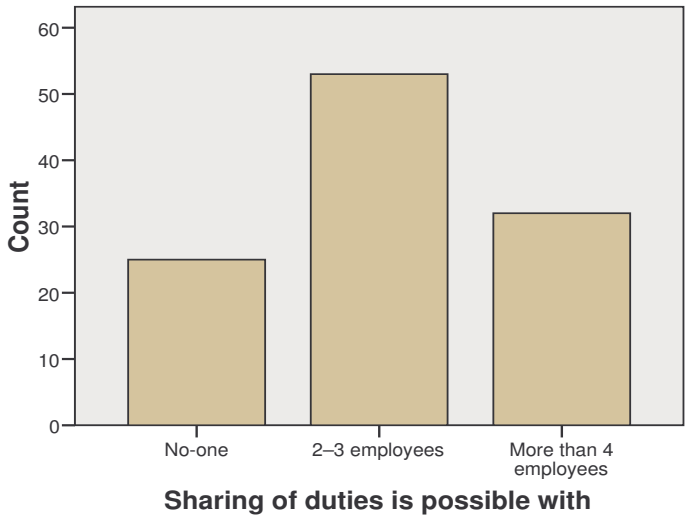

Figure 6. Possibility to share duties with colleagues.

When asking about personnel's right to rewrite personally identifiable data or user names and passwords we found out that almost all of the respondents have access to students' personally identifiable information, such as personal identity number, name and address (Table 1.). Little over half of those were Planners, around third was Secretaries, Study Advisors and Tutors and 6 % belonged to the management level of personnel. Majority of the respondents had worked at Open University for over three years and one sixth for one to three years. Only small number of them had worked at Open University for a less than a year. Most of them were permanent staff, with less than a third on a temporary contract. A quarter of the respondents who had access to students' personal details, could not share their duties with anyone. Frequency tables of the respondents' qualities are presented in the Appendix 3.

Over half of the respondents had a possibility to rewrite students' personally identifiable information (Table 1). About half of them were Secretaries, Study Advisors and Tutors and roughly another half were Planners. Most of them had worked at Open University for over three years, one fifth for one to three years and 6 % for under a year. A little less than third of them had a temporary contract and

the rest of them were permanent staff. One fifth of them could not share their duties with anyone.

One sixth of the respondents could find out colleagues' user names and passwords (Table 1.). Majority of them were Planners and Secretaries, both with equal share. One sixth were Managers and 6 % IT personnel. Most of them had worked at Open University for over three years and were permanent staff.

Table 1. Personnel's access rights.

Access rights	yes	no	total	yes %	no %
Access to students' personal details	104	9	113	92,0	8,0
Right to change students' personal details	68	45	113	60,2	39,8
Access to personnel's user names and passwords	16	97	113	14,2	85,8
Right to change user name or password for personnel	6	107	113	5,3	94,7

Six of the respondents were able to change colleague's user name and password to a system that stores students' personally identifiable information (Table 1.). Two of them were Planners, one was IT personnel and three were Secretaries. They had all worked at Open University for over a year, five of them for over three years. They were all permanent staff members of Open University.

5.2. Techniques for Analyzing Data

Descriptive statistics are used in the thesis to describe the basic features of the data. They provide simple summaries and together with simple graphics analysis, they form the basis of the quantitative analysis of data. Frequencies of data present the exact occurrence of items and their relationships with other items. Standard deviation is a measure, which shows how spread out the data is about the mean value. Thus, it measures the variability of the data. Standard deviation is useful in

comparing sets of data, which may have the same mean, but a different range. If a set has a low standard deviation, values are not very spread out.

Correlation analysis is used to describe the degree of relationship between two variables. The most common measure of correlation is the Pearson's correlation, which is used in the thesis. It reflects the degree of linear relationship between two variables and ranges from +1 to -1. A correlation of +1 means that there is a perfect positive linear relationship between the two variables. In addition to Pearson's correlation, we have used partial correlation, which is a procedure that allows us to determine what the correlation between any two variables would be, if the third variable was held constant.

5.3. Protection of Information

Most of the respondents would check the personal identity number with a student on the phone (Table 2.). However, three of the respondents selecting "strongly agree", stated in the comments that they would have checked the personal identity number with a student on the phone only, if the student was the one revealing the personal identity number and not the other way round. A respondent, who selected "agree", stated in the comments that she had been advised to check the possible missing or faulty personal identity number of a student by phone. The same person selected "strongly disagree" to the question on whether the personal identity number may be checked by email, and commented that "the use of email [in this context] is forbidden". One person selecting "strongly agree" stated in the comments that she would have not sent the whole personal identity number by email. Most of the respondents declined verifying the personal identity number with a student by email. However, 15 % of the respondents selected "strongly agree" to the question (Table 3.).

Table 2. Will to verify the personal identity number with a student on the phone.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	27	23,9	24,8	24,8
	Disagree	13	11,5	11,9	36,7
	Neither agree nor disagree	8	7,1	7,3	44,0
	Agree	14	12,4	12,8	56,9
	Strongly agree	47	41,6	43,1	100,0
	Total	109	96,5	100,0	
Missing	System	4	3,5		
Total		113	100,0		

Table 3. Will to verify the personal identity number with a student by email.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	59	52,2	54,1	54,1
	Disagree	15	13,3	13,8	67,9
	Neither agree nor disagree	11	9,7	10,1	78,0
	Agree	7	6,2	6,4	84,4
	Strongly agree	17	15,0	15,6	100,0
	Total	109	96,5	100,0	
Missing	System	4	3,5		
Total		113	100,0		

Almost 60 % of the respondents stated that the keys to the office were held only by those who also had the right to access the information stored at the office. However, over 40 % stated the contrary or they stated in the comments that they were not certain of who had the keys to the office. Almost half of the respondents did not lock their PC when they were not by it. 28 % of the respondents did not lock their office door when they left the office for a short while. Even students, contract workers, and maintenance people pose a possible security threat, as when inside the office walls, they have access to any unlocked workstations or documents and passwords left out in the open.

Over third of all respondents had outsiders coming to their office daily. People who did not lock their PCs or office doors when leaving the office for a short while

and had outsiders coming to their office daily represent 12 % of all the respondents. They are all females and represent all age groups. They represent 11 % of all management level respondents, 11 % of all Planners and 15 % of the Secretaries (Table 4.). They stand for 2 % of all respondents from large Open Universities and 22 % of all respondents from medium-size Open Universities. They represent 12,5 % of all the people who have worked at an Open University for one to three years and 14 % of all the people who have worked for over three years (Table 5.). They consist of 12 % of all the permanent staff and 13 % of all the personnel on a temporary contract. All of them had access to students' personal details and only two of them were unable to rewrite the details. In addition, two of them had access to personnel's user names and passwords.

Table 4. Job description of the respondents who did not lock their PCs or office doors and had outsiders coming to the office daily.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Manager	1	7,1	7,1	7,1
	Planner / Head of Study Affairs	7	50,0	50,0	57,1
	Secretary / Study Advisor / Tutor	6	42,9	42,9	100,0
	Total	14	100,0	100,0	

Table 5. Duration of employment of the respondents who did not lock their PCs or office doors and had outsiders coming to the office daily.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1–3 years	2	14,3	14,3	14,3
	Over three years	12	85,7	85,7	100,0
	Total	14	100,0	100,0	

Almost everyone locked the office door when leaving for a longer period of time. Around 10 % of the respondents did not shut down or log off of their PC when leaving the work place for a longer time. About 6 % of people did not always leave the programs they used according to the instructions. The respondents who did

not log off of the programs according to the instructions may complicate their and other users' attempts to connect to the system. For example, on a remote access computer programs may stay running and documents may be damaged. Availability of information may be threatened due to an abnormal logging out of a program.

Table 6. Never leaving documents with students' personal information to My Documents or Desktop.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	6	5,3	5,4	5,4
	Disagree	11	9,7	9,8	15,2
	Neither agree nor disagree	7	6,2	6,3	21,4
	Agree	34	30,1	30,4	51,8
	Strongly agree	54	47,8	48,2	100,0
	Total	112	99,1	100,0	
Missing	System	1	,9		
Total		113	100,0		

15 % of the respondents may leave documents with students' personal details stored in to My Documents or Desktop (Table 6.). Seven of them do not lock their PCs or office doors when leaving the office for a short while and have outsiders coming to the office daily. Out of these they all have access to students' personal details and only one of them does not have the right to rewrite data. Most of them have worked at the Open University for over three years. They represent 11 % of the management level respondents, 6 % of all Planners and 5 % of all Secretaries. They represent large and medium-size Open Universities.

42 % of the respondents may have kept documents with students' personal details on their desk (Table 7.). Ten of them do not lock their PCs or office doors when leaving the office for a short while and have outsiders coming to the office daily. Out of these they all have access to students' personal details and only one of them does not have the right to rewrite data. Most of them have worked at the Open University for over three years. They represent 11 % of the management level

respondents, 8 % of all Planners and 10 % of all Secretaries. The respondents were from large and medium-size Open Universities.

