Master Thesis:

“An overview of the current level of Security Awareness in Greek companies”

Master Program
Of
Economics and ICT

Supervisor: **G.J. van der Pijl**

Second supervisor: **Ad de Visser**

Name: **Kostas Papagiannakis**
SID: **345386**

Erasmus University of Rotterdam

Erasmus School of Economics

'A chain is only as strong as its weakest link'

David Sustaita

‘The user's going to pick dancing pigs over security every time’

Bruce Schneier

‘If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees’

Kahlil Gibran

Abstract

Information Security is one of the main concerns during the last years. Too much effort and funds are invested in the security of information asset by the enterprises. A crucial factor in Information Security is the human factor. End-users could provoke several damages to the Information Systems even if there are plenty of security measures in place. Security Awareness is the field of Information Security which handles the human factor. The main purpose of this study is to investigate the level of Security Awareness in Greek companies. The method used in this study was a questionnaire survey which reveals how employees behave with the Information System that they use, how they behave within physical security and how they handle their passwords. The main finding of the research is the medium to low level of Information Security Awareness. The level seems to be decreasing down while one is descending the hierarchy pyramid in Greek IT companies.

Key Words: *Security awareness, social engineering, information security, Greek companies/ organizations – case of Greece, security awareness practices/ techniques/ policies, security awareness evaluation/ assessment, information security culture/behavior/routine*

Table of Contents

1. Introduction **6**

2. Literature Review **7**

3. Research Question **13**

4. Theoretical Review **14**

4.1 Security Awareness Definitions 14

4.2 Implementation of Security Awareness – practices, techniques and policies 15

4.2.1 Preparing Information Security Awareness campaign 15

4.2.2 Practices of Information Security Awareness 16

4.2.3 Information Security Awareness policies 18

4.3 Evaluation of Security Awareness policies and campaigns 20

4.4 Advantages and Disadvantages of Security Awareness 21

4.5 Barriers in implementing Information Security Awareness programs........ 22

4.6 Conclusion 23

5. Research Methodology **25**

5.1 Sample and Survey Design 25

5.2 Questionnaire Design 26

5.2.1 Measurement 27

5.2.1.1 Demographic Data 28

5.2.1.2 Technology Usage 29

5.2.1.3 Physical Security 30

5.2.1.4 Information System Security 31

5.2.1.5 Password Handling 31

6. Results **34**

6.1 Demographics 35

6.2 Other Remarkable Measurements 36

6.2.1 Information System Security Awareness 37

6.2.2 Physical Security Measurements 37

6.2.3 Information System Security Measurements 38

6.2.4 Password Handling Measurements 39

6.3 Various clustered Bar graphs 40

6.4 Chi-square Analysis 42

6.4.1 Differences between working position 42

6.4.2 Differences between years of seniority 47

7. Discussion 51

8. Conclusion 53

8.1 Limitations 55

8.2 Further Research 55

9. References 57

10. Appendices 60

1. Introduction

Much effort is spent by organizations in implementing technological solutions in order to cover security gaps that consist of potential risks for companies' assets. People play a key role in the 'game' of security in organizations. Security awareness is a crucial factor that directly affects the safety of assets in an organization.

Technology is being developed on a daily basis. New technological solutions arise every day and so do the threats [6]. As long as IT is developing, security threats arise simultaneously. People that operate the systems can create an open back door and will always be a potential vulnerable gateway in abusing an information system [10]. People should not only be trained on how to use the system, but also on how to use it in a safe way. Every organization should establish security policies and furthermore, has to instruct people to follow the security guidelines in their daily routine.

The field of security awareness is underestimated [13]. The majority of the organizations, especially in the small and medium sized enterprises (SMEs), do not pay attention in raising security awareness. They are not aware of the dangers that could potentially arise. Mainly, the problem stems from the top management [6]. As a consequence, this has a negative impact on low level managers and on users of the information system in an organization.

My working experience in Greek companies (IT company, construction company etc.) gave me the opportunity to observe several security issues. This motivated me to investigate the current situation in Greek companies regarding the field of Security Awareness. A research among Greek companies will give information that can bring conclusions to both the academic and industrial sector. On one hand, companies could learn the importance of security consciousness of employees and the ways they could eliminate potential vulnerabilities. On the other hand, such a research could trigger in depth, future research which examines the ways that led Greek companies in the current situation that I am going to investigate.

2. Literature Review

Last decades, technological inventions have been expanded all over the world including tools that have been used on a daily basis for various purposes. People use technology in their daily routine; from their houses, their workplace and their entertainment. More specifically, with the internet expansion, people became more familiar with the technology. Hundreds of millions of people use the internet and are now more aware than ever, of technological inventions and development. Many of them do not stop there. Access to knowledge is easier than in the past and people can obtain information and study in depth issues that they are interested in.

In the next paragraphs, the role of users is presented based on recent literature. Users seem to be aware of security issues and terms, but they lack in acting in a secure way. Users can be divided into home-users and users of organizations; employees. This study focuses on the later group of users.

A great number of people have access to in depth knowledge of technology and to technical details. This makes them capable to abuse it. At this point the Information and Communication Technology (hereinafter referred to as 'ICT') intervenes by fulfilling the security gaps of information systems and protecting them technically. What is more, the enhancement (i.e. from the perspective of security) of the information systems makes them less vulnerable to outside threats. However, while technology changes over the time, security threats follow these changes [6]. In other words, although technology will always be developed in order to cover security gaps, there will always be different ways to abuse it. In this 'game', one factor, the human factor, is still there and is of a great concern regarding security issues. Users have to be aware of security tactics and procedures and they have to know how to use technology in a safe way. In other case, even a contemporary and highly developed system is under serious threats because of its dependency on the users that operate it.

Simultaneously, with the expansion and use of the internet people became familiar with the terms virus, hacker etc. [4]. Although people are aware of those terms, it seems that they do not take care of the systems' security in their daily routine neither at their workplace nor at their home. There is research that has examined the attitude of users and more specific employees in companies [2] [4] [7]. The results of those surveys showed that media contributed for several incidents of technology abuse and crimes to become widely known [4]. Nevertheless, media did not act as a 'security lesson' for people. They did not urge people to change their behavior so as to guarantee security to some extent.

To be more specific, amongst all different user categories, I will focus on employees in corporate institutions. In this field a great range of losses are recorded and several incidents are reported. More specifically, in the EU-27 excluding Estonia, 15% of the enterprises reported at least one ICT security incident experienced in 2009 according to Eurostat's data[1]. There are several security threats an enterprise has to face. First of all, employees who work for the company are considered to be a serious threat if they do not use properly the IT systems. Employees use equipment that they do not own. Many factors lead to inappropriate activities that harm the companies' asset or even their reputation such as anger, abasement etc. However, companies have to deal with both internal and external threats (i.e. people) [8]. People outside the company try to abuse the system in order to gain benefits for themselves. That could happen either because they would like to take revenge or because they would like to gain advantages that could be used against company's IT system [8]. Based on that literature, we can identify three major categories of potential dangers that a company has to face. According to Euripidis Loukis and Diomidis Spinelis (2001), there are malicious authorized users, negligent authorized users and outsiders that can provoke loss and damages to an organization. Malicious authorized users refer to employees of the company that have access to its assets and act harmfully in order to cause damage. Except for the people inside the company, that want to cause damages intentionally, there is a great part of employees who harm organization's assets unintentionally. Those employees compose the second category; negligent authorized users. During the daily routine, they are not aware of the dangers and their negative impact on the information system or they do not follow the company's security policy and procedures in order to accomplish their goals in an easier way. In those cases, they cause losses to the company, too. Finally, as it is mentioned before, there are people outside the company that have the intention to harm the company's assets in order to gain advantages in the future.

Comparing the three types of dangers that are recognized, the first one (i.e. malicious authorized user) is the most dangerous for a company. Such users cause more damage and have many advantages over an outside attacker [8]. This is obvious because an insider attacker has the authority to reach information which is crucial for the company and can compromise the confidentiality, integrity and availability of information. Moreover, as Carl Colwill (2010) mentions, insider attackers are usually trusted employees that hold a senior position within the company, meaning that they are authorized to reach any type of information of the company and they can even recruit low level employees to work for their inappropriate activities.

[1] *http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises#Security_incidents*

Within the next paragraphs, the importance of Security Awareness is highlighted. Training of employees is crucial in order to raise their security consciousness and face the phenomenon of social engineering and widely known practice of phishing.

Every company has to face those three types of potential dangers. Information is the life line of the majority of the organizations and it is crucial for them to keep it safe [9]. First of all, a company has to recruit and train people so they can be trusted employees who are aware of the threats and the security policies and procedures of the company. Secondly, every company has to set up a system of defense so as to make it difficult for outsiders to reach the company's assets and compromise them. Such a system refers to both technological security measures and security awareness practices that aim in training employees and guarantee a safe behavior on behalf of the employees.

One of the major threats for companies is social engineering. This is "is essentially the art of gaining access to buildings, systems or data by exploiting human psychology"[2]. In addition, by phishing one can "acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication"[3]. Employees as users of the information system of a company are an open back door for outsiders into the organization's network [10]. According to the Anti-phishing Working Group in 2006, 23.670 unique phishing attempts were recorded, targeting 14.191 websites. Ronald C. Dodge Jr, Curtis Carver and Aaron J. Ferguson (2007) conducted a survey in which they set up an attack/ defense scenario and they applied it in 512 students of United States Military Academy (USMA). They sent three types of e-mails; phishing through e-mail (by clicking a link), social engineering (taking personal information) and downloading an application. The results were important for the confidentiality and integrity of data. Students downloaded attachments easier than clicking a link, while, students who were longer in the academy, reported incidents such as phishing, easier than the new students (later on the paper is recorded the great issue of reporting security incidents inside an organization). The survey highlighted that exercises like this bring positive results to people and increase their security consciousness (Ronald C. Dodge Jr, Curtis Carver and Aaron J. Ferguson, 2007).

Several models and protocols have been written in order to achieve Security Awareness. In addition, research on security of information systems have been conducted and set a range of security issues that should be learnt by both the employees and the high-level management that applies security policies. It shows the importance of Security awareness and set it in the basic level of knowledge for a

[2] http://www.csoonline.com/article/514063/social-engineering-the-basics#1

[3] http://www.scribd.com/doc/46495486/Phishing-Seminar-Report

user. Below literature that refers to such research is presented in order to highlight the importance of security awareness.

In 2008, Marianthi Theocharidou, Dimitra Xidara and Dimitris Gritzalis introduced a Common Body of Knowledge (CBK) for information security and critical information and communication infrastructure protection. Writers of that paper refer that there is too much information about a great range of information security issues but they highlight the human factor that plays an important role in security. Within their research they construct a CBK where they categorize all the kinds of security fields in ten domains. They prioritized all security aspects from the generic (domain 1) to more specific and specialized security issues (domain 10). It is very interesting that the field of security training and awareness exists in the 2nd domain. Security awareness is of a great importance. According to the writers and their CBF, it is categorized early enough for humans to understand the way that they have to behave when dealing with information systems (Marianthi Theocharidou, Dimitra Xidara, Dimitris Gritzalis, 2008).

Another research is introduced by E. Kritzinger and E. Smith in 2008. Based on the concept that information is the life line of many companies and security incidents can cause loses in time, manpower money and business opportunities, they introduced an information security retrieval and awareness model for the industry. They argue that both employees and the stakeholders of security issues must be grouped together and participate in security awareness programs. They separate the stakeholders of security awareness program in six categories. First of all, there is the board level. Executive (senior) management level follows. After this, there is the middle management level and the technical management level. In the fifth and sixth position there are the information security management level and the user level respectively. These categories consist of the groups that stakeholders in a company (regarding security issues) have to participate in common in security awareness programs. Such a program must be applied in a top-down approach, while the reporting of incidents has to be implemented in a bottom-up approach [9]. In the first case, a security awareness program must be applied from the top level of management in order to transmit the policy and the behavior of security consciousness. At the same time, the reporting system of security incidents is crucial to be applied from the lower levels (users, low level managers etc.) to the higher layers of management in order to be taken corrective decisions for the entire process [9].

In addition, S. Shaw, Charlie C. Chen, Albert L. Harris and Hui-Jou Huang in 2009, highlight the need of a continuous security awareness program for the users. Users of an information system must change from “become aware” to “be aware” and finally they must “stay aware” (Schlenger & Taufel, 2003). The first separates the awareness of security risks in three levels; perception, comprehension and projection. They claim that perception of security awareness is far away from a behavior of security consciousness. Within the first level, the sense and the detection of potential risks are assessed. At the second level, users must understand, comprehend and assess the dangers posed (they can change the way they think and their behavior). Within the level of projection, prevention is the main concern. People behave proactively and they can predict security attacks and potential risks before they happen.

Below the main reasons that lead to security incidents are illustrated. Reporting system of security-related events, economical crisis and outsourcing are few of the reasons.

Reporting security issues is of a great importance for organizations which aim at eliminating such events. Employees, who work in a company and face such incidents, are afraid to report them to the stakeholders of security-related issues of the company. Even if they know that the incident happened unintentionally, they are worried about the possible penalties that the security policy of the organization imposes [20]. On the other hand, there are cases where employees do not care to report an unusual attitude or behavior of another employee [8]. Furthermore, company's unclear procedures could prevent employees to report a security incident. They do not know how or where to report such an incident [8]. However, such a behavior does not help organizations and governmental institutes to confront the general phenomenon of security abuses.

Organizational, cultural, economical and social factors influence the employees' attitude. Interestingly enough, Carl Colwill (2010) refers that outsourcing and recession are two circumstances that in this time play an important role in the safety of companies' assets and their security issues. Outsourcing, as he claims, is blurring the boundaries of the organization between the actual employees and the third-party co-operators while recession has a crucial impact on employees' ethical behavior. Uncertainty during a recession period makes employees more vulnerable in inappropriate activities.

Evaluating the security consciousness before and after applying a security awareness program is a crucial factor in order to achieve the best results. However, this is the most difficult part of applying such a program in an organization.

Very interesting is the research that is conducted by Aggeliki Tsohou et al, in 2008. Through an extended literature review gaps are highlighted between research and practice. Issues are discussed about the evaluation of security awareness programs and the stakeholders that have to participate in such programs. A crucial question for the evaluation of the programs is referring to what should be evaluated. One great issue could be how it can be done in practice. Most of the publications that were examined, agree that all kind of stakeholders from the top management to low level management and users must participate in security awareness programs. Based on their research, we can argue that in the field of security researchers, practitioners and managers are frustrated with security awareness efforts because of lack of classification in many issues of concern.

Literature has been written previously related to this topic.

Closing this literature review, I have to mention a survey related to this topic and conducted in Greece. This survey conducted in 2001. Loukis and Spinellis created a structured questionnaire and sent it to information system users of 53 Greek public sector organizations which yielded interesting results. There is a limited emphasis on training users of information system. The Greek public sector had only a basic level of information system security. Only the 35% of the respondent users had a proper training in the correct and secure use of information system. According to the authors, the main reason for that is the underestimation of the importance of proper training and security consciousness from the users. In general the main conclusion of that publication is that the information system security awareness level and the priority given to it have to be raised in the public sector [13]. However, this research aimed at the users and to what extent they are aware of secure attitude.

3. Research Question

By studying the recent research on Security Awareness, one can easily observe that researchers mainly focus on the attitude of the end-users and their security consciousness [2] [3] [4] [10] [12] [13]. The main topics of such research are the evaluation of the security consciousness of the users, the reasons that prevent users from acting in a secure way and the creation of models that have the maximum positive impact on their behavior and attitude in order to act securely.

In addition, research that has been conducted concerning Greece is that of Loukis and Spinelis in 2001 that is examining end-users' security consciousness. However, this survey is outdated (2001) and is referring only to the public sector of Greece. The security status of Greek companies probably has changed since then. The public sector consists of organizations that serve the private organizations and the citizens of a country, while the backbone of a country is considered to be its private sector which is the one that brings real value to the country and is of great importance for the continuous wellbeing of a modern organization.

Nevertheless, there is no literature yet, on employees' level of security awareness in the Greek private sector. To what extent do they behave in a secure way? Do they follow the security guidelines (if any) that top-management gives? Have they ever faced security incidents during their work? Questions crucial for investigating the current level of security awareness in Greek private sector lead to the main research question:

- ***What is the current level of security awareness in Greek companies?***

Several sub-questions occur directly from the main research question.

- To what extent do Greek companies provide Security Awareness programs to their employees?
- How do employees handle their passwords?
- Do employees follow company's security policies?
- How do employees handle security-related incidents?

With the term employees in the above questions, it is considered everyone who works at the company regardless their position in organization's hierarchy. The questions concerns from CEOs, Head of Department, Supervisors and the low level employees.