Table 7. Keeping documents with students' personal information on desk.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	28	24,8	25,0	25,0
	Disagree	24	21,2	21,4	46,4
	Neither agree nor disagree	12	10,6	10,7	57,1
	Agree	37	32,7	33,0	90,2
	Strongly agree	11	9,7	9,8	100,0
	Total	112	99,1	100,0	
Missing	System	1	,9		
Total		113	100,0		

4,5 % of all respondents threw away documents containing students' personal details. Two people would have let an outsider to use their PC even if they were not sure of the person's identity and access right. 43 % of the respondents did not run a virus check on an unknown memory stick or a floppy disc. 16 % did neither disagree nor agree to the question whether they would run a virus check on an unknown memory stick or a floppy disc. The reason for asking the question was to measure the level of employees' awareness of their actions. Usually virus check is run automatically on external devices, for example memory sticks.

5.4. User Names and Passwords

Almost 70 % of the respondents would have let an IT support person to use their computer with them still logged on with their user name and password. Some of the people commented that they would have allowed it only if it was for testing or stated that they always stood next to the IT support person while s/he was using their computer. Some people stated that they would have done exactly what the IT support person asked them to do. 15 % of the respondents would have given their

user name and password to an IT support person (Table 8.). One of them stated that she did exactly what the IT support person asked her to do.

Table 8. Will to give user name and password to an IT support person.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	64	56,6	56,6	56,6
	Disagree	21	18,6	18,6	75,2
	Neither agree or disagree	11	9,7	9,7	85,0
	Agree	7	6,2	6,2	91,2
	Strongly agree	10	8,8	8,8	100,0
	Total	113	100,0	100,0	

Most of the respondents (over 80 %) believed that they used long and difficult enough passwords. In addition, over 90 % of the respondents stated that they kept passwords in a safe place and did not give them to anyone else. However, quarter of the respondents admitted that they kept passwords written on a piece of paper in the office (Table 9.). Around 19 % of the respondents who believed that they stored passwords in a safe place also stated that they stored their passwords written on a piece of paper in their office. Over 80 % of these are over 40-years-old. They are all female and 13,6 % of them are Managers, 36,4 % belong to the Planners and half of them are Secretaries. Over half of them are from medium-size Open Universities, around 36 % are from large Open Universities and one from a small Open University. Over 80 % of them have worked at the Open University for over three years and almost everyone is on a permanent contract. Only one of them does not have access to students' personal details and over 60 % of them are able to rewrite the details. By writing a password on a piece of paper employees are often not directly trying to cause harm, but only trying to make their day-to-day tasks easier.

Table 9. Keeping passwords written on a piece of paper in the office.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	62	54,9	54,9	54,9
	Disagree	15	13,3	13,3	68,1
	Neither agree or disagree	9	8,0	8,0	76,1
	Agree	17	15,0	15,0	91,2
	Strongly agree	10	8,8	8,8	100,0
	Total	113	100,0	100,0	

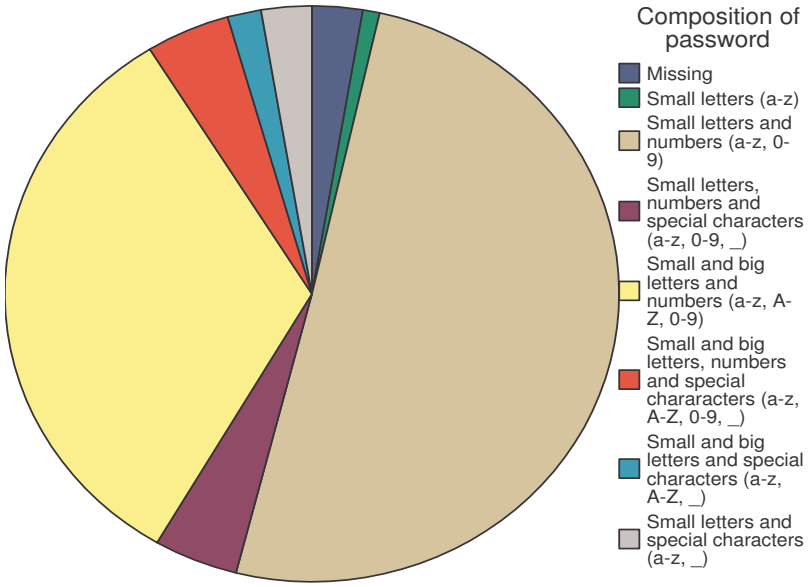

Figure 7. Composition of password.

Over two thirds of the respondents stated that they only entered their password from a trusted computer. 80% of the respondents confirmed that they did not let people to look over their shoulder while they were processing sensitive data or keying a password. Half of the respondents' password consisted of lower-case letters and numbers. Another large group, around 33 % of respondents had a password, which consisted of lower-case and uppercase letters and numbers (Figure 7.). According to the Ministry of Finance (2003: 14) a good password consists of uppercase and lower-case letters, numbers and even special characters.

Most of the respondents changed their password when the system reminded them. 13,5 % of the respondents changed it more often and around ten percent less frequently. Having a large number of passwords for different applications tend to force the user to simplify the passwords or write them down. In the case of Open University, it seems that to some degree, both options are in use.

5.5. Email and Internet

Around fifth of the respondents would have opened a link in an email message arriving from an unknown address, if the message was interesting enough. 60 % of the respondents used work email also for personal communication. 40 % of the respondents declined setting an automated holiday response to their work email. Over half of the respondents stated that they did use an automated holiday message in their work email when on holiday. The reason for setting an automated holiday message was a will to provide good customer service. Some of the respondents stated that the message was forwarded only to the addresses within the university. Some stated that setting an automated message was forbidden by the organization. Setting an automated holiday message, which is forwarded to all senders, confirms to the possible spam mail sender that the email account is in use.

21 % of the respondents may have at times directed their work email to their personal email. Most of the respondents declined ever doing so. Over 90 % of the respondents stated that colleagues did not have access to their email account and one out of the four people stating the opposite was guessing that IT support had access to her email account.

Over 80 % of the respondents used the Internet several times a day (Figure 8.). The Internet was used mainly for work related information retrieval and communication. The respondents used the Internet also for random surfing, for searching information on their hobbies and for chatting (Figure 9.). When using the

Internet, users leave tracks on their actions in the network that can be found out even by a modestly skilled person.

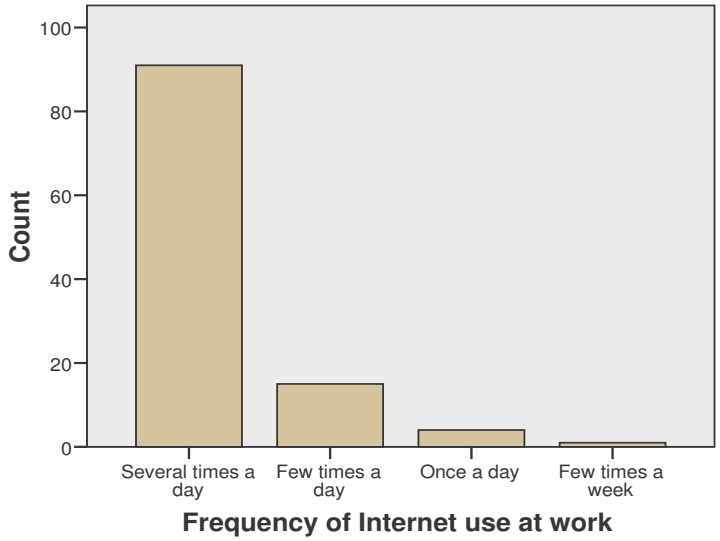

Figure 8. Frequency of Internet use at work.

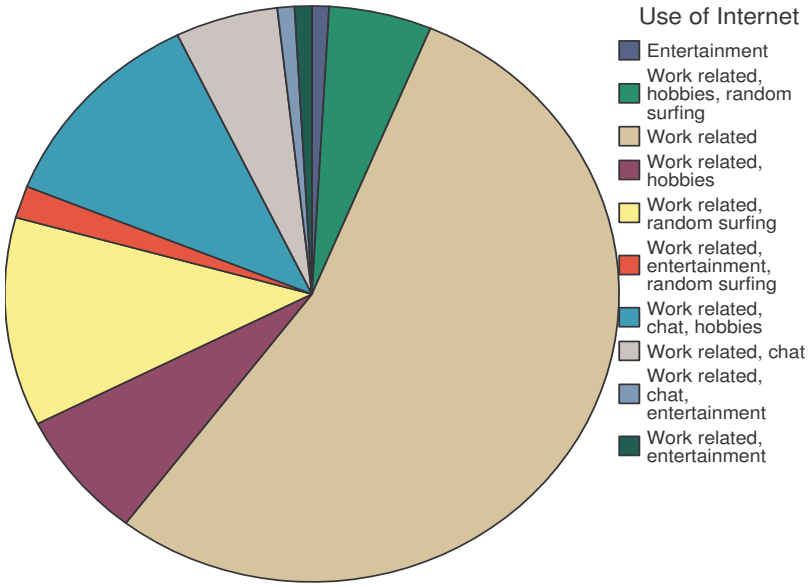

Figure 9. Use of Internet.

5.6. Motivation and Attitude

Most of the respondents agreed to have a sufficient level of education to fill the requirements of their current job (Figure 10.). However, some of the respondents stated that further training is always needed.

Almost 90 % of the respondents stated that they found new things as challenges at work. Around 85 % of the respondents found that they adapt easily to the use of new tools at work. With new tools we mean new systems or programs. Most of the respondents wanted to develop and learn new at work (Table 10.). They were also happy to help colleagues to solve problem situations. Most of the respondents stated that they found work satisfying.

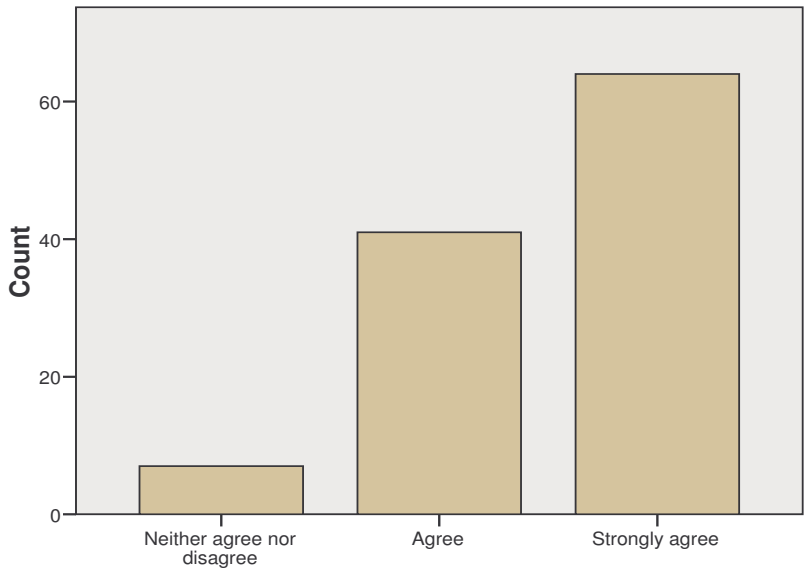

Figure 10. Sufficient education for current job.

Table 10. Descriptive statistics of will to develop and learn new, will to help colleagues and work satisfaction.

	Mean	Std. Deviation	N
Will to develop and learn new	4,50	,646	110
Will to help colleagues	4,50	,554	110
Work satisfaction	4,07	,786	110

The correlation between will to develop and learn new and will to help colleagues when general work satisfaction is maintained constant is not significant (df > 0.05) (Table 11.). The four respondents who did not find work satisfying are all from medium-size Open Universities and have access to students' personal details. Unsatisfied employees may pose a security threat to an organization.

Table 11. Partial correlation coefficients when controlling for work satisfaction.

Control Variables			Will to develop and learn new	Will to help colleagues
Work satisfaction	Will to develop and learn new	Correlation	1,000	,361
		Significance (2-tailed)	.	,000
		df	0	107
	Will to help colleagues	Correlation	,361	1,000
		Significance (2-tailed)	,000	.
		df	107	0

Most of the respondents did not find their work tiresome (Figure 11.). 33 % of the respondents finding work tiresome are Planners, 44 % belong to Managers and 17,6 % are Secretaries (Table 12.). 33 % of them are from large Open Universities, 26 % are from medium-size Open Universities and 23 % are from small Open Universities. Three fourths of people finding work tiresome have worked as a permanent staff for over three years. Almost all of them have access to students' personal details and about half of them are able to rewrite the personal details of students. In addition, three respondents have access to personnel's user names and passwords and one is able to change them.

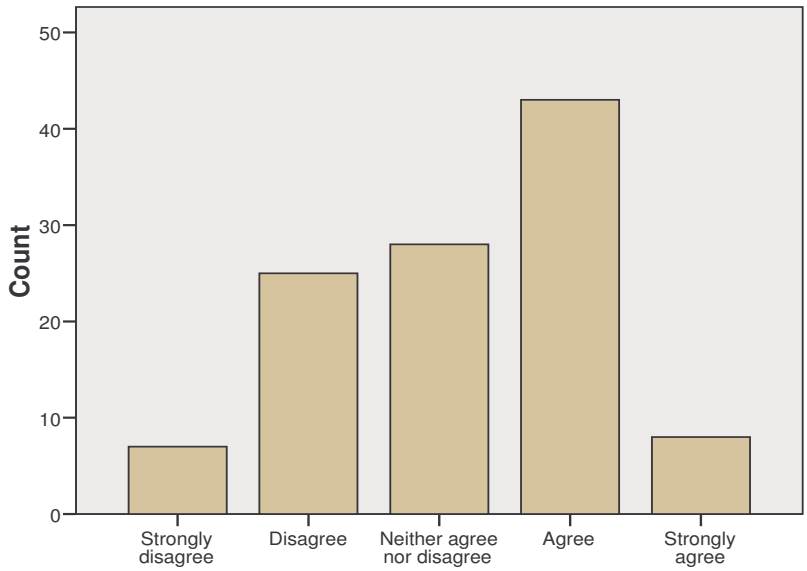

Figure 11. Work is not tiresome.

Table 12. Job description of those finding work tiresome.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Manager	4	12,5	12,5	12,5
	Planner / Head of Study Affairs	21	65,6	65,6	78,1
	Secretary / Study Advisor / Tutor	7	21,9	21,9	100,0
	Total	32	100,0	100,0	

Most of the respondents agreed to having received enough information from Managers in order for them to perform well in their jobs. However, 9 % of the respondents stated that they would have required more information from Managers for them to perform well. One respondent commented that Managers were distant, but she was more content with the immediate Supervisors. 22 % of the respondents did neither agree nor disagree to the question. Some of the respondents whose opinion was "neither agree nor disagree", stated that receiving enough information from Managers was not consistent and called for

improvement of communications. Good leadership skills and healthy working environment create a good foundation for information security awareness.

Only around 4 % of the respondents did not have a good relationship with their colleagues. A little over tenth of the respondents did not however either agree or disagree to the question whether the relationships between the colleagues were good. The relationship between receiving enough information from Managers and colleagues and good relationships among colleagues is significant and positive linear relationship (Table 13.). The relationship is strongest between receiving enough information from Managers and receiving enough information from colleagues. Thus, most of the respondents who thought they received enough information from Managers also found that they received enough information from the colleagues. The positive linear relationship is still significant between good relationships among colleagues and receiving enough information from Managers, but it is not as strong.

Table 13. Correlation between good relationships at work and whether enough information was received from Managers and colleagues.

		Receiving enough information from Managers	Receiving enough information from colleagues	Good relationships between colleagues
Receiving enough information from Managers	Pearson Correlation	1	,609(**)	,294(**)
	Sig. (2-tailed)		,000	,002
	N	111	111	111
Receiving enough information from colleagues	Pearson Correlation	,609(**)	1	,454(**)
	Sig. (2-tailed)	,000		,000
	N	111	111	111
Good relationships between colleagues	Pearson Correlation	,294(**)	,454(**)	1
	Sig. (2-tailed)	,002	,000	
	N	111	111	111

** Correlation is significant at the 0.01 level (2-tailed).

5.7. Information Security Guidelines and Training

Around 80 % of the respondents stated that the personnel were trained to use the systems that were in use at the Open University (Figure 12.). Some of the respondents commented not having received any formal training for using the systems. Information security training was received by around 24 % of the respondents (Figure 13.). Around 30 % of the respondents declined having received any information security training and around 44 % of the respondents did nor agree or disagree to having received information security training. Respondents who selected "agree" or "strongly agree" were requested to state the nature of information security training they had received. Most of the respondents who had received information security training had received it in a form of a lecture or as assistance from an IT support person. Rest of the respondents had received information security training at new programs' introduction training session or in a form of written guidelines.

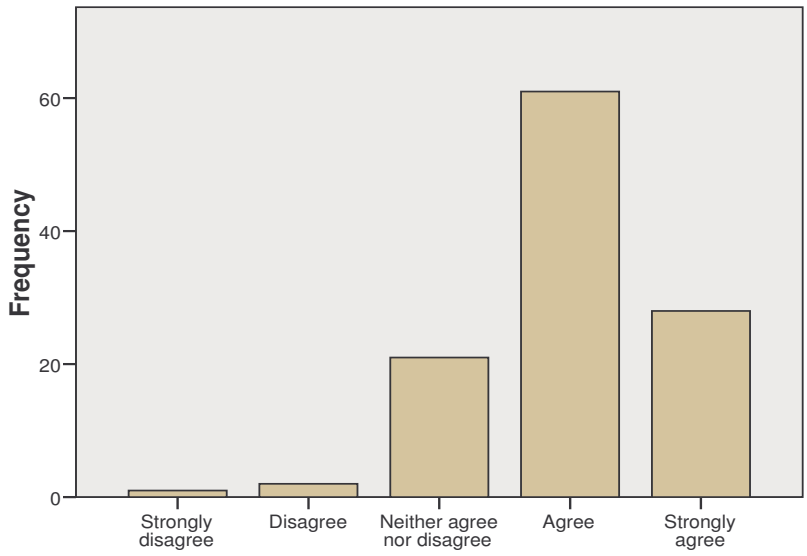

Figure 12. Personnel was trained to use the systems.