4. Theoretical Review

In this chapter, some introductory information is discussed. A theoretical review on important topics within Security Awareness field has been conducted. A more detailed definition about Security Awareness is given based on the literature and articles from the Internet. . Moreover, topics such as practices/ techniques/ policies as for Security Awareness, evaluation of it, pros and cons and possible barriers in implementing Security Awareness campaigns are gathered from recent literature in order to support the theoretical background of this research.

4.1 Security Awareness - Definitions

As it is mentioned before in this paper, Information System Security involves not only technical security controls, but also administrative, procedural and managerial controls [14]. The way that the users (employees, managers, IT personnel) employ the Information System of an organization plays a crucial role for the sustainability and the wellbeing of the system and apparently, for the information assets of the company. Security Awareness is the field of the science of Security that deals with human factor regarding the security of an organization's information assets.

Definitions of Information Security Awareness (ISA) are presented below, according to the literature that has been published.

Aggeliki Tsohou et al. (2008) published a review on Security Awareness investigating the gaps between theory and practice. Based on previous literature (NIST 800-50, 2003; Peltier, 2005; Katsikas 2000) concerning the definition of ISA, they quoted.

"ISA aims at attracting the attention of all users to the security message, making them to understand the importance of information security and their security obligations

Earlier in time, Maeyer (2007) defines security awareness as,

"an organized and ongoing effort to guide the behavior and culture of an organization in regard to security issues."

In 2003, the Information Security Forum (ISF) defines information security awareness as, "the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization, their individual security responsibilities, and acts accordingly."

It is worthy to mention the difference between Security Awareness, training and education that Aggeliki Tsohou et al. (2008) highlighted in her publication. Many researchers make this distinction between those three terms while there are others who consider them to be the same. In order to be precise regarding the aforementioned issue, it is going to be given an unofficial definition of the terms, which this paper is based on.

In this research, ISA is considered to be the level of security consciousness of IS users concerning the safety of information assets of an organization. Training is the tool which can raise the ISA of the IS users, while education increases the expertise of users (NIST 800-50, Aggeliki Tsohou et al., 2008).

As it mentioned before through the appropriate training, users' ISA can be raised. There are different types of training that have been employed in the past. In the next subchapter, practices, techniques and policies that have been referred in the recent literature are presented.

4.2 Implementation of Security Awareness (practices, techniques and policies)

In this section is presented a range of practices, techniques and policies that have been discussed in the recent literature. In order to proceed in the implementation of those techniques, one must evaluate the level of ISA of the users. By doing so, it is then known which practices and to what extent it must be implemented. The most common method, which is referred extensively in the literature [9] [23] [24] [25] in evaluating the ISA level of users, is by interviewing or questioning the users (a more extensive description is presented in the next subchapter).

4.2.1 Preparing an ISA campaign

In a more general view, J Andrew Valentine (2006) criticizes the traditional ISA training methods (at that point of time) that are within the 'one-size-fits-all' approach [6]. That means that specific ISA campaigns are applied to every organization and all the employees regardless the specifications of each company or the different features of each employee. A specific multi-phased methodology that is proposed by J Andrew Valentine (2006) seems to be the solution to this problem by analyzing the specific needs of each company and their employees. According to this methodology there are three phases; assessment, identification and education. Within this approach, at first, an assessment is being conducted in order to find out the current level of ISA of the users. After that, points that need to be developed are identified and finally the phase of training starts aiming at specific security areas that need enhancement.

Regarding the level of ISA, R.S. Shaw et al. (2009) distinguishes three main levels of it; perception, comprehension and projection [11]. In the first level of ISA, perception, users can just sense and detect possible risks that might harm the information assets of the organization. By giving an overall picture of the possible threats that could provoke damage to the company, users' ability in detecting security risks can be raised. Within the second level of ISA, comprehension, users can understand and assess the dangers that several security risks can pose. By achieving this level of security awareness, the way that users think and act about risks and controls can be altered. The final and most advanced level that a user can reach is the projection. While in an earlier stage users can handle a threat, within the level of projection they obtain the ability to project/ predict a potential threat and prevent a possible damage that it could provoke [11].

Assessing the current level of ISA and aiming at raising it to an advanced one are two of the most crucial steps in implementing ISA campaigns in an organization. Additionally, it is highlighted in the literature the separation of groups that are going to attend the ISA training. Users must be grouped based on their working position and their knowledge. Regarding the working position, there are several functions in an organization [6]. Few of them are key processes for the organization managing crucial information assets of it. Other functions do not make extensive use of company's information assets and as a result, users like them do not need in depth training. Moreover, users must be grouped according to their technical knowledge. Users with more technical knowledge should be trained in depth, while the other should attend the basic training first [6] [9] [27]. At this point, it is clear what kind of practices must be employed in order to achieve the specific goal and raise the ISA of users according to the needs of the organization.

4.2.2 Practices of ISA

Based on the literature several practices of maintaining (analyzing in next paragraph) or raising users' ISA have been noticed. In many cases, organizations set up a range of rules and guidelines in order to keep users' security awareness in a reasonable for the company level.

This kind of practice can distribute responsibilities but its effectiveness on keeping up the ISA of users is limited (behavior due to the users' lack of knowledge about the documents and information security as well as their lack of motivation for viewing the documentation) (Eirik Albrechtsen, 2007).

In the same study, ISA campaigns based on mass-media seem to be ineffective in influencing users' ISA level. It is stated that means such as mass-media offer one-way communication, which is not interesting to the receivers of the program [2]. This type of ISA campaigns includes practices such leaflets, booklets, films, posters, e-mails, presentations, seminars, intranet pages, screen savers, training courses, lunch meetings [2], [27]. Slovik (2000) in Albrechtsen (2007) support the two-way communication through information exchange and discussion. User-involving approaches in the information security can achieve alteration and development in users' behavior regarding security related issues [2]. Such approaches can be discussion, interactive workshops, problem solving, scenario thinking.

In addition, according to Prenski (2001) in Benjamin D. Cone et al. (2007) the use of video games as a teaching tool, triggers the interest of the users and makes them more active and willing receivers. That is approved in several sectors such as health, education, management etc. [3]. In the same way, Aggeliki Tsohou et al. (2008) argues that aiming at raising the users' ISA level and change their behavior, a two-way interactive communication should be employed in order to alter users' passive role into an active participation in the whole process [14].

Web based applications could not be missing in implementing ISA campaigns. Using the Web the problem of learning ineffectiveness can be surpassed [11]. Moreover, by analyzing and incorporating the Human Computer Interface (HCI) criteria into the design of ISA training programs, the interest of the trainees can be triggered and at the same time the effectiveness of the campaign can be increased [11].

R.S. Shaw et al. (2009) distinct ISA practices implemented in the media, in three main categories based on their ability to transmit knowledge. Hypertext, multimedia and hypermedia are the three aforementioned categories. Hypertext includes plaintext with hyperlink features. Within this practice, there is no available feedback. Multimedia constitutes the second category, which combines text, image, sound, music animation, video, virtual reality in a linear sequence. Still multimedia techniques do not provide feedback and interaction. The last one hypermedia uses video, graphics, plaintext, audio and hyperlinks in a non sequential structure, which can provide an interactive environment interesting to the trainees (R.S. Shaw et al., 2009). The three aforementioned categories can be assigned to the broader distinction of one or two-way communication that Albrechtsen (2007) refers to in his study. Hypertext and multimedia are within one-way communication, while hypermedia is a two-way interactive communication technique (presented in Table 1).

Much effort has been spent on analyzing how to trigger the interest of users in attending ISA trainings and how to keep their attention as long as possible. The article of Wendy Goucher (2009) is a very interesting publication combining ISA campaigns with the science of psychology regarding the human mind and memory abilities. She argues that there are three crucial elements that must be examined in order to achieve a successful security awareness training; attention, retention and motivation [30]. For this study it is highlighted the retention, which refers to the safely memorization of information that a human receives. From a psychological point of view, the human memory consists of two main types; declarative and procedural. The first one refers to the memories which can be consciously recalled such as facts and knowledge (e.g. road signs), while the second refers to unconscious memories such as skills with which people judge and change their actions according to specific procedures (e.g. driving a car). Based on the aforementioned, ISA campaigns should aim at learning through the procedural memory [30]. The need for practice and discussion within ISA training is of a great importance in order to achieve this [30]. The two-way communication and the interaction seem to be a tool that could assure the attention and retention from users' point of view.

4.2.3 ISA Policies

Each one of the aforementioned practices is useful depending on the culture, the organization style of the company and the specials features of the different groups of employees that are occupied there [29]. Based on those functions a general security policy must be designed, tailored to the organization's features, and be applied to the company's employees. Every company should have established clear security policies and guidelines widely known by employees in order to distinguish clearly the right attitude against the wrong. In that way, top management do not let employees to guess what is right or wrong [8].

A security policy gives the guidelines and sets responsibility areas within employees in an organization [2] [29]. Setting an information security policy is not a simple task in a company. Several aspects must be examined in order for the policy to be fitted to the organization. On the one hand, the hardware and software that is used should be fully analyzed [28]. Furthermore, the organization structure regarding the IT facilities must be taken into account. On the other hand, there is the '*social system*' which consists of the IS users [29]. Their educational level, especially the technological knowledge, has to be considered, as long as their attitude and behavior regarding the company's information assets [29]. Vital role for the security policy plays the organization culture [8]. In an organization, the establishment of a sub-culture within security policy is the key in order to manage the human factor which is involved in ISS [18].

M. Karyda et al. (2005) refers to three phases in setting up a security policy in an organization; formulation, implementation and adaptation. Formulation is a general plan, where the goals of the security policy are being defined in conjunction with the security measures and practices that will be employed. During the stage of implementation, users are being educated based on the security policy. Guidelines and procedures are set concerning their actions and attitude. Finally, in the last phase of adaptation, it is required by the users to follow the aforementioned guidelines and support them with their actions and behavior. A review and evaluation of the changes that the implementation provoked, is being conducted. The feedback is analyzed and several corrective actions are implemented if it is necessary. In Figure 1 below, the whole process is presented in a graph.

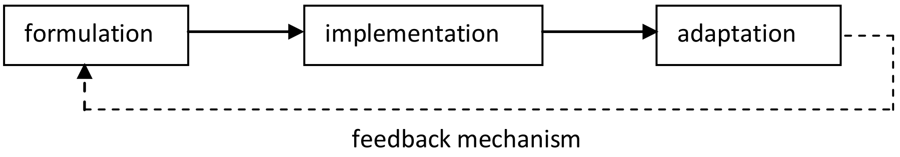


Figure 1: The security policy application process (source: Maria Karyda et al., 2005, 'Information systems security policies: A contextual perspective', Computers & Security 24, p.246-260)

Finally, there is a significant relationship between policy and reporting system of security related incidents. The reporting system consists of a crucial factor within security policies in an organization [15]. Every company should have included a reporting system where employees can state an unusual event. A clear procedure of reporting security related incidents could prevent the events to be widely extended and provoke huge losses to the organization. Top management should enforce employees to use the reporting system so it will have a clear image of what happened in the company. In a situation where employees do not care or do not know how or where to report an incident, a great range of security incidents can be noticed [8]. Strict penalties and punishments about events that happened unintentionally by employees can prevent the later to report them [20]. In that way, this event could be magnified and its outcome could lead to severe losses in the organization.

Table 1: Aggregated table of practices and their effectiveness on users' behavior.

Practices		**Effectiveness**	**Authors' reference**
One-way communication (hypertext, multimedia)	leaflets, booklets, films, e-mail, posters, seminars, presentations, intranet pages, screen savers, training courses, lunch meetings, e-learning(plaintext with hyperlink, image, sound, music animation, video, virtual reality)	No effect on behavior, boring procedure for receivers without paying attention and gaining knowledge	Eirik Albrechtsen (2007) Eirik Albrechtsen, Jan Hovdeb (2010) Benjamin D. Cone et al. (2007) Aggeliki Tsohou et al. (2008) R.S. Shaw et al. (2009) Wendy Goucher (2009)
Two-way interactive communication (hypermedia)	Discussion, Interactive workshops, problem solving, scenario thinking, Video games, e-learning(combination of image, sound, video etc. - The Web)	effective for changing users' behavior and development of their attitude	

4.3 Evaluation of Security Awareness policies and campaigns

As it was mentioned previously, among the three phases of Andrew Valentine's model, (2006), the first is the assessment of the current level of employees' ISA [6]. However, the evaluation phase after implementing an ISA campaign is of a great importance. Subsequently, the stage of applying an ISA program is referred. The crucial question after finishing an ISA campaign is to what extend was the campaign successful and met the primary goals.

It is referred extensively in the literature the issue of what exactly should be measured and which is the appropriate way to do it [6] [14] [25]. Aggeliki Tsohou et al. (2008) make a distinction of the possible answers of the great question, "what to evaluate?" based on the previous literature. The evaluation could refer to the awareness process itself, to the resulting change, to the level of audience awareness or to the ultimate return on investment [14].

The evaluation techniques are usually applied through questionnaires or interviews that are being conducted by the participants after implementing the ISA program [9] [23] [24]. There are references in the literature where the evaluation phase could be conducted by measuring indicators such as the virus infections or events that are recorded regarding the compromises of data integrity, confidentiality etc. [25] (Mathisen (2004) in [14]). It is important to refer the suggestion of NIST (2003) that merges the evaluation phase of ISA program with the program itself. In that way, practitioners must involve a series of questionnaires or interviews during the period of implementing the ISA campaign in order to identify the alterations that came out of the program [22].

However, the phase of evaluation is not a standard process and the researchers are still searching for the appropriate and most reliable way to evaluate an ISA program, which is thought to be of great importance. In this stage, top-management receives the feedback about the effort that has spent on raising the level of employees ISA. Moreover, correctible actions could be taken in order to close the gaps that may be caused by the previous ISA program.

4.4 Advantages and disadvantages of Security Awareness

After analyzing the field of ISA, how it can be evaluated and assessed, how can be raised and maintained, it is obvious which are the advantages, that could be gained by implementing ISA programs to employees of an organization. In this section, those advantages presented are based on the literature, while potential disadvantages that ISA programs can cause to the company's employees are referred according to researchers' study.

A well-designed ISA campaign could give several advantages to the organization's security. By doing so, knowledge about security related issues is transmitted to employees. After training, they are more cautious about security issues. Their attitude and behavior is changing to a greater secure level. Employees start participating and following the guidelines and procedures that information security policy indicates [26]. This can be translated in saving money, time and manpower while the chances in grabbing business opportunities are increased [9].

In contrast, a few disadvantages are being identified in the literature. Albrechten (2006) refers to the trade-off between the functionality and the Information System Security (ISS). Strict rules and guidelines are set by security policy and procedures act against the functionality of the work process. Many researchers have focused on the design of an ISA campaign. While a well-designed ISA program (i.e. who and how to train, organization structure, organization culture etc.) can give advantages as it is mentioned before, in the other case, an organization could face several losses and costs (i.e. effort, time and money) without gaining any positive result [2] [3].

Another disadvantage that was identified is the gap between the theory and practice in the field of ISA. There are still many ISA issues that are ambiguous in practice [14]. Such a fact makes practitioners to be frustrated in the implementation of such a program and consists of serious drawback of ISA. Finally, strict rules and security procedures can affect employees' communication channels. Bad communication can cause problems in their cooperation which could lead to problems in functionality and losses in the company in general [14].

Concluding, we can claim that advantages, which can be gained by ISA are of a great importance for an organization. Nevertheless, several disadvantages can be stemmed without paying attention in the design and implementation of an ISA campaign. A well-designed ISA program in a fully analyzed organizational environment (i.e. organizational structure and culture, specific goals in specific targets etc.) could minimize the risk of facing the disadvantages might stemmed by an ISA program.

4.5 Barriers in implementing ISA program

Closing the theoretical review, possible barriers that could appear during the implementation of an ISA campaign are discussed. Several barriers must be surpassed in order to reach the expected result and gain the advantages that ISA campaign can yield.

Briefly barriers that identified in the literature are presented below:

- Pure organizational budgets.
- Employees' computer skills -Language used to the campaign.
- Employees' lack of interest / top-management's lack of involvement.

First of all, the great issue of organizational budgets must be discussed. Top management does not pay attention in the field of security awareness [6]. Such a fact leads to a lack of resources which can result in a pure ISA campaign without a significant outcome or even not a practicing ISA training to employees at all [25].

To continue with, lack of interest of several stakeholders of ISA training indicates a crucial difficulty [2][25]. On the one hand, employees are not interested in ISA training. This is something that increases their responsibilities, changes their daily routine and raises the workload [2]. On the other hand, top-management lacks in involving in the procedure of ISA program and that does not help in triggering and motivating users to pay attention in the training and follow the guidelines [6] [25].

4.6 Conclusion

In this chapter, the theoretical background regarding the field of ISA was discussed in order to cover the topic of this research. In the beginning several definitions of ISA based on the previous literature were given. In the second sub-chapter an extensive analysis on the preparation and implementation of ISA campaigns and policies was presented. Consequently, the evaluation phase of ISA is discussed. Several advantages and disadvantages have been noticed through the literature review and are illustrated in the fourth sub-chapter. Finally, potential barriers that can act against a successful ISA campaign are discussed.

We could claim that each one of the practices and techniques that are referred has a specific goal to achieve (i.e. long term or sort term, detailed security knowledge or basic security knowledge etc.). Furthermore, each organization has its own features and ways to operate (organization structure, organizations culture etc.). First of all, an extensive analysis/evaluation of the needs of the organization must be conducted. A combination of practices depending on the company, the group to be trained and the grade of security knowledge that needs to be transmitted is the most successful tool in order to achieve the best results on raising and/or maintaining the level of ISA. Campaigns should be designed according to the policy that the organization would like to set up. Moreover, the policy that is going to be established must be fully analyzed and tailored according to the needs of each organization. In that way, it could be clear; which are the specific targets that must be processed, which is the level that needs to be reached and which are the practices that are going to be used.

The phase of evaluation consists of a non standard procedure that is still being discussed and studied by the scientific community. Nevertheless, it is one of the most crucial steps that should be carefully made in order to measure the results of an ISA campaign and lead to corrective reaction which is going to close the gaps remained.

Regarding the pros and cons we can claim that a well-designed and careful analysis of each case (i.e. the implementation of ISA campaign in a specific organization) could be the key factor to avoid disadvantages and restrict them out of the procedure. A wrong and pure in design ISA program can provoke losses and several costs to the organization.

Finally, potential barriers can lead to an unsuccessful ISA campaign. Again, the phase of designing and analyzing a case of an organization in order to apply an ISA campaign could act as a prevented tool for surpassing those barriers. Barriers that mentioned are based on the human factor, both the end users and the top-management, and that is why they are difficult to surpass.

5. Research Methodology

In chapter three, the methodology that is chosen for conducting this research was introduced. More detailed, within the next sub-chapter, it is analyzed, how the survey was designed and how the sample was defined. Moreover, an extensive reference on the way of construction of the questionnaire is presented in the following section supported by the literature.

5.1 Sample and survey design

Two main methods of scientific research were used in order to accomplish the goal of this research and reach the desirable results.

- Literature Review
- Quantitative analysis through questionnaires or Descriptive research

First of all, an in depth study and analysis of recent literature that has been written in academic level was conducted. Several articles, papers, monographs and books were gathered through the Internet from specific web sites (Appendix A).

The required data was gained by means of measuring employees' current level of Security Awareness in Greek companies by means of a survey. Within this survey, a quantitative analysis was conducted and useful data are gathered to answer the main question of this research. There is not any previous research aiming at employees' consciousness concerning Security Awareness in Greek private sector. To be more precise a specific industry was chosen for investigation, the industry of Greek, private, ICT (Information and Communication Technology) companies. Geographic limitations could be over passed due to the nature of this specific industry. An ICT company can easily operate beyond the borders of its physical existence with the use of internet. A descriptive research is designed to reveal the current level of security awareness and give an answer to the main research question. A structured questionnaire was created and sent to the majority of Greek ICT companies aiming at all kind of employees working there. In total, three sources are used in order to identify target-companies of this survey. The main source of addressing the target-companies for this survey is:

- www.sepe.gr/gr/Members : "Federation of Hellenic Information Technology & Communications Enterprises (SEPE). It is a non-profit organization, established in

> 1995. SEPE's members collectively they hold more than 95% of the country's turnover in the Information and Communications Technologies Industry."

SEPE is the oldest federation where the majority of Greek ICT companies are gathered I order to be organized and develop the sector of ICT in Greece. All those years more than 95% of ICT companies are gathered in this federation as SEPE mentions. Moreover, two more web pages which operate as directories of various businesses all over Greece are used to further reinforce the survey.

- http://www.ananas.gr/directory/
- http://dir.vres.gr/category.php?cat_id=12

Both of the web pages consist of pan-Hellenic directories of Greek private organizations in several sectors/industries of the market including the industry of Information & Communication Technology.

At first, questionnaire was sent to three different function levels within Greek ICT companies in order to review the structure and the content of the questionnaire. For this pilot survey, one CEO and founder of a company selling IT hardware and software products, a project manager of a company which sells hardware and software while developing their own software and finally, a programmer of a software development company sent their feedback in order to further develop the questionnaire. The three people who completed the pilot-questionnaire did not participated in the final survey.

Afterwards, the questionnaire was sent to the target-companies (65 in total) through e-mail explaining the nature and the purpose of the survey (further information is given in Appendix C). The starting date of the data collection is 15/11/2011. The progress of the data gathered was not satisfactory. Companies seem not to be willing to participate in the survey. On 25/11/2011 a second e-mail was sent to the same companies in order to remind them of the survey that is running. On 10th of December, collection of data finished and only 71 employees had participated in the survey. Greek employees' unwillingness to response in the survey is obvious, but this consists of a finding in this survey. Further information about the findings is presented in the section of Results.

5.2 Questionnaire design

In this section, the structure of the questionnaire is described. Based on the literature (mainly [6] [12] [22] [25]) a structured questionnaire was designed in order to gather data for answering the main research question. Previously on time, researchers have conducted similar surveys (Terpsiadou, Economides, 2009). Based on those surveys and additional studies that support other parts of the questionnaire, the later was created and consists of 5 items of 20 questions in total. Below, those items and questions are described in detail among their interconnection with the theory.

The nature of questions, words that are used and the way of asking questions and the expected answers are based on the Don A. Dillman's book; "Mail and Internet Surveys - The Tailored Design Method", (2007). Due to the nature of the survey and the way of collecting data through questionnaire that was sent through the Internet, a self-administered questionnaire is an appropriate tool for this research [33]. Based on the principles that Dillman defines in his book, each one of the questions used in the questionnaire are carefully designed and tailored in the needs of this survey and the specific topic.

5.2.1 Measurement

In this section the measurement of the questionnaire is analyzed supported by similar previous studies and further literature (mainly [6] [12] [22]). It is separated in five (5) different groups; Demographic data, Technology Usage, Information System Security, Physical Security, Password Usage. The first two parts are focused on data concerning the respondents' personal details about them and their role in company's Information System. To continue with, security is separated in physical and information system security. That is why there are two separated parts in this questionnaire with each question cover a specific section of this security aspect in a general way. The last part is getting deeper in the security field concerning the part of passwords. In the majority of previous surveys password field consist of an important field in order to measure the level of security awareness. The five parts of the questionnaire are further discussed below.

At first, a set of demographic questions was created in order to gather information about the background of the respondents and their personal information. Afterwards, in the part of Technology Usage, information is gathered about the role of respondents in the Information System usage. To continue with, the general category of security has split into two main categories; Information System Security (ISS) and the Physical Security (PS). Within the third and the fourth groups, questions about respondents' behavior and attitude concerning Information System Security and the Physical Security are asked. Those questions gather general information about the two topics. Finally, a set of questions, which are more detailed concerning the Security Awareness, collect information about how respondents handle and manage their passwords. The password usage consists of a common topic in similar surveys in the past. Information can be gathered about the behavior and the attitude of employees concerning Security Awareness. First of all, to what extent do the respondents use the IS of their organization. Afterwards, the daily habits regarding Information System Security and Physical Security take place. Finally, the most common technique in order to investigate the level of Security Awareness is the password handling by end-users.

Below a more detailed reference of the construction of each one of the questions is presented ordered by the groups that are defined previously. By the abbreviation Q.## writer refers to the number of question that is recorded in the questionnaire in Appendix C.

5.2.1.1 Demographic data

In the first part of the questionnaire (i.e. *Demographic Data*) a set of questions (4) ask for personal information about the participant. Based on the theory and mainly on surveys ([6] [12] [21] [22]) items were reviewed from previous similar research and tailored in the needs of this specific survey.

Data about the age, the working position, the educational level and the seniority of respondents are gathered in this part. It has been referred plenty of times in the literature the issue of the final receivers of ISA training. In the beginning ISA trainings were conducted concentrated on the end users of IS. Later in time, the need of training upper levels of management was stemmed [6] [21]. NIST (2003) states that all the people that are related to the company's Information System must be trained in order to understand their roles and responsibilities and follow organization's security policy and guidelines. Based on that, it would be interesting to investigate to what extent the working position is related to the ISA level. Four areas are distinguished; CEO, Head of Department, Supervisor and employee [12] [22].

Regarding the age of respondents (Q.2), the measurement has been set based on the previous research conducted by Terpsiadou and Economides (2009); a)18–30, b)31–40, c)41–50, and d)over 51 [12].

Based on the same article, [12], which describes a survey on ISA level of Greek public sector, the educational level of respondents (Q.3) has defined; a)primary education, b)secondary education, c)higher education, and d)postgraduate/doctorate.

Finally the seniority level has defined based on Terpsiadou and Economides (2009). The measurement for Q.4 consists of a)0–14, b)15–24 and c) over 25. The three last questions are based on the same article, [12], which is a survey on ISA level of users in Greek public sector. This is a good reflection of the Greek reality regarding the seniority level, the educational level and the age of employees and that is why the measurement has been used in the same way. In the same way like the working position, seniority level could be influence the ISA level of the respondents.

5.2.1.2 Technology Usage

The second part (i.e. *Technology Usage*) consists of questions (4) which refer to the current status of the participant related to the IS of the company. Here in this part, information is gathered about the current usage of the IS by the participant, the preparation of using the IS and if the participant has attended any ISA training program before of filling the questionnaire [1] [6] [22] [25].

0reHere, the questions are related with the usage of Information System by the respondent. Which is the role of the respondent concerning the IS? What kind of privileges does he/she have on the IS? Did the participants have the appropriate training on using the IS?

Q.5 refers to the extent that the respondent can use the IS. It is based on NIST (2003) which makes clear reference to the separation of privileges and the responsibility areas among users of an IS in a company [22].

Q.6 refers to the training that users must have before start using an Information System. Crucial for the well-being of an organization's system is the way that users have learnt to use the IS. An organization can use several Information Systems. It is mentioned in the question and three possible answers derive from this. "Yes for all the IS", "Yes for some of IS" and "No for none of IS" that the company might use [1].

Q.7 asks respondents if they have significant security responsibility. Based on NIST (2003) it is important for the security within an organization that the employees realize their responsibility regarding the safety of company's assets [22].

In Q.8, a Yes/No question make the first reference to Security Awareness. Respondents are asked if they have participated in any ISA program in the past. A derivative of this item is the next question which is referred to the reasons that according to respondents that not participated in an ISA training. Based on the literature, three main reasons have identified;

lack of time, lack of funds and lack of SA meaning while a fourth option is given to participants in order to fill their own perspective [6] [22] [25].

5.2.1.3 Physical Security

Afterwards, three parts follow which are referred to ISA and gather information about the behavior and the attitude of participants in security related issues and procedures. Several articles and publications previously mentioned in this study are relevant here: [6] [9] [14] [22] [23] [24] [25]. In this study, the general meaning of ISA which consists of several different tasks has been split into two main categories; Security of the information System in a company and security of the physical assets of it. In order for the level of ISA to be investigated, it is necessary to gather data about participants' behavior concerning both physical and electronic aspect of information. By distinguishing those groups, a range of questions based on the theory ([8] [22] for Information System Security and [2] [35] for Physical Security) are being asked in order to collect information about participants' behavior in security related procedures.

In the section of physical security, a set of five questions related with the security regarding the physical assets of the company are presented. Questions are based mainly on the publications of Eirik Albrechtsen (2006) and Dario Forte & Richard Power (2007).

In both of the aforementioned articles, the safety of the organization's building is being highlighted. Crucial for the company's assets is to control the access in buildings and specific areas of the company. Furthermore, everyone entering the company must have special badge that indicates the specific reason of being there [2] [35]. Q.9 makes a reference on how the participants entering the company's building. Possible answers according to previous research are; "I just enter the building freely", "The reception opens the door after checking my ID", "I use my special magnetic card" while an option for another personal choice is given to the respondent (i.e. "Other") [2] [35]. Q.10 is asking how the participants act in case of seeing a stranger in the company [22]. The answers had been chosen are the followings; "I lead him/her to the destination that he/she wants", "I follow the policy of the company (e.g. lead him/her to the reception in order to be registered as a visitor)", "I do nothing" and "Other" in order to be filled by participants who act in a different way from the aforementioned.

The last question of this section refers to the safety of the data center of the organization (servers, network communications, storage areas etc.) [35]. Q.11 is a YES/NO question that examine if the respondent has access to that sensitive area of the company.

5.2.1.4 Information System Security

The part of Information System Security (ISS) refers to actions that are taken in order for the Information System to be kept safe. It has been referred extensively in the literature, in which mode do the users leave their terminals when they leave their office. At first, Q.12 asks if the respondents lock their system when they have a break or meeting etc [2].

To continue with, Q.13 is based on NIST (2003), and it is referred to the actions that respondents take into account in order to keep their system in a safe shield. Four main practices according to NIST (2003), are presented through YES/NO questions; password usage, data backup, antivirus protection and report incidents.

Based on NIST (2003) and Carl Colwill (2009), survey continues with focusing on the reporting system and the users' attitude concerning this task.

Q.14, asks the reasons that could prevent users from reporting a security-related incident. No sufficient policy from company's point of view, fear of potential penalties and loss of benefits are three of the options that respondent can choose [8] [22]. Additionally, a fourth option (i.e. 'other') of expressing their own opinion is given to the participants.

The last item in this section, Q.15, refers to security related incident that the respondents have faced in the past and if they reported it (this consists of Q.15.1).

5.2.1.5 Password Handling

Regarding the last part of the questionnaire (i.e. *Password Handling*), it is noticed extensively in the literature as an example of measuring ISA level in IS users the password handling. Also, most of the later on time similar surveys have included a separate group of questions asking password-related issues to participants. Based on that, the fifth part refer to the way that participants handle their passwords; how do they create them, how do they remember them, how often do they change their passwords [8] [26] [34].

The most common way in order to protect an IS and limit the possibility of compromising the IS, is the combination of username and password [34]. However, this technique seems to be much more ineffective when the human factor is involved. Users tempt to generate predictable password in order for them to remember those easily [26] [34]. Another common mistake that is made by the users is the habitat to write down and post their passwords in their desks. In many previous studies, researchers use the password handling in order to investigate the level of security awareness of end-users. In the last part of the questionnaire is researched the way that respondents use the passwords.

Questions about using different passwords for different platforms/applications, the way that respondents remember their passwords, the number of characters that they use, the frequency of changing them and the content of the password itself are asked to the respondents. Researchers refer the importance of using different passwords for different platforms/ applications. In that way, even if one of them has been compromised, it wouldn't have lost all the crucial data that users keep in different application or web application (i.e. email, e-banking, e-shopping etc.) [26] [34] (referred to Q.16).

Q.17 is referred to the way that respondents remember their password(s). A common problem, as it has been previously mentioned, is that users post their password prominently (e.g. in the monitor), or sharing it with third people (colleagues) [34].

Crucial for the strength of password is the number of digits is used. Q.18 is referred to this issue. It is well-known that a strong password must include eight or more digits (also referred in [34]). The measurement defined from a range of 4 digits to more than 10 digits (a) 4, b) 5-7, c) 8-10, d) >10) in order to investigated the proportion of the respondents that pay attention or not in such a crucial issue.

The frequency of changing the password is of a great importance concerning the level of safety. Researchers have concluded that, in order for a password to be safe and secure, it must be changed every month [34]. In Q.19, the measurement is defined based on that reference (a) "At least every week", b. "Every few week", c. "Once a month" and d. "Never").

Finally, Q.20 is referred to the complexity of characters that are used as a content of passwords. A common mistake by the users is the generation of passwords based on personal data (date of birth, name, working position, department etc.) [26] [34]. The complexity of password is of a great importance. Many different types of characters must be used in order to assure the strength of the password (a combination of special characters, upper and lower case letters and numbers) [22] [34]. Based on the aforementioned six options are given to the respondents; "Personal data (date of birth, your name, your age etc)”, ” Randomly generated passphrases”, ” Lower case letters”, ” Upper case letters”, ” Numbers”, ” Special characters (!, @, #, $, %, ^ etc.)”.

6. Results

From the 65 companies that the questionnaire has been sent, only a few of them participated in the survey. Due to the confidentiality of the data, there is no log kept with the details of each company that took place in the survey (i.e. who answered what). Most of participants replied after receiving the notification mail that has been sent 10 days after the initial request for participating in the survey. Most of the companies did not send any kind of feedback for the research. Only 2 out of 65 companies replied negatively by e-mail, stating that they are not willing to respond to this questionnaire. They referred clearly that they do not want to share that kind of information concerning security, with entities outside the company.