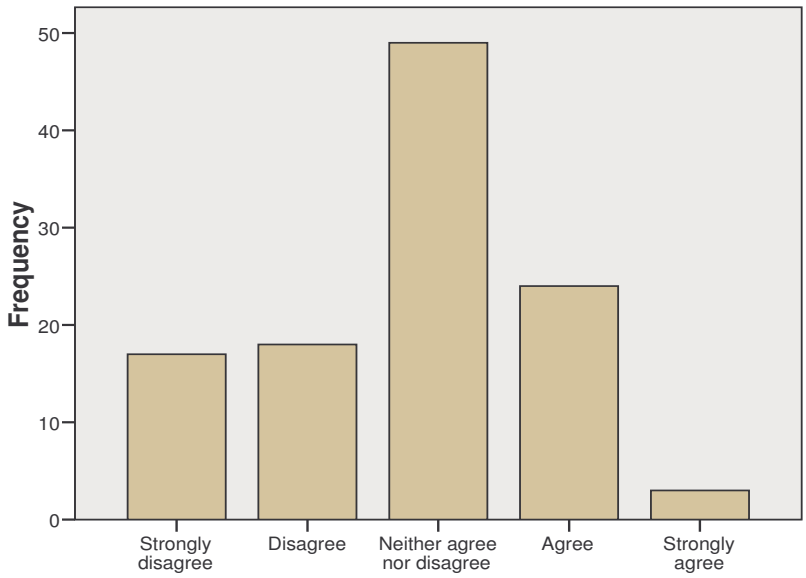

Figure 13. Personnel had received information security training.

Over half of the respondents stated that they had never received any kind of information security training or chose not to respond to the question on the frequency of information security training (Figure 14). Around 20 % of the respondents stated that they had received information security training less often than once a year. Roughly another 20 % stated that they had received information security training only once. Only around 8 % of the respondents replied that they had received information security training once a year or more frequently.

Almost 40 % of the respondents stated that new employees did not receive information security training in the beginning of their employment (Figure 15.). Around 44 % did not agree nor disagree to the question and only around 16 % stated that new employees did in fact receive information security training in the beginning of their employment. 15 % of the respondents stated that information security guideline was provided for the personnel (Figure 16.). Around 32 % stated that there was no information security guideline for the personnel and over half of the respondents were not certain of it.

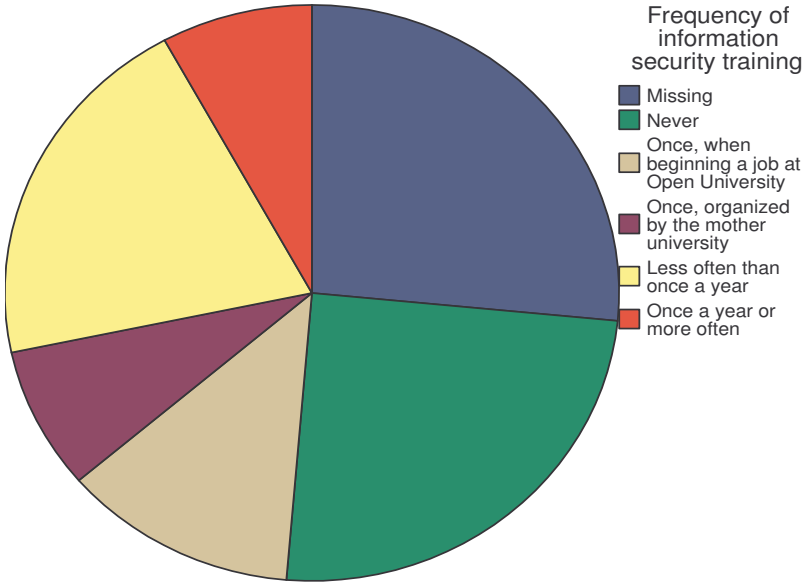

Figure 14. Frequency of information security training at Open University.

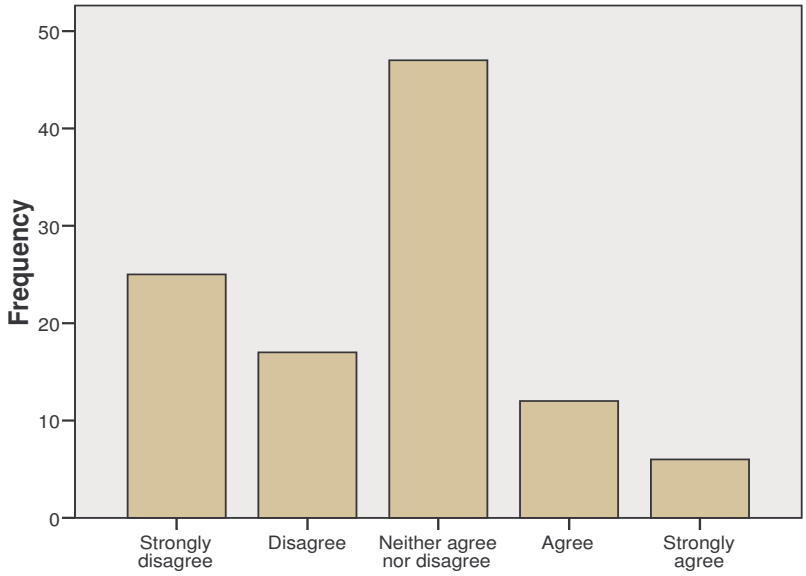

Figure 15. New employees receiving information security training.

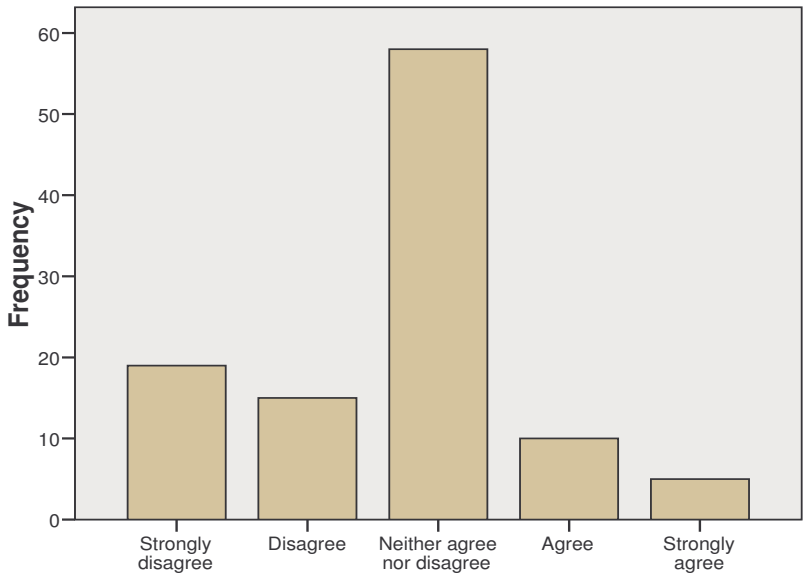

Figure 16. Information security guideline was provided for the personnel.

The answers to the question on preference of information security training method were spread (Figure 17.). Most of the respondents, 42 %, would have preferred training in small group environment. A lecture was a preferred method of training by 27 % of the respondents. Training through intranet was preferred by 9 %, bulletins through email by 8 % and personal training by 7 % of the respondents.

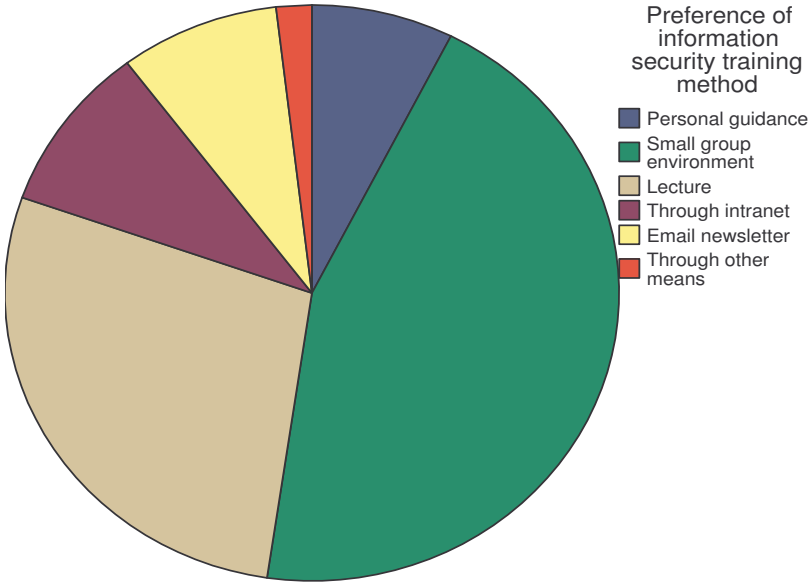

Figure 17. Preference of information security training method.

6. DISCUSSION

The major security awareness issues affecting the level of information security at Open Universities in Finland are collected in Table 14. The table contains issues, which most clearly present the level of information security awareness at the Open Universities. Another requirement for the issues in the table was at least 10 % representation of the responses.

Table 14. Security awareness issues affecting the level of information security at Open Universities.