More specifically, Mr. X (the name is not referred for reasons of confidentiality), of a company stated[4], 'Pay attention to the last part (or even remove it)'. Mr. X was referring to the last section of the questionnaire regarding the password-related questions. He considered that the depth of details that were asked goes beyond the limits of security. Mr. X continues with referring the department of Greek police responsible for the e-crime section; 'be aware of the office against the electronic crime and I'm afraid that if you continue', (i.e. with this survey), 'many people are not going to understand the real meaning of your master thesis! In this period that we are living everything around us is suspicious. You may replace your questionnaire.' That reflects several thoughts about Security Awareness in Greek private sector. The issue is discussed further in the 'Discussion' section of this paper.

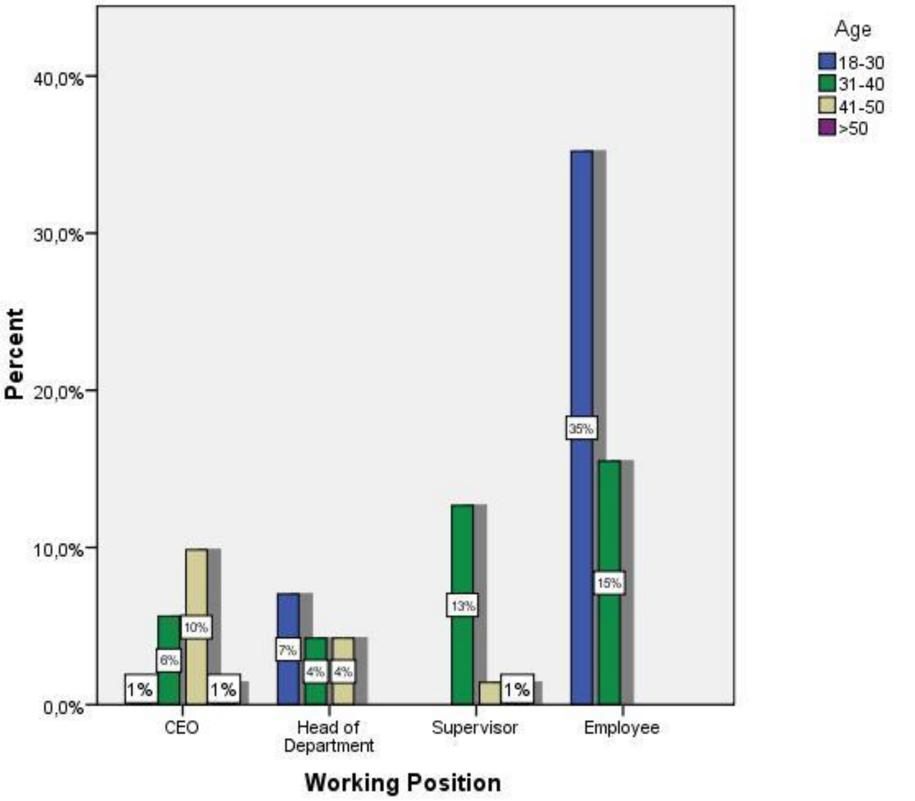
After receiving the completed questionnaires, data were inputted to the SPSS statistical tool. A statistical analysis was performed and interesting results describing the current level of security awareness in Greek companies were gathered. Interesting findings are illustrated later on this chapter. In the first section of the chapter, general information is presented about the respondents of this survey. Frequencies that describe several measurements about Security Awareness are illustrated in tables and graphs in the following section. Finally, during the data analysis, differences in the level of security awareness are noticed concerning respondents' working position and years of seniority. For that reason, chi-square analyses between those variables are performed in order to present the strength of dependence that occurred.

[4] The original message is presented in Appendix B in Greek language giving the precise translation of it in English.

6.1 Demographics

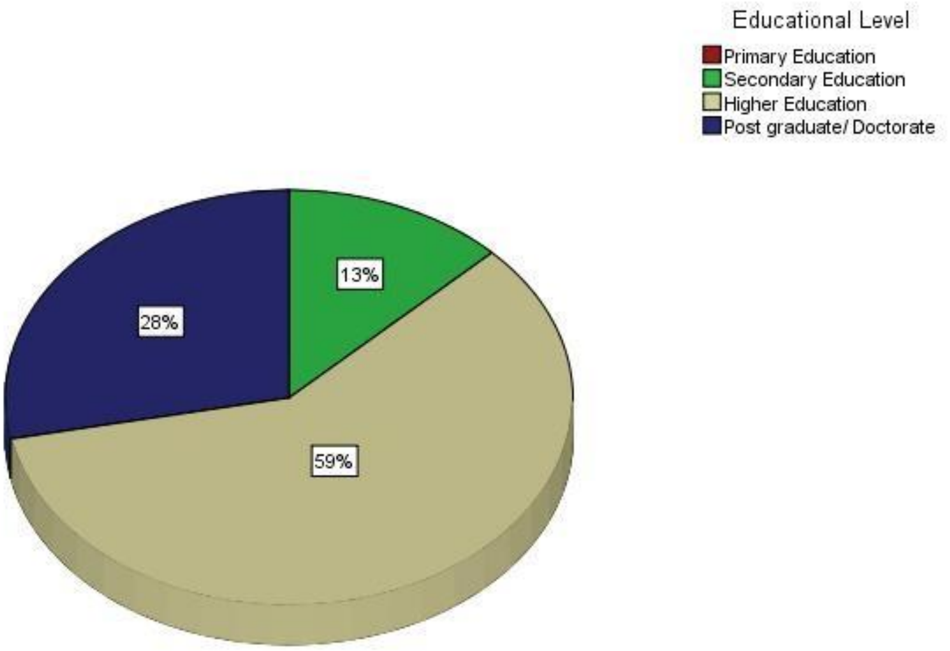
Here is presented the general profile of the participants in this survey. Half of the respondents are employees, 36 in number (51%). Equal amount of Head of Department and Supervisors recorded with the frequency of 11 respondents (15%). Finally, the number of CEOs who participated in the survey is 13 (18%). It was expected that the number of employees to be the majority of the respondents. On the other hand, the number of participants in the working positions of Head of Department and Supervisor is small due to the companies' profile that respondents work. Most of the companies that participated in the survey must be small and medium size companies where the working tasks are not sufficiently separated.

The age of respondents varies mainly between 18 and 40 years old. 31 of the respondents (44%) are between 18 and 30 years old and 27 of them (38%) are between 31 and 40 years old. 11 of the participants (15%) are between 41and 50 years old while only two are over 50 years. The majority of the respondents in this sample are young people that either work in a company or run their own business. Interesting enough is the Bar graph 1 that shows the working position of respondents based on their age.



Bar graph 1: Working position and age of respondents.

Quite increased is the educational level of the participants. Most of them, the number of 42 respondents (59%), have at least a university degree (higher education). 20 of the respondents (28%) have post graduate or doctorate education, while only 9 of them (13%) have reached the secondary educational level. Below in the Pie chart 1, the frequency of participants' age is illustrated.



Pie chart 1: Frequency of Age

Regarding the working years of respondents in that company, the majority, 57 respondents (80%), work in the company from 0 to 14 years, while only 14 of the participants (20%) are working between 15-24 years in the company. It is remarkable that none of the respondents has worked more than 25 years at the time that the survey took place. Based on that information, it is considered that the sample mainly consists of people that recently started working in those working position.

6.2 Other remarkable measurements

It is important for a survey about security, to investigate the role of every participant in the Information System of the organization that it works. The majority of the respondents are simple users (55%), while 29 of them (41%) have administrative privileges in the company's system. Meanwhile, the great majority of the participants had the appropriate training for some of the Information Systems that they use (63%), while only 14 respondents report that they had a fully training program. 12 respondents (17%) had no training at all before starting to use the Information Systems of the organization. Moreover, there is a great gap between the aforementioned and the frequencies of the significant security responsibility that reported by the respondents. Most of the respondents (60%) stated that they do not have significant responsibility regarding the security of information assets in the company. 24 participants (35%) stated that they have responsibilities concerning the security, while 4 respondents (6%) stated that they are not sure if their role is important for the information system security.

6.2.1 Information System Security Awareness

Concerning Information Security Awareness (ISA) programs that respondents may have participated during their career in that working position, results show that only 24 of the respondents (34%) have participated in ISA programs that the company organized. The rest of the participants, 47 of them (66%), have not attended any Security Awareness training(s) while working in that specific position. An interesting finding is respondents' opinion regarding the reason that they have not yet participated in an ISA program. 8 out of the 47 respondents (17%) that had no ISA training claim that the busy schedule is the repressive factor. 12 of them (25%) support the lack of funds that prevent top-management for not organizing ISA program. The great majority of the participants (38%) believe that the main reason of not taking ISA training is that the top-management does not pay attention in this field and does not consider it important for the safety of company's information assets. It could be claimed that they belong to the great majority of respondents that believe in lack of ISA meaning. Finally, 9 of the respondents (19%) expressed their own point of view. 2 out of 9 claimed that they work in a small company and such a program is out of the scope, while 3 of the 9 could not answer.

The last not least important measurement of this section is about security-related incidents that respondents have faced and their reaction. Half of the participants (51%) stated that they have experienced a security breach during their working hours. The great majority of those participants, 30 out of 36 (83%), have reported the incident to the responsible person or department.

6.2.2 Physical Security measurements

This section is about measurements regarding the physical aspect of security in companies.

Most of the respondents stated that in their company's building after reception's control (39 out of 71, 55%), while 12 participants (17%) stated that they use magnetic cards in order to open the company's main entrance. It is remarkable that 20 of the participants (28%) walk into the company freely. Even if there are small and medium size companies participated in that survey, they had to take care of the physical security. They must have a control procedure in order to check who enters the company.

To continue with the physical security, interesting is the reaction of the participants when they meet a stranger inside the organization. 20 out of 71 (28%) lead the stranger where he or she wants. The rest of the participants are almost equally allocated in two completely different answers that are given. 24 respondents (34%) replied that they follow company's policy, which means that top-management has considered this issue, while 25 of them (35%) replied that they do not react in this case. In total, 63% of the participants does not handle this issue in a proper way for the security of the organization.

Finally, concerning the core task of an IT company, which is its data center, 34 respondents (48%) have access to that room, while the rest (52%) don't. This might be useful information combined with other data that come from the questionnaire and it is further analyzed in following section.

In an overall view of the physical security of the sample, it can be claimed that in Greek IT companies, top-management does not take into serious consideration the physical security. However the majority of the companies use a control procedure in entering company's building (reception, magnetic card), there is a non-overlooked percentage of participants that are moving freely inside and outside the company without being controlled. Meanwhile, a great number of participants do not react when they see a stranger inside the company, which can lead to serious loses for the organization.

6.2.3 Information System Security Measurements

Regarding the safety of the Information System in an organization, each one of the employees-users in work stations has a part of responsibility in security. Out of 71 respondents, only 18 (25%) lock their work stations, while 22 respondents (31%) do not lock it at all. Most of them, 31 with the percentage of 44%, do lock their work station every time they go way for different reasons (break, toilet, lunch etc.). In total, the small percentage of 25% of the participants always leaves the work station secure against any threat.

It is of a great importance the practices –password, backup, antivirus protection and report incidents- that are used in order to protect the Information System from potential threats. The majority of the participants (34%) use password and antivirus protection only, while the 30% of them use the data backup in addition. Only 20 out of 71 respondents (28%) use all the four practices for securing their work stations (as proposed by NIST SP800-50).

Finally, the great majority of the participants, 73%, believe that the main preventive reason for not reporting security related incidents is the lack of sufficient policy in the organization. When the responsibility areas are not clearly separated and there is not any specific procedure in order to report incidents in the appropriate person/ department, employees/ users of the Information System avoid or do not even have the chance to report incidents. 11 participants stated that they would not report such an incident in order not to lose benefits.

Based on the aforementioned, it can be claimed that the Security Awareness concerning Information System in Greek IT companies is not in high level. Only the small percentage of 25% of the participants keep their work station locked every time that they left it for any reason, while only the 28% of them use all the four practices against both the internal and external threats.

6.2.4 Password handling Measurements

In the great field of password handling, many interesting findings come up from the survey. Half of the participants (51%) have different passwords for the different applications that they use during their work, while the rest (49%) use only one common password in all applications. It is notable the way that the respondents remember their passwords. 57 out of 71 with the percentage of 80% remember their password(s) by heart, while only 14 of them (20%) stated that they keep a note somewhere in their desk in order not to forget it. No other ways were mentioned in order to remember their passwords.

The frequency of changing the password is a crucial factor for the safety of the information system. In order to keep the safety in high levels, users must change their passwords once a month. Only the 24% of the participants follow the aforementioned, while the vast majority of the respondents (75%) do not change the password at all.

Regarding the issue of the numbers that are used in passwords, it is wide known that passwords must include 8-10 characters. The results agree with that and the great majority of the participants, 55%, stated the same, while the 35% (25 out of 71) of them use 5-7 characters. Additionally, small percentages use only four characters (2 out of 71, 3%) or more than 10 characters (5 out of 71, 7%) in their passwords.

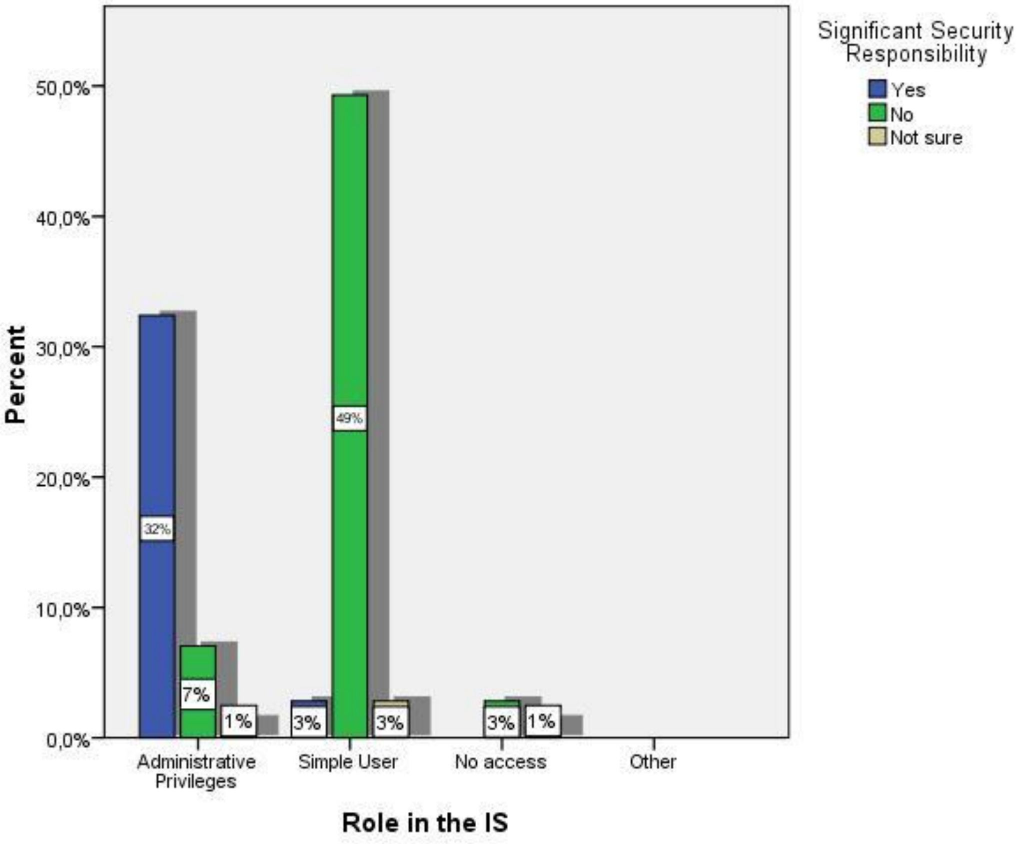
[Content] Crucial for the strength of the passwords is their content. A combination or different groups of characters makes the password stronger therefore, it is more difficult to break them. In this task, participants' replies vary. It is worthy to mention that the majority of the respondents with only 14% (10 out of 71) uses the most difficult combination of different characters in their passwords (including randomly generated passphrases, upper & lower case letters numbers and special characters). To continue with, 9 out of 71 (13%) use their personal data altered by different kind of characters. However this consists of the majority of replies, those percentages are still very low. It is remarkable that 51% of the participants use their personal data as a password(s), but nevertheless, most of them still trying to enforce the strength of passwords by using combination of different kind of characters.

In general, regarding the field of passwords, it can be claimed that employees in Greek IT companies have a medium to high level of consciousness concerning security in passwords, applying most of the basic requirements that a password needs in order to be strong. What does not keep them in the highest level is that the majority uses only one password for several information systems and/or applications, while most of them are not used to change their password(s). Finally, the extensive use of personal data in passwords by the participants drops the level of security in them.

6.3 Various clustered Bar Graphs

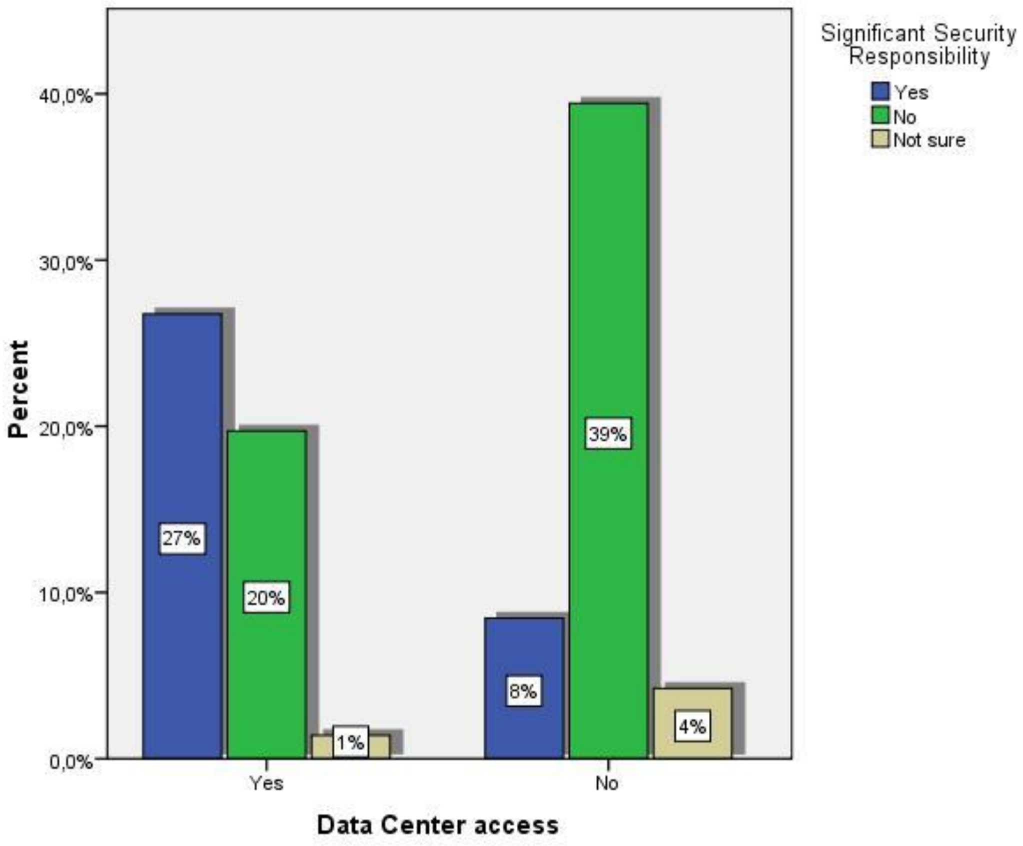
In this section, clustered bar graphs are presented, showing interesting findings about the level of security awareness in this sample of Greek IT companies.

In the bar graph Bar graph 2 below, it is clear that most of the employees with administrative privileges are conscious about their responsibility in the security of organization's information assets (79%). However, there is a small percentage of participants, (21%), who while they have administrative privileges in the information system; they believe that they do not have an important role in the safety of Information System.



Bar graph 2: Role in the information System and significant security responsibility.

To continue with the great issue of responsibilities areas in a company, another bar graph (Bar graph 3) below, illustrates participants' access in the data center of the organization with their security responsibility. The data center of a company, especially for an ICT company, is of a great importance concerning security. All the data and the services that the company offers to its customers are stored and operated in there. Thus, this specific room should be well protected from both natural and human related disasters. Regarding the human factor, only specific employees should have access to the data center while a log should be kept in order to record who got in and what the reason was. However, it is remarkable that the 44% of the respondents have access to the company's data center, while simultaneously they believe that they do not have or they are not sure if they have significant responsibility concerning the organization's security. According to those measurements, it could be claimed that the data center is not properly secured regarding its physical safety.



Bar graph 3: Access to data center and significant security responsibility.

6.4 Chi-square analysis

Though the data analysis, differences in ISA level of respondents regarding the working position and the years of seniority was observed. In this section the differences between the working position of participants on one hand, and the differences between their years of seniority on the other, are analyzed based on the chi-square analysis. Through chi-square analysis the dependence between variables can be found in a small sample like this. In the tables that follow (Table 2 and 3 the significant dependence between variables is highlighted).

6.4.1 Differences between working position

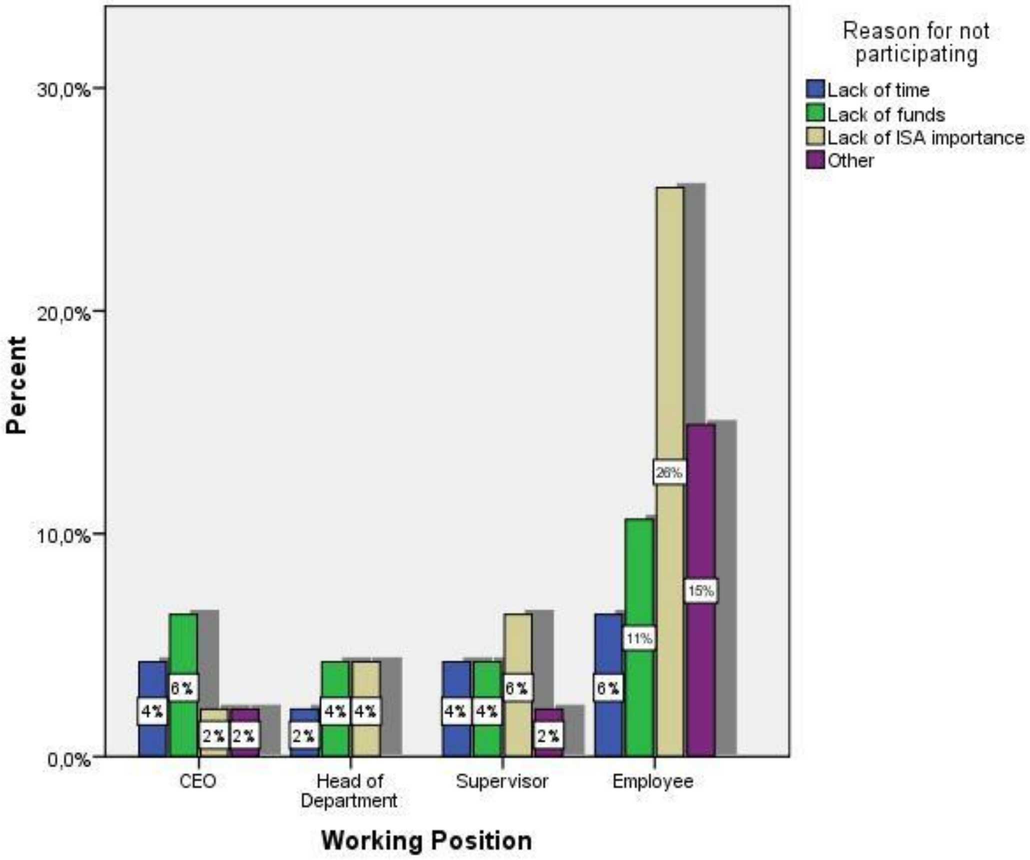
Below, in the Table 2, the results of chi-square analysis with the rest of variables are presented.

Table 2: Chi-square analysis in working position.

	x2	*DF*	*P*	*Contingency Coefficient*
Working position	-	-	-	-
Age	43,889	9	**0,000**	0,618
Educational level	13,552	6	**0,035**	0,400
Years of seniority	14,539	3	**0,002**	0,412
Role in the IS	19,325	6	**0,004**	0,463
Training for the IS	5,739	6	0,453	0,273
Significant security responsibility	23,879	6	**0,001**	0,502
Participation in ISSA program	4,458	3	0,216	0,243
Reason for not participating	6,383	9	0,701	0,346
Entering company's building	9,836	6	0,132	0,349
Behavior to a stranger	16,419	9	0,059	0,433
Access to Data canter	3,155	3	0,368	0,206
Locking work station	15,277	6	**0,018**	0,421
IS security techniques	27,136	15	**0,028**	0,526
Reason for not reporting incident	7,185	9	0,618	0,303
Experience of security related incident	1,417	3	0,702	0,140
Report it?	0,107	3	0,991	0,054
Use different passwords	15,725	3	**0,001**	0,426
Way of remembering password(s)	1,806	3	0,614	0,157
Num of password(s) characters	5,391	9	0,799	0,266
Frequency of password(s) change	14,035	6	**0,029**	0,406
Content of password(s)	69,077	75	0,671	0,702

Working position differences in reason for not reporting a security related incident

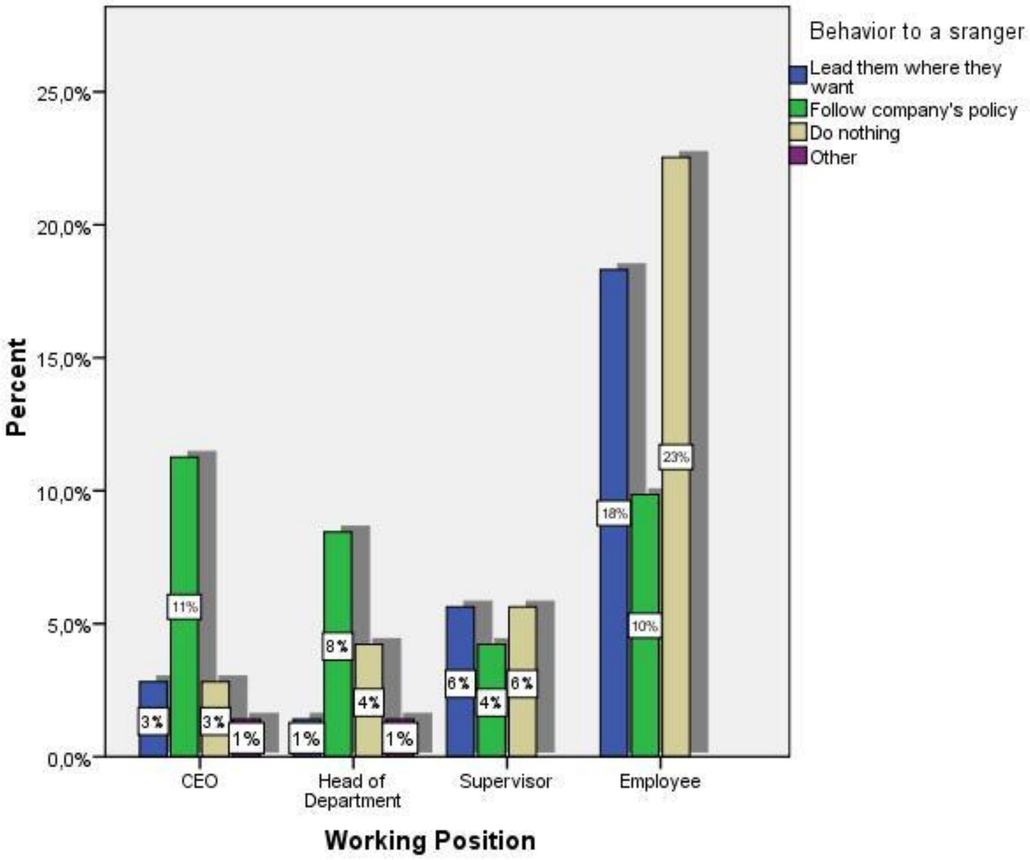
The first notable point that derives from the table above is the working position differences with the reason for not participating in an ISA. Most of CEOs, 71%, claim that the lack of both funds and time consist of the main reasons for not participating or not performing ISA training programs in the companies. On the other hand, the majority of employees, 67%, believe that the main problem in that task is underestimation of such programs, which could be claimed, that comes from the top-management. A gap between beliefs of CEOs and employees is noticed. It could be claimed that the communication channels between those two stakeholders in companies must be redefined and designed in order to achieve a common policy and guidelines. In the Bar graph 4 below, this gap is clearly presented.



Bar graph 4: Working position and reason for not reporting.

Working position differences in behavior to a stranger

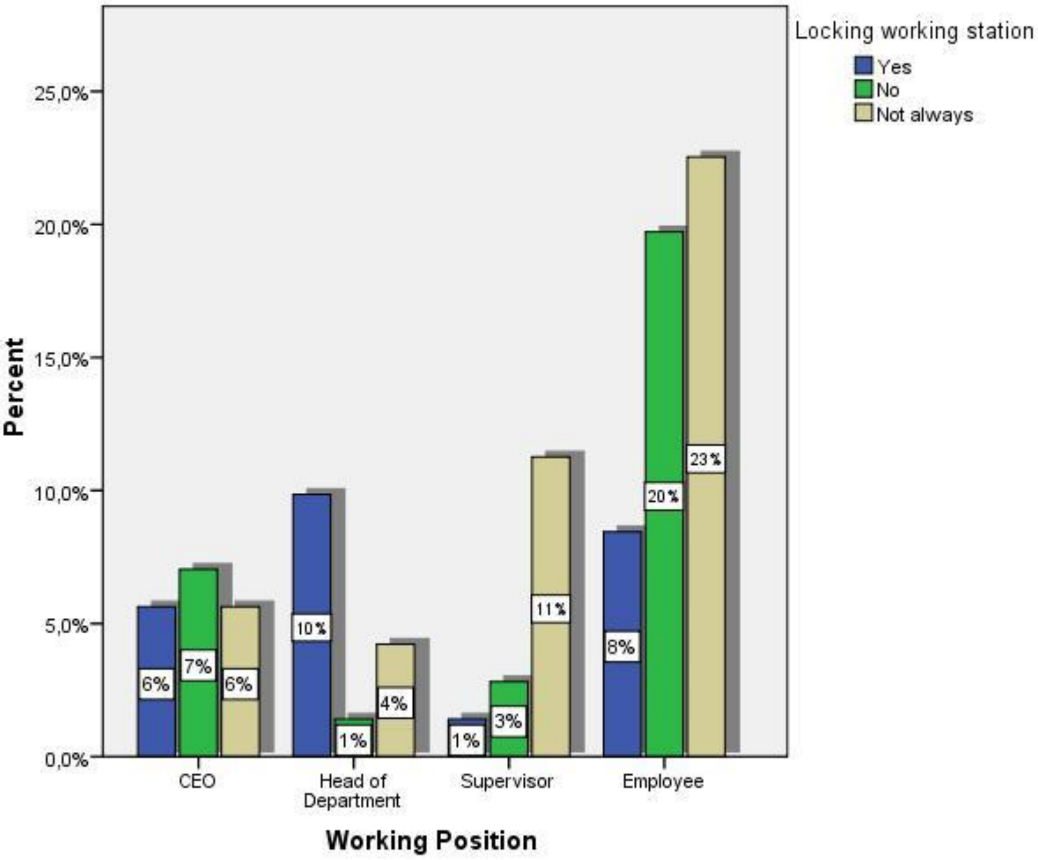
As bar graph 5 shows, there is a difference between the way that CEOs react in the sight of a stranger and the way that employees do. 8 out of 11 CEOs (33%) follow the specific policy that probably exists in the organization. On the contrary, employees who stated that follow company's existing policy are only 7 out of 36 (19%), while the majority of them (44%) do not react at all in the sight of a stranger inside the company. It is obvious that top-management do not handle in a proper way their communication with employees. Even if standard policies exist within the studied companies, they are not well-defined and known to their final receiver - employees of the organization.



Bar graph 5: Working position differences in behavior to a stranger.

Working position differences in locking their work station

A quick look at the Bar graph 6 shows that both for CEOs and employees it is not usual to lock their work stations when the go away. The 69% of the CEOs do not lock their work stations or do not lock them always. Meanwhile, the 70% of the employees act in the same way like their top-management does. It can be claimed that CEOs' actions in that issue, reflects employees' reaction in the same task. Nevertheless, both CEOs and employees have to keep their work station locked.



Bar graph 6: Working position differences in locking the work station.

Working position differences in using different passwords

Based on the results there is a significant dependence between the two variables with the p-value equal to 0,001. Most of the CEOs, having administrative privileges, maintain different passwords, while employees, as simple users mainly use one password. From 13 CEOs participated in the survey, 11 (a percentage of 85% out of them) use different passwords in different application/ information systems. Meanwhile, only 13 out of 36 employees use different passwords. The majority of them (64%) just use one password for all the applications they operate in the organization. It is worthy to observe what is happening with the Head of department and the Supervisors. Regarding the first, 9 out of 11 (81%) use different passwords, while, only 3 out of 11 Supervisors (27%) follow the same way.