			Size of Open University		
Security awareness issues	**Frequency**	**Percent**	**Large**	**Medium**	**Small**
Willing to verify the personal identity number with a student on the phone	61	**54,0**	21	33	7
Willing to verify the personal identity number with a student by email	24	**21,2**	6	17	1
Not locking the PC when not by it	52	**46,0**	20	29	3
Not locking the office door when leaving for a short time	32	**28,3**	10	20	2
Not locking the PC or office door when leaving the office for a short time and having outsiders coming to the office daily	14	**12,4**	1	13	0
Keeping documents with students' personal information on the desk	48	**42,5**	15	29	4
Letting an IT support person to use PC with my user name and password	79	**69,9**	31	39	9
Giving an IT support person my user name and password	17	**15,0**	7	10	0
Believes to store passwords in a safe place but keeps them written on a piece of paper in the office	22	**19,5**	8	13	1
Willing to open a link in an email from an unknown address if the message is interesting enough	23	**20,4**	5	16	2
Total number of respondents	**113**	**100**	**42**	**58**	**13**

The results in Table 14 show the issues, which threaten the confidentiality, integrity and availability of information at the Finnish Open Universities. One of

the biggest possible security threats at the Open University is the trust of the personnel in the student to be the one s/he claims to be as well as in an IT support person even to the extent of giving them own user name and password. However, in the case of an IT support person we must consider the fact that at many Open Universities the turnover of employees is not high and that people know each other. In addition, it is common that IT personnel are bound by professional secrecy. However, we do not suppose what might happen in the worst case, but we consider different possibilities for accidents due to the level of employees' awareness of their actions.

Another major possible security threat at the Open University is carelessness of the employees. Almost half of the respondents do not lock their PCs and almost third of the respondents do not lock the office door when leaving the office for a short period of time. Out of these, over 12 % of the respondents have outsiders coming to the office daily. All of them have access to students' personal details and only two of them are unable to rewrite the details. In addition, two of them have access to personnel's user names and passwords. An outsider can have easy access to an unlocked PC of 12 % of the respondents if s/he is patient and smart enough. Fifth of the respondents state that they keep passwords stored in a safe place even though they admit keeping them written on a piece of paper in the office. Another fifth of the respondents would open a link in an email arriving from an unknown address if the message of the email was interesting enough. Over 40 % of the respondents keep documents containing students' personal information on their desks. Some of them, however, state that it is usually only for a short period of time or that the door is locked when the room is unoccupied.

Personnel of the Open University do use fairly difficult passwords. Florêncio & Herley (2007) found in their research that around 70 % of all passwords consist of only lower-case letters. According to the results of this thesis, half of the respondents use passwords, which contain lower-case letters and numbers and around third of the respondents use passwords that contain lower-case letters, uppercase letters and numbers. However, as a result of observation of the habits of the personnel of the Open University of the University of Vaasa, we can state that

the password is often a name of a relative and it is also written down on a piece of paper.

Most of the respondents have only access to their own email account. This is important, as an email message has a protection, which could be related to secrecy of correspondence. Internet usage is frequent at the Open University. The Internet is mainly used for work related information retrieval and communication, but also for random surfing. Surfing on the Internet can be tracked down and even messages may be discovered by a modestly skilled person.

Motivation of the personnel does not pose a significant threat to the information security of Open Universities. The personnel are mainly content with their jobs. The main possible security threats resulting from the personnel at the Open Universities are trust in others and carelessness. Trust can be exploited with the use of social engineering methods. Carelessness may provide even a good-hearted student with a possibility to have access to, for example employee's password or other students' personal details or study records.

The comments to questions on whether the respondent would verify the personal identity number of a student by phone or by email suggest that the questions should have been formulated better. Although majority of the respondents stated to be willing to verify the personal identity number with a student on the phone, we can not expect that all of them would have given the personal identity number to the student, but would have possibly demanded the student to give it to the respondent. However, we can expect that among the majority of the respondents can be found those, who actually would have given the personal identity number to a student, who the respondent expected to be the holder of the identity. Therefore, instructions on how to behave in such a situation should be made clear and given to everyone.

Interestingly, there were a large number of "neither agree nor disagree" -answers to the questions on information security training. This suggests that the respondents do not know whether an organization has provided information

security training or not. Another possibility is that the respondents do not know what information security training entails. When the respondents were asked about the frequency of information security training, over half of the respondents chose not to respond or simply stated that they had never received any kind of information security training. When the respondents were asked how they would prefer to receive information security training, the question received divided answers. Not everyone wants to be trained by the same methods. Kajava & Varonen (2003: 16) point out in their paper that until every end-user is taking part in the organization's security work, there is no information security.

People who choose not to respond to a questionnaire create distortion, which may be systematic if it is focused on a particular group of people. It may be that particular types of people did not answer at all. Response rate to the questionnaire was 47,5 %. Response rate in small and medium-size Open Universities was however, over 60 %, but only third of the employees from large Open Universities responded to the questionnaire. Therefore, the results of large Open Universities are not completely comparable with the two other groups. They can be, however, examined as individual groups, as we have done. The results may be generalized to apply to the small and medium-size Open Universities, but due to the fairly low response rate of the personnel of large Open Universities, their results may only be considered as suggestive. It would have been useful to study Open Universities individually, and not when divided into small, medium and large. This would have given more representative description of the Open Universities where response rate was high.

It would have been extremely interesting to compare Open Universities with each other. However, some Open Universities only have two or three staff members and it would have been easy to connect the answer to the respondent in the results of the small Open Universities. Thus, we thought it would reduce the number of responses. With hindsight, small Open Universities could have been grouped together and all large and medium-size Open Universities could have been left on their own. This would have eliminated the risk of recognition and would have made the results more interesting.

Open Universities in Finland should give more focus on raising the awareness of information security among the personnel. Open Universities handle sensitive private data of students that is ordered by the law to be protected. Raising the awareness of personnel is, however, not enough. The personnel are also required to comply with security policies and guidelines. Employees' attitudes and practices should not be in conflict with organization's privacy policies.

Building awareness of information security in an organization has to begin with the commitment of the management and should cater for all kinds of people with various requirements for training methods. The review of organization's information security should begin with finding out the vulnerable areas, mapping the threats that the areas are faced with and clarifying the probabilities of the threats. Every organization needs information security guidelines for the personnel. In a small or middle-sized organization, commitment of each employee should be emphasized as small organizations do not usually have own information security personnel.

7. CONCLUSIONS

The objective of the thesis was to present the current level of information security awareness at the Finnish Open Universities in the light of recent theory. The belief was that the information security awareness at the Finnish Open Universities is low. The beginning of the thesis presented the basic definition of information security, the laws that touch upon the subject area as well as previous studies of topics related to the subject. The human factor of information security was approached by introducing information security awareness and presenting the risks of personnel in an organization by going through the main risks concerning the Open Universities. The empirical section of the thesis gives a good summary of the level of information security awareness among the personnel of Open Universities in Finland.

People are often the weakest link in an organization's security chain for the lack of proper training, for not knowing what security means or for not understanding what results their however small actions may have. The results of this research have given reason to assume that this is the case at the Finnish Open Universities. The main possible threats to the information security at the Open Universities in Finland are trustfulness and carelessness of the employees. The awareness of information security among the personnel of the Open Universities is at a level where a possibility of an accident taking place is high. In addition, the foundation for information security awareness at the Finnish Open Universities is weak, as information security training is rarely provided for the personnel.

We hope that the results of this thesis provide Open Universities with a foundation for raising the awareness of information security among the personnel. It would be interesting to conduct a similar empirical study on Open University personnel after a couple of years and compare the results with the results of this thesis. For the next empirical study, it would be interesting to define the questions on the basis of the results of this thesis.

REFERENCES

Albrechtsen, Eirik (2007). A qualitative study of users' view on information security. *Computers & Security* [online] 26: 4, June 2007. [cited 2008-04-06], 276–289. Available from Internet: <URL: http://www.sciencedirect.com.proxy.tritonia.fi/science?_ob=MImg&_imagekey=B6V8G-4MM25RD-1-1&_cdi=5870&_user=5391025&_orig=search&_coverDate=06%2F30%2F2007&_sk=999739995&view=c&wchp=dGLbVlW-zSkzV&md5=11f649c289b0601e765b9b96c6925d56&ie=/sdarticle.pdf>.

Anttila, Juhani, Jorma Kajava & Juha E. Miettinen (2003). Changes in ITC security education due to changing technology. In: *European Intensive Programme on Information and Communication Technologies Security, IPICS'2003, 4th Winter School, Oulu, Finland* [CD-ROM]. Ed. Jorma Kajava, Gerald Quirchmayr, Juha Röning, Ilkka Tuikkala. Oulu: University of Oulu. [cited 2008-03-23] Information Security Issues from the End-User Perspective, 8–15 p. ISBN 951-42-7013-4.

Bailey, Robert W. (1983). *Human Error in Computer Systems*. New Jersey: Prentice-Hall, Inc. 146 p. ISBN 0-13-445056-6.

Caelli, William, Dennis Longley & Michael Shain (1991). *Information Security Handbook*. New York: Stockton Press. 833 p. ISBN 0-333-51172-7.