Table 3: working position differences in using different password(s).

	Use of different passwords			
Working position	Yes		No	
CEO	11 of 13	(85%)	2 of 13	15%)
Head of Department	9 of 11	(81%)	2 of 11	(18%)
Supervisor	3 of 11	(27%)	8 of 11	(73%)
Employee	13 of 36	(36%)	23 of 36	(63%)

Looking at the table 3 above, one can easily notice that going down in the hierarchy of the observed companies in general, the security issue of different passwords is becoming more and looser except for employees where it slightly increases but it is still in low levels.

6.4.2 Differences between years of seniority

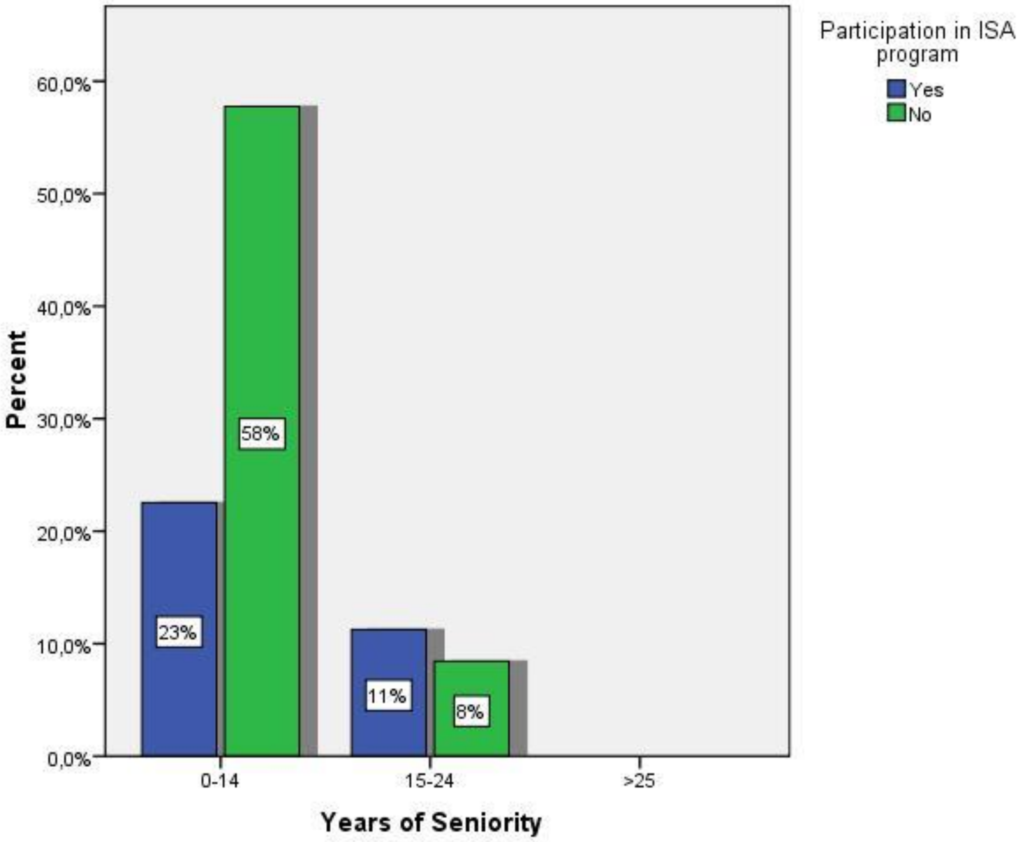
Below is presented the Table 4 which illustrates the differences of the observed measures based on the years of seniority of participants.

Table 4: Differences between years of seniority.

	x2	*DF*	*P*	*Contingency Coefficient*
Working position	14,539	3	**0,002**	0,412
Age	43,816	3	**0,000**	0,618
Educational level	2,726	2	0,256	0,192
Years of seniority	-	-	-	-
Role in the IS	11,772	2	**0,003**	0,376
Training for the IS	0,871	2	0,647	0,110
Significant security responsibility	19,603	2	**0,000**	0,465
Participation in ISSA program	4,245	1	**0,039**	0,238
Reason for not participating	2,85	3	0,415	0,239
Entering company's building	8,405	2	**0,015**	0,325
Behavior to a stranger	11,083	3	**0,011**	0,367
Access to Data canter	3,876	1	**0,049**	0,227
Locking work station	1,255	2	0,534	0,132
IS security techniques	4,611	5	0,465	0,247
Reason for not reporting incident	8,426	3	**0,038**	0,326
Experience of security related incident	1,287	1	0,257	0,133
Report it?	0,267	1	0,606	0,086
Use different passwords	5,418	1	**0,020**	0,266
Way of remembering password(s)	0,863	1	0,353	0,110
Num of password(s) characters	1,998	3	0,573	0,165
Frequency of password(s) change	10,634	2	**0,005**	0,361
Content of password(s)	34,958	25	0,089	0,574

Years of seniority differences in participation in ISA program

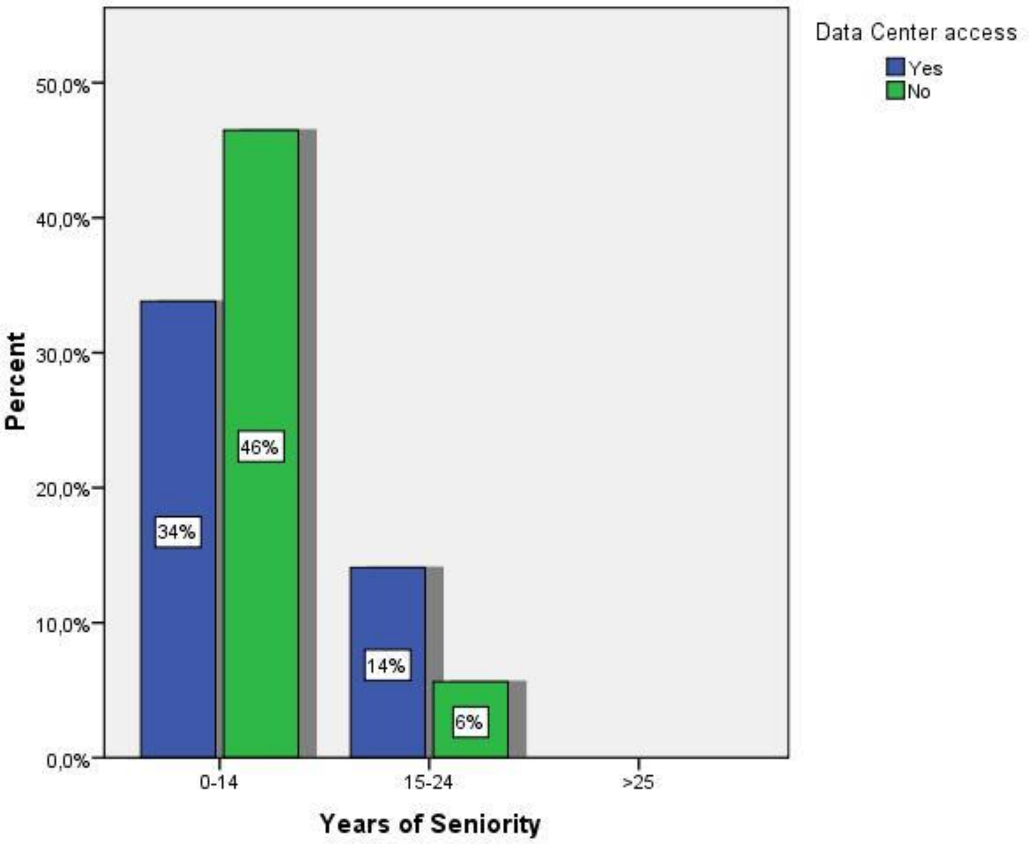
Years of seniority seem to have significant dependence with the participation in Information Security Awareness programs in the studied sample (p-value=0,039). From the participants with 0-14 years of seniority, only the 28% has participated in ISA programs while the rest 72% of them have not participated yet or they have not participated consciously. In the meanwhile, out of the few participants (14 in total) who have 15-24 years of seniority, the 57% has attended ISA program in the past, while the rest 43% has not. It could be claimed that while in the past companies had organized ISA training programs, during the following years they aborted this attempt for some reasons.



Bar graph 7: Years of seniority differences in participating in ISA programs.

Years of seniority differences in accessing the data center

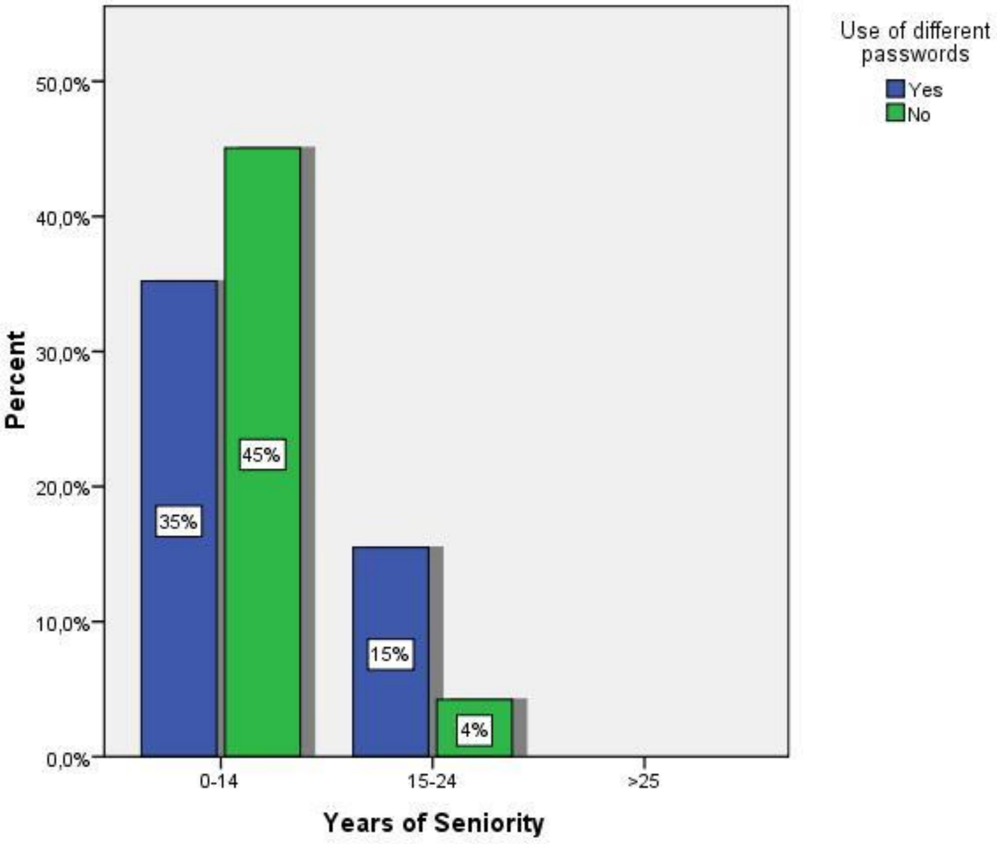
According to the Table 4, it is noticed a slight dependence between the years of seniority and the access of participants in the data canter with p-value equal to 0,049. Between the participants with the less years of seniority (0-14), the 42% (24 out of 57) has access to the data center. As the years of seniority increase, more participants have gained access to the data center. 71% of the participants with 15-24 years of seniority can reach the data center of their company. Probably, due to employees' experience in company's procedures and the years of cooperation between each other, company's security policies seem to be loosed.



Bar graph 8: Years of seniority differences in accessing the data center.

Years of seniority differences in using different passwords

The Bar graph 9 below illustrates the years of seniority differences in using different passwords. The dependence between the two variables is significant (p-value<0.05) equal to 0,020. Between the participants with 0-14 years of seniority almost half of them use different passwords in different application that they use (44%). Different results recorded from the participants with 15-24 years of seniority. The majority of them (79%) use different passwords for the applications that they use.



Bar graph 9: Years of seniority differences in using different password(s).

7. Discussion

As it mentioned to the theoretical part of this research, Security Awareness was not always considered as important. Later in time, it was discovered that the human factor has a very important role in the security of organizations. The academic society started doing research in this field while practitioners started applying techniques and practices in order to raise employees' level of security awareness and establish a security-related culture in organizations.

Based on the results and the sample of those Greek ICT companies that took part in the survey, it can be clearly stated that there is a difference between the security actions that top-management performs, with those of low level employees. A gap in security measures between the two stakeholders of organization is noticed, while the security awareness level of the intermediate hierarchal levels of employees (i.e. Head of Department, Supervisor) is decreased when following the hierarchical pyramid from the top to the bottom. According to this finding it could be claimed that there are problems in the communication channels between the several layers that the companies are separated. Even if there is a security policy established in the organizations, it is not clearly communicated by top-management to the low level employees. The same finding was recorded by Erik Alberchten (2007) who stated that ISA level is limited due to the lack of knowledge about documentation and Information Security policy that already exists.

Focusing on working years in the current participants' position and the ISA programs that are organized during that period, it is recorded that while in the past a number of ISA training programs had run, later on time the frequency of such programs has decreased. Several reasons could lead to that outcome. One could assume that top-management, after practicing ISA programs in the past, did not receive tangible results. Considering that, top-management could lose the meaning of importance of Security Awareness. A similar statement has recorded in the literature, where lack of interest in ISA from top-management's point of view can lead to employees' low level of Security Awareness [2] [25].

In addition, looking at the economy of Greece lately, huge problems can be observed. Business activity has been decreased and a lot of companies have been bankrupted while the rest of them are trying to survive in a really unfriendly for business environment. Within this attempt, companies might have cut all the unnecessary tasks of their businesses (it could be investigated in a future research). Combining this fact with the aforementioned finding (i.e. top-management's lack of interest in ISA development and maintenance), it could be claimed that due to the recession that Greece is facing (the year of 2011) companies' top-management cut the budget of raising and/or maintaining Information Security Awareness. That seems to be opposed to the theory that Carl Colwill (2010) has stated. According to him, in a recession period inappropriate activities, mainly from inside employees, are increased. Employees, due to their uncertainty for their jobs, are more willing to compromise organization's assets [8]. Therefore, ISA techniques and practices must be reinforced.

As it is mentioned previously in this paper , within this survey the great issue of data confidentiality arises, simultaneously with the difficulties that researchers of ISA (and in general Security field) face when trying to conduct research for further development of the field. Security is a neuralgic field for the practitioners (i.e. organizations). There is a big trade-off between the willingness of enhancing the security and the use of organizations data for research and investigation. On one hand, top-management wants to enhance security but on the other hand, confidential data must not be published and be spread outside the organization in order not to be used against the company. Within this survey same problems arise. Most of the companies did not participate in completing the questionnaire that was sent. In the same time, one of them replied by e-mail stating that crucial information is asked and many people may think of trying to steal confidential information from the companies. The same reaction is recorded in a similar survey in the past within the Greek public sector where publishers refer that during their survey, they had to face the unwillingness of respondents to complete the questionnaires [13].

Based on this response, it could be claimed that security consciousness in Greek ICT companies does exist. Respondents seem to pay attention to the kind of information that they share with unknown people. On the other hand, none of the questions is something that is not widely known (i.e. password related information). They seem not to have the knowledge to distinguish which kind of information they can share without having security problems. Potential attackers could compromise a system even if they did not know information about the number of characters or the content of passwords. Analyzing the reference of that respondent about the difficulties that people face in this period (maybe meaning of the economic crisis), it can be claimed that recession is referred in the background meaning of that. Economic crisis in Greece has led people to think more suspiciously for the incidents that happen in their environment.

8. Conclusion

In this final chapter of this survey the general conclusions are presented based on the results and findings. However interesting findings are come from the data analysis, results should not been considered as facts for entire population of employees in Greek ICT companies. The participation in this survey is so small, that results should not be generalized. The unwillingness of companies to respond in such a survey highlights once more time the difficulties and the barriers that act against the conduction and further research in the field of Security.

Based on the 71 respondents' data, the level of Security Awareness seems not to be adequate. Focusing on the sections that this survey is separated, the overall level of ISA can be reached. Regarding the Physical Security, while most of the companies seem to control their physical areas, still there are people who enter freely. In the same time, the majority of respondents do not handle strangers inside organizations in a secure way. The security actions that are performed by the respondents are very few. The level of Security Awareness is very limited concerning the physical security.

To continue with the Information System Security, respondents in their vast majority do not keep their work stations in a secure way when are away of them, while only few of the participants use the four basic protection measures (password, data backup, antivirus protection, reporting incidents). It is notable the lack of a clear security policy in Greek ICT companies between the low level employees. The level of Security Awareness could be described as medium to low.

In the last part regarding password handling, participants seem to be really aware of how to keep passwords strong and ensure the safety of IS. Nevertheless, there are few exceptions regarding the frequency of changing passwords and the use of personal data in passwords' content (nevertheless participants combine them with various types of characters). It could be claimed that respondents' security consciousness concerning passwords is medium to high. Key factor that led to that result could be the specific industry that is studied in this research. It was expected by participants, as ICT professionals, to be even more aware of how to use passwords in a secure way.

The above conclusions aggregated form the following list:

- Very limited in Physical Security

- Medium to low Information System security
- Medium to high level of password handling consciousness

Based on the above list it can be stated that the level of ISA in Greek ICT companies is medium to low.

One of the most important findings of this survey is the differences in the level of Security Awareness between the working positions of participants. It is observed that top-management has a medium level of ISA performing the basic actions concerning security and the safety of information assets. When one is going down to the hierarchy pyramid can easily notice that the level is getting decreased with the final (lower) layer of employees approach a very low level of ISA without performing many basic security tasks or not following the security policy (if there is one they do not know about it or do not pay much attention on it).

It can be assumed that bad communication channels have led in that situation. While top-management has a level of ISA lower levels of employees lack in knowledge and information concerning security and as a result their level of ISA is even lower than top-management's one. Out of that conclusion, a scheme (Figure 2) is created in order to present graphically the general status that exists in Greek ICT companies.

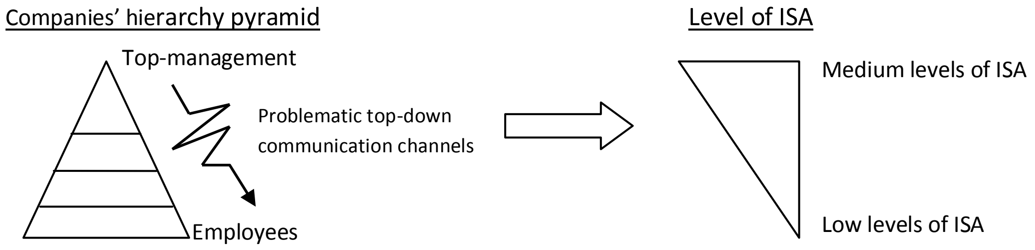


Figure 2: Level of Information Security Awareness in Greek ICT companies.

A medium to low level of security awareness lead to the conclusion that top-management does not pay attention to the human factor in security. Many gaps that exist due to that could lead to security breaches both by physical and electronic threats. Information Security Awareness should be raised further in Greek ICT companies. Top-management has to put the task of security higher in the priority list. Human factor consist of one of the most important parts in security. Even the most secured technically information system could be compromised because of users' unsecure way of operating.

8.1 Limitations

During this survey several limitations were recorded. First of all, the size of sample does not allow us to conduct a more precise survey and make conclusion for the overall level of Security Awareness in Greek ICT companies. Due to the nature of the questions (security-related) asked, it was difficult to collect more data. Several other factors resulted in not having more data for statistical analysis. Time and funds acted preventive in conducting a large-scaled survey.

Within a master thesis like this, neither time nor funds are given in order to conduct a proper survey in a complete extent. In this way, researchers must comply with techniques that may not bring the desirable outcome. In such a survey, a more organized from time and funds points of view attempt could reach really useful information and conclusion that could help both the academic society and the practitioners.

Finally, in this survey, only a limited number of security measures are examined. Due to the unwillingness of the respondents to participate in surveys, in general, authors tried to create a small and easily understandable questionnaire with as less questions as it was possible without provoking strict argumentations about security issues and data confidentiality from respondents' point of view. Even based on that, unwillingness and fear of releasing confidential data could not be avoided.

8.2 Further research

Several questions for investigation are come out of this survey. Both this and a previous survey [13] have shown that level of Security Awareness is kept low. Even if there is a gap in time between the two surveys nothing seems to have been changed positively. The question that comes up directly is what causes this outcome. Thinking about the causes it would be interesting to be investigated the real impact of recession on Security Awareness level in practice or on the frequency of ISA programs. Additionally, interesting enough would be an investigation of Greek organizations' culture's impact on Security Awareness level.

Regarding the measures that are investigated in this research, in the future, several other measures could be included such as internet access, mobile systems, document security, e-mail usage etc. Especially the mobile systems, tables and smart phones consist of the contemporary technology that is massively spread and it is already introduced in companies even as a tool for business. Great issues concerning Security Awareness arise. How those technological achievements influence Security and which is the impact on Security Awareness level of employees? Further research in the future could give answers to all those questions.

9. References

1. Marianthi Theocharidou, Dimitra Xidara, Dimitris Gritzalis, 2008, 'A CBK for Information Security and Critical Information and Communication Infrastructure Protection', International Journal of Critical Infrastructure Protection 1, p.81-96

2. Eirik Albrechten, 2006, 'A qualitative study of users' view on information security', Computers and Security 26, p.276-289

3. Benjamin D. Cone, Cynthia E. Irvine, Michael F. Thompson, Thuy D. Nguyen, 2006, 'A video game for cyber security training and awareness', Computers and Security 26, p.63-72

4. P.S. Dowland, S.M. Furnelll, H.M. Illingworthl, P. L. Reynolds, 1999, 'Computer crime and abuse - A survey of public attitudes and awareness', Computers & Security Vol.18, No.6, pp.715-726

5. H.A. Krugera, W.D. Kearney, 2008, 'Consensus ranking – An ICT security awareness case study', Computers and Security 27, p.254-257

6. Andrew Valentine, 2006, 'Enhancing the employee security awareness model', Cybertrust's ICSA Labs, p.17-19

7. E. Kritzinger, S.H. von Solms, 2010, 'Cyber security for home users- A new way of protection through awareness enforcement', Computers and Security 29, p.840-847

8. Carl Colwill, 2010, 'Human factors in information security-The insider threat – Who can you trust these days', Information Security technical Report 14, p.186-196

9. E.Kritzinger, E.Smith, 2008, 'Information security management: An information security retrieval and awareness model for industry', Computers and Security 27, p.224-231

10. Ronald C. Dodge Jr., Curtis Carver, Aaron J. Ferguson, 2007, 'Phising for user security awareness', Computers and Security p.73-80

11. R.S. Shaw, Charlie C. Chen, Albert L. Harris, Hui-Jou Huang, 2009, 'The impact of information richness on information security awareness training effectiveness', Computers & Education, p.92-100

12. Marianthi H. Terpsiadou, Anastasios, A. Economides, 2009, 'The use of information systems in the Greek public financial services: The case of TAXIS', Government Information Quarterly 26 468–476

13. Euripidis Loukis, Diomidis Spinelis, 2001, 'Information system security in Greek public sector', Information Management & Computer Security 9/1 p.21-31

14. Aggeliki Tsohou, Spyros Kokolakis, Maria Karydo, Euaggelos Kioutounzis, 2008, ‘Investigating Information Security Awareness: Research and Practice Gaps’, Information Security Journal: A global perspective, 17:207-227

15. Terry L. Wiant, 2005, ‘Information security policy’s impact on reporting security incidents’, Computer & Security 24, p.448-459

16. Martin Caminada, Reind van de Riet, Arjen van Zanten, Leendert van Doorn, 1998, ‘Internet Security incidents, a survey within Dutch organizations’, Computer & Security vol. 17, No 5, pp.417-433

17. Thomas Schlienger, Stephanie Teufel, 2003, ‘Information security culture – From analysis to change’, In 3rd annual information security South Africa conference, 9–11 July 2003, information security South Africa – Proceedings of ISSA 2003

18. J.F. Van Niekerk, R. Von Solms, 2010, ‘Information security culture: A management perspective’, Computers & Security 29, p.476–486

19. Sarandis Mitropoulos, Dimitrios Patsos, Christos Douligeris, 2006, ‘On Incident Handling and Response: A state-of-the-art approach’, Computers & Security 25, p.351-370

20. Tejaswini Herath, H.R. Rao, 2009, ‘Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness’, Decision Support Systems 47 p.154–165

21. Maeyer D.D., 2007, ‘Setting up an effective information security awareness program’, In ISSE/SECURE 2007 Securing Electronic Business Processes Highlights of the Information Security Solutions Europe/ SECURE 2007 Conference (part 1), Vieweg, p.49–58

22. Mark Wilson and Joan Hash, 2003, ‘Building an information technology security awareness and training program’, NIST Special Publication 800–50. Gaithersburg, MD: National Institute of Standards and Technology

22. Mark Wilson and Joan Hash, 2003, *‘Building an information technology security awareness and training program’*, NIST Special Publication 800–50. Gaithersburg, MD: National Institute of Standards and Technology

23. H.A. Krugera, W.D. Kearney, 2006, *‘A prototype for assessing information security awareness’*, Computers & Security 25 p.289–296

24. Farhad Daneshgar, Jim Wang, 2007, *‘Validation of the awareness net model for the Australian security investment processes’*, Knowledge-Based Systems 20 p.736–744

25. L. Drevin, H.A. Kruger, T. Steyn, 2007, *'Value-focused assessment of ICT security awareness in an academic environment'*, Computers & Security 26, p.36 – 43

26. Mete Eminagaoglu, Erdem Ucar, Saban Eren, 2009, *'The positive outcomes of information security awareness training in companies - A case study'*, Information Security Technical Report 14, p.223-229

27. Eirik Albrechtsen, Jan Hovden, 2010 , *'Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study'*, Computers & Security 29, p.432 – 445

28. Maria Karydaa, Evangelos Kiountouzisa, Spyros Kokolakis, 2005, *'Information systems security policies: A contextual perspective'*, Computers & Security 24, p.246-260

29. Nick Gaunt, 1998, *'Installing an appropriate information security policy'*, International Journal of Medical Informatics 49, p.131–134

30. Wendy Goucher (Security Empowerment Consultant, Idrach Ltd.), October 2009, *'The challenge of security awareness training'*, Computer Fraud & Security, p. 15-16

31. Professor Steven Furnell (University of Plymouth), June 2010, *'Jumping security hurdles'*, Computer Fraud & Security, p. 10-14

32. Steven Furnell, Valleria Tsaganidi, Andy Phippen, 2008, *'Security beliefs and barriers for novice Internet users'*, Computers & Security 27, p.235 – 240

33. Don A. Dillman, 2007, 'Mail and Internet Surveys - The Tailored Design Method', Second Edition

34. Kim-Phuong L. Vu, Robert W. Proctoe, Abhilasha Bhargav-Spantzel, Bik-Lam (Belim) Tai, Joshua Cook, E. Eugene Schultz, 2007, *'Improving password security and memorability to protect personal and organizational information',* Int. J. Human-Computer Studies 65, p.744-757

35. Dario Forte and Richard Power, 2007, *'Physical security –overlook it at your own peril'*, Computer Fraud & Security, August 2007, pp.16-20

10. APPENDICES

Appendix A: Sources

In this section, the sources that used in order to support the research are presented. An extended research was conducted based on the following sources.

- http://www.sciencedirect.com/
- http://www.ermeraldinsight.com/
- http://portal.acm.org/
- http://scholar.google.com/
- http://books.google.com/
- http://thesis.eur.nl/theses/
- http://www.eur.nl/ub/english/

Several key words are used in all of those sources and the analogous literature is gathered in order to supports the research and more specifically the theoretical background. Below are presented the key words that used during this research

Appendix B: Negative replies

Mr.'s X reply:

"Δώσε λίγο προσοχή στην τελευταία ενότητα να μην πω να την (εξαφανίσεις). Να ξέρεις ότι υπάρχει οργανωμένο γραφείο για το ηλεκτρονικό έγκλημα και φοβάμαι ότι αν συνεχίσεις θα υπάρξει θέμα γιατί αρκετός κόσμος δεν θα καταλάβει την πραγματική έννοια τις μεταπτυχιακής εργασίας σου!

Στους καιρούς που ζούμε όλα γύρω μας είναι ύποπτα, ίσως να μπορείς να ανακατασκευάσεις το ερωτηματολόγιο ελπίζω τα καλύτερα για εσένα."

Translation in English:

"Pay attention in the last part or even remove it. Be aware that there is an office against electronic crime and I'm afraid if you continue you will have problem because enough people are not going to understand the real meaning of your master thesis!

In this period that we are living everything around us is suspicious; maybe you can re-create the questionnaire. I hope the best for you."

Appendix C: Questionnaires Greek-English – Codebook

In this section the questionnaire that is sent is presented. The questionnaire is sent in Greek language. Here is illustrated the English version of it. The questionnaire is created and sent using Google Docs. Here is the link of this document:

https://docs.google.com/spreadsheet/viewform?formkey=dEh2LVJSa3BTc2haTzR1V1dPRzBuZHc6MQ&theme=0AX42CRMsmRFbUy04ZWQwMDYwMS02YjZhLTQ2ZjMtYjcyNy0zYWNlMzlmYTAxNmY&ifq

I. The questionnaire

Survey concerning Security Awareness

In the following questionnaire the level of Security Awareness is investigated in Greek companies. The required time for completing it is 15 minutes. Questions are separated in five (5) groups. During the conduct of this survey participants' anonymity will be kept. The data will be kept safely in the ownership of researcher and they are going to be deleted after finishing with the survey.

A. Demographic Data

Which is your working position in the company?

a.CEO c. Head of Department
c. Supervisor d. Employee

1. Which is your age?

a. 18–30 b. 31–40
c. 41–50 d. over 50

2. Which is your educational level?

a. Primary education b. Secondary education
c. Higher education, d. Postgraduate/doctorate

3. Which is your seniority (years) in the company?

a. 0–14 b. 15–24 c. over 25

B. Technology Usage

4. Which is your role in company concerning the Information System?

a. I have administrative privileges b. I'm a simple user
c. I don't have access to IS d. other

5. Did you have the proper/specific training for the information system(s) your companies (are) using?

a.Yes, for all IS b. Yes, for some c. No, for none of them

6. Do you have significant security responsibility (e.g. database administrator etc)?

a.Yes b. No c. I'm not sure

7. Have you ever participated in a S.A. program?

a.Yes b. No

7.1 If not, what is the reason for this according to you?

a.Lack of time b. Lack of Funds c. Lack of S.A. importance d. other

C. Physical Security

8. How are you entering the company building?

a. I just enter the building freely b. The reception opens the door after checking my ID
c. I use my special magnetic card d. Other

9. How do you behave when you see an unknown person inside the company?

a. I lead him/her to the destination that he/she wants
b. I follow the policy of the company (e.g. lead him/her to the reception in order to be registered as a visitor)
c. I do nothing
d. Other

10. Do you have access to the data center (i.e. servers' room)?

a.Yes b. No

D. Information System Security

11. Do you lock your Computer when you leave it for any reason (toilet, break, meeting etc)?

a. Yes b. No c. Not always

12. Which of the followings applies to you?

12.1 Password usage	a.Yes	b. No
12.2 Data backup	a.Yes	b. No
12.3 Antivirus protection	a.Yes	b. No
12.4 Report incidents	a.Yes	b. No

13. What is the reason that could prevent you from reporting a security incident?

a.No sufficient company policy b. Afraid of potential penalties
c. Afraid of losing benefits d. Other

14. Have you ever faced a security related incident?

a.Yes b. No

14.1If yes, did you report the incident?

a.Yes b. No

E. Password Handling

15. Do you have different passwords for different Information Systems or applications that you use?

a.Yes b. No

16. How do you remember your password(s)?

a. By heart b. Keep it on a note at my desk
c. tell it to a colleague d. other

17. How many characters do you use for your password(s)?

a. 4 b. 5-7 c. 8-10 d. >10

18. How often do you change your password?

a. At least every week b. Every few week c. Once a month d. Never

19. Which one of the option below do you use in your current password? (you choose more than one)

□ a.Personal data (date of birth, your name, your age etc)

□ b.Randomly generated passphrases

□ c. Lower case letters

□ d. Upper case letters

□ e. Numbers

□ f. Special characters (!, @, #, $, %, ^ etc.)

Thank you very much for your time!

This survey is conducting within the Master Thesis of Erasmus University. For any kind of comments please contact to: kpapagian@yahoo.gr

II. Codebook

Codebook consists of a map with the names of variable with their code names on SPSS and the measurements.