Coe, Kathy (2004a). Behind the firewall – the insider threat, part 1. *eWeek, Enterprise News & Reviews*. [online] [cited 2004-12-09]. Available from Internet: <URL: http://www.eweek.com/c/a/Security/Behind-the-Firewall-The-Insider-Threat-Part-1/>.

Coe, Kathy (2004b). Behind the firewall – the insider threat, part 2. *eWeek, Enterprise*

News & Reviews. [online] [cited 2004-12-09]. Available from Internet: <URL: http://www.eweek.com/c/a/Security/Behind-the-Firewall-The-Insider-Threat-Part-2/>.

Earp, Julia B. & Fay C. Payton (2001). Data protection in the university settings: Employee perceptions of student privacy. *Proceedings of the 34th Hawaii International Conference on System Sciences*. [online] [cited 2008-04-05] Available from Internet: <URL: http://ieeexplore.ieee.org/iel5/7255/20032/00927152.pdf?tp=&arnumber=927152&isnumber=20032>.

Florêncio, Dinei & Cormac Herley (2007). A Large-Scale Study of Web Password Habits. *Proceedings of the 16th international conference on World Wide Web*. [online] [cited 2008-04-09] Available from Internet: <URL: http://delivery.acm.org/10.1145/1250000/1242661/p657-florencio.pdf?key1=1242661&key2=6900477021&coll=ACM&dl=ACM&CFID=23484120&CFTOKEN=60925226>.

Hakala, Mika, Mika Vainio & Olli Vuorinen (2006). *Tietoturvallisuuden käsikirja*. Jyväskylä: Docendo Finland Oy. 422 p. ISBN 951-846-273-9.

Henkilötietolaki 01.06.1999/523.

Järvinen, Pertti & Annikki Järvinen, (2000). *Tutkimustyön metodeista*. Tampere: Opinpajan kirja. 221 p.

Järvinen, Petteri (2002). *Tietoturva & yksityisyys*. 2nd ed. Jyväskylä: Docendo Finland Oy. ISBN 951-846-152-X.
456 p. ISBN

Kajava, Jorma (2000). Hallinnon tutkimus. *Tietoturvan yksilöön ja organisaatioon*

kohdistamat haasteet 2000 -luvun alussa 19:2 [online] [cited 2008-03-27], 159–176. Available from Internet: <URL: http://www.ulapland.fi/files/20040114143337.pdf>.

Kajava, Jorma (2003a). Henkilöturvallisuus osana organisaation tietoturvaa. *Oulun yliopisto. Tietojenkäsittelytieteiden laitos. Sarja D 12, Sovellukset ja hallinto*. [online] [cited 2008-03-24], 1–14. Available from Internet: <URL: http://www.ulapland.fi/files/2004011415044.pdf>. ISSN 1459-1987.

Kajava, Jorma (2003b). Information security issues from the end-user perspective. In: *European Intensive Programme on Information and Communication Technologies Security, IPICS'2003, 4th Winter School, Oulu, Finland* [CD-ROM]. Ed. Jorma Kajava, Gerald Quirchmayr, Juha Röning, Ilkka Tuikkala. Oulu: University of Oulu. [cited 2008-03-23] Information Security Issues from the End-User Perspective, 3–7 p. ISBN 951-42-7013-4.

Kajava, Jorma & Rauno Varonen (2003). Incorporating information security into university infrastructure. In: *European Intensive Programme on Information and Communication Technologies Security, IPICS'2003, 4th Winter School, Oulu, Finland* [CD-ROM]. Ed. Jorma Kajava, Gerald Quirchmayr, Juha Röning, Ilkka Tuikkala. Oulu: University of Oulu. [cited 2008-04-07] Information Security Issues from the End-User Perspective, 16–26 p. ISBN 951-42-7013-4.

Koskinen, Seppo, Leena Alapuranen, Anna-Maija Heino & Minna Salli (2005). *Henkilötietojen käsittely työelämässä*. Helsinki: Edita Publishing Oy. 449 p. ISBN 951-37-4393-4.

Krutz, Ronald L. & Russell Dean Vines (2003). *Tietoturvasertifikaatti CISSP*. Helsinki: Edita Publishing Oy, IT Press. 557 p. ISBN 951-826-657-3.

Laki sähköisestä asioinnista viranomaistoiminnassa 16.10.2003/13.

Lantto, Eeva (1999). *Sähköinen asiointi hallinnossa*. Sosiaali- ja terveysturvan

katsauksia 38. Helsinki: KELA. 113 p. ISBN 951-669-491-8.

Machiavelli, Niccolò (1950). *The Prince and The Discourses*. [online] New York: The Modern Library. Random House Inc. [cited 2008-04-07]. Available from Internet: <URL: http://design.caltech.edu/erik/Misc/design_quotes.html>.

Miettinen, Juha E. (1999). *Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan*. Helsinki: Kauppakaari Oyj. 318 p. ISBN 952-14-0229-6.

Ministry of Finance (2005). *Information Security and Management by Results 1/2005*. [online] Helsinki: Ministry of Finance. Available from Internet: <URL: http://www.vm.fi/vm/en/04_publications_and_documents/01_publications/05_government_information_management/20060320Inform/94247.pdf>.

Mäkinen, Olli (2006). *Internet ja etiikka*. Helsinki: BTJ Kirjastopalvelu Oy. 251 p. ISBN 951-692-621-5.

Paananen, Juha (2005). *Tietotekniikan peruskirja*. Jyväskylä: Docendo Finland Oy. 491 p. ISBN 951-846-250-X.

Pahnila, Seppo, Mikko Siponen & Adam Mahmood (2007). Employees' behavior towards IS security policy compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences* January 2007 [online] [cited 2008-04-06] Available from Internet: <URL: http://ieeexplore.ieee.org.proxy.tritonia.fi/iel5/4076361/4076362/04076692.pdf?tp=&arnumber=4076692&isnumber=4076362>.

Penido, Christopher (2007). Data handling. With ease comes responsibility. *Connect: Information Technology at NUY* Spring/Summer 2007 Edition [online] [cited 2008-04-04]. Available from Internet: <URL: http://www.nyu.edu/its/pubs/connect/spring07/penido_data.html>.

Ruohonen, Mika (2002). *Tietoturva*. Jyväskylä: Docendo Finland Oy. 428 p. ISBN

951-846-163-5.

Räsänen, Tuula (1998). Henkilöriskikysely [online]. PK-RH hanke. 1.12.1998. [cited 24 March 2008].

Schneier, Bruce (2000). *Secrets and Lies: Digital Security in a Networked world*. New York: John Wiley & Sons, Inc. 412 p. ISBN 0-471-25311-1.

Siponen, Mikko T. & Jorma Kajava (1997). *Dimensions of Information Security Awareness*. Oulu: Oulu University Press. 16 p. ISBN 951-42-4835-X.

Siponen, Mikko T. & Jorma Kajava (1998). Ontology of organizational IT security awareness – from theoretical foundations to practical framework. *Proceedings of the 7th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*. [online] [cited 2008-03-29] Available from Internet: <URL: http://ieeexplore.ieee.org/iel4/5881/15665/00725713.pdf?tp=&isnumber=&arnumber=725713>.

Sähköisen viestinnän tietosuojalaki 16.6.2004/516.

Toivonen, Kaisa (2008). *Kyselylomake avoimen yliopiston hallintohenkilökunnalle*. [online] [cited 2008-04-19] Available from Internet: <URL: http://forms.uwasa.fi/lomakkeet/393/lomake.html>.

Turner, Marcia Layton (2007). Training your staff to protect SIS data. *University Business* September 2007 [online] [cited 2008-04-04]. Available from Internet: <URL: http://www.universitybusiness.com/viewarticle.aspx?articleid=868&p=1#0>.

Valtiovarainministeriö (2003). *Käyttäjän tietoturvaohje 5/2003*. [online] Helsinki: Valtiovarainministeriö. Available from Internet: <URL: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/vanha01_julkaisut/05_valtionhallinnon_tietoturvallisuus/51027/51024_fi.pdf>.

Valtiovarainministeriö (2006). *Tietoturvallisuuden arviointi valtionhallinnossa 8/2006*. [online] Helsinki: Valtiovarainministeriö. Available from Internet: <URL: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060802Tietot/A_vahti_08_netti.pdf>.

APPENDIX 1.

Kyselylomake avoimen yliopiston hallintohenkilökunnalle

Tällä kyselylomakkeella kartoitetaan miten suuri rooli hallintohenkilöstöllä on avoimen yliopiston tietoturvallisuudessa.

Tietoturvaa ei voi ostaa. Rahalla saa ainoastaan teknisiä apuvälineitä tietoturvallisuuden tasoa kohentamaan. Järvisen (2002) mukaan todellinen turvallisuus syntyy organisaation sisäisestä luottamuksesta, oikeista menettelytavoista, koulutuksesta ja huolellisuudesta. Tämän kyselylomakkeen tarkoituksena on selvittää Suomen avointen yliopistojen henkilökunnan tietoturva-asioiden tietoisuuden taso.

Tuloksia käytetään ainoastaan tutkimusaineistona pro gradu -tutkielmassa. Vastaajan henkilöllisyys ei paljastu missään vaiheessa eikä tutkimuksen tuloksia voi yhdistää tiettyyn henkilöön.

Tutkimus on osa Kaisa Toivosen pro gradu -tutkielmaa. Tutkielman ohjaaja on professori Jari Töyli, Vaasan yliopisto, Tietotekniikan laitos.

Vastaathan viimeistään to 20.3. klo 16.15. Kaikkien vastanneiden kesken arvotaan opinto-oikeus syksyllä 2008 järjestettävälle Tietojenkäsittely-verkkokurssille. Voit ilmoittaa halukkuutesi osallistua arvontaan sähköpostitse.
Yhteystiedot: Kaisa Toivonen, kaisa.toivonen@uwasa.fi, 06-324 8759
Lähde: Järvinen, Petteri (2002). *Tietoturva & yksityisyys*. Jyväskylä: Docendo Finland Oy.

Vastaajan tiedot

Luethan kysymykset huolellisesti ja vastaathan kysymyksiin ajatellen miten toimit ollessasi töissä. Kommentit-kenttiin voit lisätä kysymyksistä mieleen tulleita ajatuksia tai avata omaa vastausta. Lomakkeen lopussa on vielä erillinen laatikko yleisille kommenteille.

1. Ikä -
2. Sukupuoli -
3. Työnimike -
4. Avoimen yliopiston koko hallintohenkilökunnan määrän mukaan -
5. Olen ollut töissä avoimessa yliopistossa -
6. Virkani/työsuhteeni on -
7. Työntekijöiden määrä, joiden kanssa voin jakaa työtehtäviä –

Tietojen muokkausoikeudet
kyllä ei Kommentit
8. Saan halutessani selville (esim. paperilomakkeelta/opiskelijatietojärjestelmästä) opiskelijoiden henkilötiedot (esim. hetu, nimi- ja osoitetiedot)
9. Voin muuttaa opiskelijatietojärjestelmässä opiskelijan perustietoja (esim. hetu, nimi- ja osoitetiedot)
10. Saan halutessani selville työntekijöiden käyttäjätunnustiedot
11. Voin vaihtaa tunnuksen tai salasanan työntekijän puolesta järjestelmään, jossa säilytetään opiskelijoiden tai työntekijöiden henkilötietoja

Kysely

Arviointiasteikko: 1=täysin eri mieltä, 2=eri mieltä, 3=ei samaa mieltä eikä eri mieltä, 4=samaa mieltä, 5=täysin samaa mieltä

Tietojen suojaus

1 2 3 4 5 Kommentit
12. Voin tarkistaa opiskelijan kanssa puhelimitse opiskelijatietojärjestelmässämme hänestä tiedossa olevan hetun
13. Voin kertoa opiskelijalle sähköpostitse opiskelijatietojärjestelmässämme hänestä tiedossa olevan hetun
14. Toimistoon ei ole avaimia muilla ihmisillä (pl. siivooja), kuin heillä, joilla on oikeus päästä käsiksi toimistossa säilytettäviin tietoihin
15. Lukitsen pöytätietokoneeni aina, kun en ole sen ääressä
16. Lukitsen työhuoneeni oven poistuessani esim. kopiomaan materiaalia
17. Lukitsen työhuoneeni oven työpäivän päättyessä tai poistuessani huoneestani pidemmäksi aikaa (esim. lounaalle)
18. Katkaisen virran koneestani tai suljen yhteyden (log off) aina, kun poistun pidemmäksi aikaa työpaikalta
19. Poistun käyttämistäni järjestelmistä aina ohjeiden mukaan (kirjaudun ulos järjestelmästä, en siis vain sulje selaimen ikkunaa)
20. En koskaan jätä opiskelijan henkilötietoja sisältäviä dokumentteja (esim. opintosuoritusote) talteen omiin tiedostoihin (My Documents) tai koneen työpöydälle (Desktop)
21. Säilytän opiskelijoiden henkilötietoja sisältäviä papereita työpöydälläni (jos valitset 4 tai 5, kerrothan
Kommentit-kohdassa miksi näin voi tapahtua)
22. En laita henkilötietoja sisältäviä tulosteita roskakoriin
23. En anna ulkopuolisen käyttää konettani, ellen ole varma hänen henkilöllisyydestään ja käyttöoikeudesta
24. Aina ennen vieraan levykkeen tai muistitikun avaamista koneellani ajan virustarkistuksen levykkeelle tai muistitikkuun
25. Huoneeseeni tulee päivittäin organisaation ulkopuolisia ihmisiä (esim. opiskelijoita)

Arviointiasteikko: 1=täysin eri mieltä, 2=eri mieltä, 3=ei samaa mieltä eikä eri mieltä, 4=samaa mieltä, 5=täysin samaa mieltä

Käyttäjätunnukset ja salasanat

1 2 3 4 5 Kommentit

26. Voin päästää ATK-tukihenkilön koneelleni ollessani kirjautuneena omilla tunnuksillani, jotta hän voi asentaa koneelle uuden ohjelmistopäivityksen
27. Voin antaa ATK-tukihenkilölle kirjautumistunnuksen ja salasanani
28. Käytän riittävän pitkiä ja vaikeita salasanoja
29. Säilytän salasanojani turvallisessa paikassa enkä luovuta niitä kenellekään toiselle
30. Säilytän salasanojani paperille kirjattuna työhuoneessani
31. Syötän oman salasanani vain koneelta, johon tai jonka omistajaan luotan
32. En anna ihmisten kurkkia olkani yli, kun käsittelen arkaluonteisia tietoja tai syötän salasanoja
33. Koostuuko salasanasi yleensä? -
34. Kuinka usein vaihdat salasanasi? –

Arviointiasteikko: 1=täysin eri mieltä, 2=eri mieltä, 3=ei samaa mieltä eikä eri mieltä, 4=samaa mieltä, 5=täysin samaa mieltä

Sähköposti ja Internet

1 2 3 4 5 Kommentit

35. Voin avata tuntemattomasta osoitteesta lähetetyn sähköpostin linkin, jos sähköpostin viesti on tarpeeksi
kiinnostava
36. Käytän työsähköpostiosoitettani myös henkilökohtaiseen viestintään
37. Lomalle lähtiessäni asetan työsähköpostiini automaattisen lomaviestin
38. En ole koskaan ohjannut työsähköpostiani henkilökohtaiseen sähköpostiosoitteeseeni
39. Poissaollessani työsähköpostiini ei pääse kirjautumaan kukaan muu työntekijöistä
40. Kuinka usein käytät töissä Internetiä? -
41. Mihin käytät Internetiä? (voit valita useampia pitämällä Ctrl-näppäintä pohjassa)
työhön liittyvän materiaalin hakuun ja työhön liittyvään viestintään
verkkokeskusteluun
etsin harrastuksiin liittyvää tietoa
surffailen satunnaisesti
luen viihdesivuja

Arviointiasteikko: 1=täysin eri mieltä, 2=eri mieltä, 3=ei samaa mieltä eikä eri mieltä, 4=samaa mieltä, 5=täysin samaa mieltä

Osaaminen

1 2 3 4 5 Kommentit

42. Koulutukseni on riittävä nykyiseen tehtävääni
43. Koen uudet asiat haasteena työssäni.
44. Uusien työkalujen (ohjelmien, järjestelmien) käyttöönotto sujuu minulta helposti

Arviointiasteikko: 1=täysin eri mieltä, 2=eri mieltä, 3=ei samaa mieltä eikä eri mieltä, 4=samaa mieltä, 5=täysin samaa mieltä

Työkyky ja motivaatio

1 2 3 4 5 Kommentit

45. Koen työni mielekkääksi
46. Työni ei ole rasittavaa
47. Haluan kehittyä työssäni ja oppia uusia asioita
48. Autan mielelläni työtovereitani ongelmatilanteiden ratkaisemisessa

Arviointiasteikko: 1=täysin eri mieltä, 2=eri mieltä, 3=ei samaa mieltä eikä eri mieltä, 4=samaa mieltä, 5=täysin samaa mieltä

Työyhteisö

1 2 3 4 5 Kommentit

49. Saan riittävästi tietoa johdolta, jotta voin hoitaa työni hyvin
50. Saan riittävästi tietoa työtovereiltani, jotta voin hoitaa työni hyvin
51. Työtovereiden välit ovat työpaikallani hyvät

Ennen seuraaviin kysymyksiin vastaamista haluan selventää, että tietoturvallisuuskoulutuksella tarkoitetaan henkilöstön työ- ja toimintatapojen ohjeistusta. Tietoturvallisuuskoulutuksen tavoitteena on varmistaa, ettei työ- tai toimintatavoissa ole organisaation tietoturvallisuutta heikentäviä tekijöitä.

Tietoturvaohjeistus

1 2 3 4 5 Kommentit

52. Henkilöstö on koulutettu käyttämään avoimessa yliopistossa käytettäviä järjestelmiä
53. Avoimen yliopiston henkilökunta on saanut tietoturvallisuuskoulutusta. (jos 4 tai 5, minkälaista?)
54. Kuinka usein avoimen yliopiston henkilökunta on saanut tietoturvallisuuskoulutusta? -
1 2 3 4 5 Kommentit
55. Uusille työntekijöille on tarjolla tietoturvallisuuskoulutusta
56. Avoimella yliopistolla on henkilökunnalle tarkoitettu tietoturvaohjeistusdokumentaatio (jos 4 tai 5, mistä sen voi löytää?)

Tietoturvakoulutus

57. Miten mieluiten oppisit lisää mahdollisuuksista toimia tietoturvallisesti työpaikallasi ja suojata organisaatiossa käsiteltäviä tietoja? -
Yleisiä kommentteja

Tietojen lähetys
Lähetä tiedot Tyhjennä

APPENDIX 2.

Questionnaire for administrative personnel of Open University

This questionnaire is used to examine how big role administrative personnel play in the information security of Open University.

Information security can not be bought. Money can only help you acquire technical devices, which can assist in increasing the level of information security. According to Järvinen (2002: 47) the real information security is composed of internal trust, correct operational practices, education and carefulness. The aim of this questionnaire is to find out the level of information security awareness at the Finnish Open Universities.

The results are used only as a research material in pro gradu -thesis. Respondents' identity will not be revealed at any time and the results can not be connected to a particular person.

The survey is part of Kaisa Toivonen's pro gradu -thesis. Thesis' Tutor is Jari Töyli PhD, University of Vaasa, Department of Computer Science.

Please send your response latest by Thursday 20th of March at 16.15. Among all the respondents there will be a raffle where the prize is a right to attend a web-course Data processing in the autumn 2008. You may inform of your will to take part in the raffle by email.
Contact details: Kaisa Toivonen, kaisa.toivonen@uwasa.fi, 06-324 8759.
Source: Järvinen, Petteri (2002). *Tietoturva & yksityisyys*. Jyväskylä: Docendo Finland Oy.

Data of the respondent

Please read the questions carefully and answer thinking how you behave while at work. You may add your thoughts on the questions or elaborate your answer in the Comments-field. There is an additional field for general comments in the end of the questionnaire.

1. Age (Under 29-years-old, 30–39-years-old, 40–49-years-old, 50–65-years-old)
2. Gender (Male, Female)
3. Job description (Manager, Planner / Head of Study Affairs, IT personnel, Secretary / Study Advisor / Tutor)
4. Size of the Open University (Large, Medium, Small)
5. Duration of employment (Less than three months, Less than a year, 1–3 years, Over three years)
6. Nature of the contract (Permanent, Temporary)
7. Sharing of duties is possible with (No-One, 2–3 employees, more than 4 employees)

Right to rewrite data

8. Access to students' personal details (Yes, No)

9. Right to change students' personal details (Yes, No)
10. Access to personnel's user names and passwords (Yes, No)
11. Right to change user name and password for personnel (Yes, No)

Questionnaire

Rating scale: 1=strongly disagree, 2=disagree, 3=neither agree nor disagree, 4=agree, 5=strongly agree.

Protection of data

12. I can verify the personal identity number we have in our student information system of a student I'm on the phone with.
13. I can tell a student by email the personal identity number we have stored of him/her in our student information system.
14. No-one else (apart from the cleaner) has keys to the office, unless they have a right to access the information stored at the office.
15. I lock my personal computer always when I'm not by it.
16. I lock the door of my office when I leave, for example to copy some material.
17. I lock the door of my office when I leave in the end of the day or when I leave the office for a longer period, for example for lunch.
18. I shut down or log off of my computer always, if I leave the work place for a longer period of time.
19. I leave the programs I use always according to the instructions (I log out and do not just close the window).
20. I never leave documents containing students' personal information (for example study records) stored to My Documents or Desktop of the computer
21. I store documents containing students' personal information on my desk (if you choose 4 or 5, please state in the Comments-field why this may happen).
22. I do not throw away printouts containing students' personal information to the bin.
23. I do not let an outsider to use my computer, unless I'm certain of his/her identity and access right.
24. I perform a virus check on a memory stick or a floppy disc always before opening it on the computer.
25. I have people from outside of the organization (for example students) coming to my office daily.

Rating scale: 1=strongly disagree, 2=disagree, 3=neither agree nor disagree, 4=agree, 5=strongly agree.

User names and passwords

26. I can let IT support person to use my computer while I'm logged in with my own user name, so that s/he can install a new update of a system.
27. I can give my user name and password to IT support person.
28. I use long and difficult enough passwords.
29. I store my passwords in a safe place and do not hand over them to anyone else.

30. I store my passwords written on a piece of paper in my office.
31. I enter my password only from a computer that I trust, or whose owner I trust.
32. I do not let people look over my shoulder, while I'm processing sensitive data or typing in my password.
33. Does your password usually contain: (Numbers (0-9), Numbers and special characters (0-9, _), Lower-case letters (a-z), Lower-case letters and numbers (a-z, 0-9), Lower-case letters, numbers and special characters (a-z, 0-9, _), Lower-case and uppercase letters (a-z, A-Z), Lower-case and uppercase letters and numbers (a-z, A-Z, 0-9), Lower-case and uppercase letters, numbers and special characters (a-z, A-Z, 0-9, _), Lower-case and uppercase letters and special characters (a-z, A-Z, _), Lower-case letters and special characters (a-z, _))
34. How often do you change your password? (More often than once in six months, When the system reminds me, Less frequently)

Rating scale: 1=strongly disagree, 2=disagree, 3=neither agree nor disagree, 4=agree, 5=strongly agree.

Email and Internet

35. I can open a link in an email arriving from an unknown address, if the message of the email is interesting enough.
36. I use my work email address for personal communication.
37. When I go for a holiday, I set a holiday message to my work email.
38. I have never directed my work emails to my personal email account.
39. When I'm not at work, no other employee can log in to my email account.
40. How often do you use the Internet at work? (Several times a day, Few times a day, Once a day, Few times a week, Once a week, Few times a month)
41. What do you use the Internet for? (You can choose several by holding CTRL: Work related information retrieval and communication, chat, I look for information on my hobbies, I surf randomly, I read entertainment pages)

Rating scale: 1=strongly disagree, 2=disagree, 3=neither agree nor disagree, 4=agree, 5=strongly agree.

Know-how

42. My education is sufficient for my current job.
43. I take new things as a challenge at work.
44. Inauguration of new tools (systems or programs) comes easy to me.

Rating scale: 1=strongly disagree, 2=disagree, 3=neither agree nor disagree, 4=agree, 5=strongly agree.

Work ability and motivation

45. I feel my work is meaningful.
46. My job is not tiresome.
47. I want to develop at my job and learn new things.
48. I'm happy to help my colleagues to solve problem situations.

Rating scale: 1=strongly disagree, 2=disagree, 3=neither agree nor disagree, 4=agree, 5=strongly agree.

Work community

49. I receive enough information from Managers for me to perform my job well.
50. I receive enough information from my colleagues for me to perform my job well.
51. Relationships between colleagues at my work place are good.

Before answering the next questions we would like to clarify that with information security training we mean guidance of personnel's work and operational habits. The objective of information security training is to ensure that work and operational habits do not include factors that could weaken organization's information security.

Information security guidelines

52. Personnel are trained to use the systems used at Open University.
53. Open University personnel have received information security training. (if you choose 4 or 5, please elaborate in the Comments-field)
54. How often Open University personnel has received information security training? (Never, Once, when beginning a job at Open University, Once, organized by the mother university, Less often than once a year, Once a year or more often)
55. New employees are provided with information security training.
56. Open University has an information security guideline provided for the personnel. (if you choose 4 or 5, please state where it can be found)

Information security training

57. How would you prefer to learn more about the possibilities on how to work securely at your work place and how to protect the information handled at the organization? (Personal guidance, Small group environment, Lecture, Through intranet, Email newsletter, Through other means)

General comments

Send information

APPENDIX 3.

Tabel 1. Gender of the respondents.

Gender	Frequency	Percent
Female	96	85,0
Male	17	15,0
	113	

Tabel 2. Age of the respondents.

Age	Frequency	Percent
Under 29-year-olds	15	13,3
30–39-years-old	33	29,2
40–49-years-old	32	28,3
50–65-years-old	33	29,2
	113	

Tabel 3. Job description of the respondents.

Job description	Frequency	Percent
Manager	9	8,0
Head of Study Affairs/Planner	63	55,8
IT personnel	1	0,9
Secretary/Study Advisor/Tutor	40	35,4
	113	

Tabel 4. Distribution of the answers from different sizes of Open Universities.

Size of the Open University	Frequency	Percent
Large	42	37,2
Medium	58	51,3
Small	13	11,5
	113	

Tabel 5. Respondents' duration of employment.

Duration of employment	Frequency	Percent
Less than 3 months	2	1,8
Less than a year	8	7,1
1–3 years	16	14,2
Over 3 years	85	75,2
No response	2	1,8
	113	

Tabel 6. Respondents' nature of contract.

Nature of contract	Frequency	Percent
Permanent	81	71,7
Temporary	30	26,5
No response	2	1,8
	113	

Tabel 7. Respondents' possibility to share their duties.

Sharing of duties is possible with	Frequency	Percent
No-one	25	22,1
2–3 employees	53	46,9
More than 4 employees	32	28,3
No response	3	2,7
	113	