Variable	SPSS variable Name	Coding Instructions
Identification Number	ID	Num assigned to each questionnaire
Working position	workPos	0=CEO 1=Head of Department 2=Supervisor 3=Employee
Age	age	0=18-30 1=31-40 2=41-50 3=>50
Educational level	edu	0=Primary Education 1=Secondary Education 2=Higher Education 3=Postgraduate/ Doctotare
Years of seniority	seniority	0=0-14 1=15-24 2=>25
Role in the IS	ISrole	0=Administrative Privileges 1=Simple user 2=No Access 3=Other

Training for IS	training	0=Yes, for all IS 1=Yes, for some 2=No, for none of them
Significant security responsibility	significantPos	0=Yes 1=No 2=Not sure
Participation in ISA program	ISAcamp	0=Yes 1=No
Reason for not participating	reasonY	0=Lack of time 1=Lack of funds 2=Lack of ISA importance 3=Other
Entering company’s building	enteringBuilding	0=Free 1=Reception Control 2=Magnetic card 3=Other
Behavior to a stranger	strangerInside	0=Lead them where they want 1=Follow company’s policy 2=Do nothing 3=Other
Data Center access	dataCenterAcc	0=Yes 1=No
Locking working station	lockWorkStation	0=Yes 1=No 2=Not always
IS security techniques	IStechniques	0=Password usage 1=Data backup 2=Antivirus protection 3=Report incidents
Reason of not reporting incident	ReasonNotReporting	0=No sufficient policy 1=Afraid of potential penalties 2=Afraid of losing benefits 3=Other
Experience of security related incident	fasingSecInc	0=Yes 1=No
Report the incident	reportThisInc	0=Yes 1=No
Use of different password	differentPswd	0=Yes 1=No
Remember the password	pswdHandling	0=By heart 1=Note in the desk 2=Share it with colleague 3=Other
Number of password characters	pswdCharacters	0=4 1=5-7 2=8-10 3=>10
Frequency of password change	pswdCahange	0=At least every week 1=Every few weeks 2=Once a month 3=Never

Content of password	pswdContent	0=Personal data 1=Randomly generated passphrases 2=Lower case letters 3=Upper case letters 4=Numbers 5=Special characters

Appendix D: Frequencies

Here are presented the tables of frequencies as derived from the SPSS.

Working Position

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	CEO	13	18,3	18,3	18,3
	Head of Department	11	15,5	15,5	33,8
	Supervisor	11	15,5	15,5	49,3
	Employee	36	50,7	50,7	100,0
	Total	71	100,0	100,0	

Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-30	31	43,7	43,7	43,7
	31-40	27	38,0	38,0	81,7
	41-50	11	15,5	15,5	97,2
	>50	2	2,8	2,8	100,0
	Total	71	100,0	100,0	

Educational Level

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Secondary Education	9	12,7	12,7	12,7
	Higher Education	42	59,2	59,2	71,8
	Post graduate/ Doctorate	20	28,2	28,2	100,0
	Total	71	100,0	100,0	

Years of Seniority

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-14	57	80,3	80,3	80,3
	15-24	14	19,7	19,7	100,0
	Total	71	100,0	100,0	

Role in the IS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Administrative Privileges	29	40,8	40,8	40,8
	Simple User	39	54,9	54,9	95,8

	No access	3	4,2	4,2	100,0
	Total	71	100,0	100,0	

Training for IS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes, for all IS	14	19,7	19,7	19,7
	Yes, for some	45	63,4	63,4	83,1
	No, for none of them	12	16,9	16,9	100,0
	Total	71	100,0	100,0	

Significant Security Responsibility

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	25	35,2	35,2	35,2
	No	42	59,2	59,2	94,4
	Not sure	4	5,6	5,6	100,0
	Total	71	100,0	100,0	

Participation in ISA program

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	24	33,8	33,8	33,8
	No	47	66,2	66,2	100,0
	Total	71	100,0	100,0	

Reason for not participating

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Lack of time	8	11,3	17,0	17,0
	Lack of funds	12	16,9	25,5	42,6
	Lack of ISA importance	18	25,4	38,3	80,9
	Other	9	12,7	19,1	100,0
	Total	47	66,2	100,0	
Missing	System	24	33,8		
Total		71	100,0		

Entering company's building

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Free	20	28,2	28,2	28,2
	Reception control	39	54,9	54,9	83,1
	Magnetic card	12	16,9	16,9	100,0
	Total	71	100,0	100,0	

Behavior to a stranger

	Frequency	Percent	Valid Percent	Cumulative Percent

Valid	Lead them where they want	20	28,2	28,2	28,2
	Follow company's policy	24	33,8	33,8	62,0
	Do nothing	25	35,2	35,2	97,2
	Other	2	2,8	2,8	100,0
	Total	71	100,0	100,0	

Data Center access

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	34	47,9	47,9	47,9
	No	37	52,1	52,1	100,0
	Total	71	100,0	100,0	

Locking working station

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	18	25,4	25,4	25,4
	No	22	31,0	31,0	56,3
	Not always	31	43,7	43,7	100,0
	Total	71	100,0	100,0	

IS security techniques

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Password usage	3	4,2	4,2	4,2
	Password, Backup, Antivirus	21	29,6	29,6	33,8
	Password Antivirus	24	33,8	33,8	67,6
	Password, Antivirus, Report Inc.	1	1,4	1,4	69,0
	Antivirus protection	2	2,8	2,8	71,8
	4	20	28,2	28,2	100,0
	Total	71	100,0	100,0	

Reason of not reporting inident

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No sufficient policy	52	73,2	73,2	73,2
	Afraid of potential penalties	4	5,6	5,6	78,9
	Afraid of losing benefits	11	15,5	15,5	94,4
	Other	4	5,6	5,6	100,0
	Total	71	100,0	100,0	

Experience of security related incident

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	36	50,7	50,7	50,7
	No	35	49,3	49,3	100,0
	Total	71	100,0	100,0	

Report the incident

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	30	42,3	83,3	83,3
	No	6	8,5	16,7	100,0
	Total	36	50,7	100,0	
Missing	System	35	49,3		
Total		71	100,0		

Use of different passwords

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	36	50,7	50,7	50,7
	No	35	49,3	49,3	100,0
	Total	71	100,0	100,0	

Remember the password

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	By heart	57	80,3	80,3	80,3
	Note in the desk	14	19,7	19,7	100,0
	Total	71	100,0	100,0	

Number of password chararacters

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	2	2,8	2,8	2,8
	5-7	25	35,2	35,2	38,0
	8-10	39	54,9	54,9	93,0
	>10	5	7,0	7,0	100,0
	Total	71	100,0	100,0	

Frequency of passwaord change

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Every few weeks	1	1,4	1,4	1,4
	Once a month	17	23,9	23,9	25,4
	Never	53	74,6	74,6	100,0
	Total	71	100,0	100,0	

Content of password

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Personal data	5	7,0	7,0	7,0
	Per. data, RGP, Lower & Uppercase let, Nums	1	1,4	1,4	8,5
	Per. data, RGP, Lower & Uppercase let, Nums, Sp. char	7	9,9	9,9	18,3
	Per. data, RGP, Lowercase let, Nums,	3	4,2	4,2	22,5

	Sp. char				
	Per. data, RGP, Uppercase let, Nums, Sp. char	1	1,4	1,4	23,9
	Per. data, Lower & Uppercase let, Nums	2	2,8	2,8	26,8
	Per. data, Lower & Uppercase let, Nums, Sp. char	9	12,7	12,7	39,4
	Per. data, Lowercase let, Nums	3	4,2	4,2	43,7
	Per. data, Lowercase let, Nums, Sp. char	1	1,4	1,4	45,1
	Per. data, Uppercase let, Nums	1	1,4	1,4	46,5
	Per. dada, Nums	1	1,4	1,4	47,9
	Per. data, Nums, Sp. char	1	1,4	1,4	49,3
	Per. dada, Sp. char	1	1,4	1,4	50,7
	RGP	1	1,4	1,4	52,1
	RGP, Lowercase let	1	1,4	1,4	53,5
	RGP, Lower & Uppercase let, Nums	6	8,5	8,5	62,0
	RGP, Lower & Uppercase let, Nums, Sp. char	10	14,1	14,1	76,1
	RGP, Lowercase let, Nums	1	1,4	1,4	77,5
	RGP, Lowercase let, Nums, Sp. char	4	5,6	5,6	83,1
	RGP, Uppercase let, Nums	1	1,4	1,4	84,5
	RGP, Sp. char	1	1,4	1,4	85,9
	Lower & Uppercase let, Nums	2	2,8	2,8	88,7
	Lower & Uppercase let, Nums, Sp. char	1	1,4	1,4	90,1
	Nums	2	2,8	2,8	93,0
	Nums, Sp. char	1	1,4	1,4	94,4
	Special char	4	5,6	5,6	100,0
	Total	71	100,0	100,0	

Appendix E: Chi-square analyses

Here are presented the chi-square analysis that conducted in variables of Working Position and Years of seniority. (Crosstab tables are not included)

I. Working Position

Working Position * Age

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	43,889[a]	9	,000
Likelihood Ratio	49,541	9	,000
Linear-by-Linear Association	23,453	1	,000
N of Valid Cases	71		
a. 12 cells (75,0%) have expected count less than 5. The minimum expected count is ,31.			

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,618	,000
N of Valid Cases		71	

Working Position * Educational Level

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	13,552[a]	6	,035
Likelihood Ratio	16,871	6	,010
Linear-by-Linear Association	10,203	1	,001
N of Valid Cases	71		

a. 7 cells (58,3%) have expected count less than 5. The minimum expected count is 1,39.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,400	,035
N of Valid Cases		71	

Working Position * Years of Seniority

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	14,539[a]	3	,002
Likelihood Ratio	13,784	3	,003
Linear-by-Linear Association	13,787	1	,000
N of Valid Cases	71		

a. 3 cells (37,5%) have expected count less than 5. The minimum expected count is 2,17.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,412	,002
N of Valid Cases		71	

Working Position * Role in the IS

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	19,325[a]	6	,004
Likelihood Ratio	20,527	6	,002
Linear-by-Linear Association	16,116	1	,000
N of Valid Cases	71		

a. 6 cells (50,0%) have expected count less than 5. The minimum expected count is ,46.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,463	,004
N of Valid Cases		71	

Working Position * Training for IS

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5,739[a]	6	,453
Likelihood Ratio	5,653	6	,463
Linear-by-Linear Association	2,194	1	,139
N of Valid Cases	71		
a. 6 cells (50,0%) have expected count less than 5. The minimum expected count is 1,86.			

Symmetric Measures			
		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,273	,453
N of Valid Cases		71	

Working Position * Significant Security Responsibility

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	23,879[a]	6	,001
Likelihood Ratio	23,957	6	,001
Linear-by-Linear Association	15,996	1	,000
N of Valid Cases	71		
a. 7 cells (58,3%) have expected count less than 5. The minimum expected count is ,62.			

Symmetric Measures			
		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,502	,001
N of Valid Cases		71	

Working Position * Participation in ISA program

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4,458[a]	3	,216
Likelihood Ratio	4,358	3	,225
Linear-by-Linear Association	3,340	1	,068
N of Valid Cases	71		
a. 3 cells (37,5%) have expected count less than 5. The minimum expected count is 3,72.			

Symmetric Measures			
		Value	Approx. Sig.

Nominal by Nominal	Contingency Coefficient	,243	,216
N of Valid Cases		71	

Working Position * Reason for not participating

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6,383[a]	9	,701
Likelihood Ratio	7,431	9	,592
Linear-by-Linear Association	4,017	1	,045
N of Valid Cases	47		

a. 13 cells (81,3%) have expected count less than 5. The minimum expected count is ,85.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,346	,701
N of Valid Cases		47	

Working Position * Entering company's building

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9,836[a]	6	,132
Likelihood Ratio	10,760	6	,096
Linear-by-Linear Association	,081	1	,776
N of Valid Cases	71		

a. 6 cells (50,0%) have expected count less than 5. The minimum expected count is 1,86.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,349	,132
N of Valid Cases		71	

Working Position * Behavior to a stranger

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	16,419[a]	9	,059
Likelihood Ratio	17,335	9	,044
Linear-by-Linear Association	,324	1	,569
N of Valid Cases	71		

a. 13 cells (81,3%) have expected count less than 5. The minimum expected count is ,31.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,433	,059
N of Valid Cases		71	

Working Position * Data Center access

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	3,155[a]	3	,368
Likelihood Ratio	3,212	3	,360
Linear-by-Linear Association	1,697	1	,193
N of Valid Cases	71		

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 5,27.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,206	,368
N of Valid Cases		71	

Working Position * Locking working station

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	15,277[a]	6	,018
Likelihood Ratio	14,395	6	,026
Linear-by-Linear Association	3,051	1	,081
N of Valid Cases	71		

a. 8 cells (66,7%) have expected count less than 5. The minimum expected count is 2,79.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,421	,018
N of Valid Cases		71	

Working Position * IS security techniques

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	27,136[a]	15	,028
Likelihood Ratio	31,033	15	,009
N of Valid Cases	71		

a. 21 cells (87,5%) have expected count less than 5. The minimum expected count is ,15.

Symmetric Measures			
		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,526	,028
N of Valid Cases		71	

Working Position * Reason of not reporting incident

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	7,185[a]	9	,618
Likelihood Ratio	8,477	9	,487
N of Valid Cases	71		
a. 11 cells (68,8%) have expected count less than 5. The minimum expected count is ,62.			

Symmetric Measures			
		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,303	,618
N of Valid Cases		71	

Working Position * Experience of security related incident

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1,417[a]	3	,702
Likelihood Ratio	1,428	3	,699
Linear-by-Linear Association	,486	1	,486
N of Valid Cases	71		
a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 5,42.			

Symmetric Measures			
		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,140	,702
N of Valid Cases		71	

Working Position * Report the incident

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	,107[a]	3	,991
Likelihood Ratio	,108	3	,991
Linear-by-Linear Association	,063	1	,802
N of Valid Cases	36		
a. 4 cells (50,0%) have expected count less than 5. The minimum			

expected count is 1,00.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,054	,991
N of Valid Cases		36	

Working Position * Use of different passwords

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	15,725[a]	3	,001
Likelihood Ratio	16,836	3	,001
Linear-by-Linear Association	12,194	1	,000
N of Valid Cases	71		

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 5,42.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,426	,001
N of Valid Cases		71	

Working Position * Remember the password

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1,806[a]	3	,614
Likelihood Ratio	1,850	3	,604
Linear-by-Linear Association	,204	1	,651
N of Valid Cases	71		

a. 3 cells (37,5%) have expected count less than 5. The minimum expected count is 2,17.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,157	,614
N of Valid Cases		71	

Working Position * Number of password characters

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5,391[a]	9	,799
Likelihood Ratio	6,575	9	,681
Linear-by-Linear Association	2,063	1	,151

N of Valid Cases	71		

a. 11 cells (68,8%) have expected count less than 5. The minimum expected count is ,31.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,266	,799
N of Valid Cases		71	

Working Position * Frequency of password change

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	14,035[a]	6	,029
Likelihood Ratio	12,435	6	,053
Linear-by-Linear Association	10,998	1	,001
N of Valid Cases	71		

a. 7 cells (58,3%) have expected count less than 5. The minimum expected count is ,15.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,406	,029
N of Valid Cases		71	

Working Position * Content of password

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	69,077[a]	75	,671
Likelihood Ratio	65,560	75	,774
N of Valid Cases	71		

a. 103 cells (99,0%) have expected count less than 5. The minimum expected count is ,15.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,702	,671
N of Valid Cases		71	

II. Years of seniority

Years of Seniority * Working Position

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)

Pearson Chi-Square	14,539[a]	3	,002
Likelihood Ratio	13,784	3	,003
Linear-by-Linear Association	13,787	1	,000
N of Valid Cases	71		
a. 3 cells (37,5%) have expected count less than 5. The minimum expected count is 2,17.			

Symmetric Measures			
		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,412	,002
N of Valid Cases		71	

Years of Seniority * Age

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	43,818[a]	3	,000
Likelihood Ratio	41,231	3	,000
Linear-by-Linear Association	35,035	1	,000
N of Valid Cases	71		
a. 3 cells (37,5%) have expected count less than 5. The minimum expected count is ,39.			

Symmetric Measures			
		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,618	,000
N of Valid Cases		71	

Years of Seniority * Educational Level

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2,726[a]	2	,256
Likelihood Ratio	2,913	2	,233
Linear-by-Linear Association	,312	1	,577
N of Valid Cases	71		
a. 2 cells (33,3%) have expected count less than 5. The minimum expected count is 1,77.			

Symmetric Measures			
		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,192	,256
N of Valid Cases		71	

Years of Seniority * Role in the IS

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	11,672[a]	2	,003
Likelihood Ratio	12,407	2	,002
Linear-by-Linear Association	6,580	1	,010
N of Valid Cases	71		

a. 2 cells (33,3%) have expected count less than 5. The minimum expected count is ,59.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,376	,003
N of Valid Cases		71	

Years of Seniority * Training for IS

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	,871[a]	2	,647
Likelihood Ratio	,813	2	,666
Linear-by-Linear Association	,619	1	,431
N of Valid Cases	71		

a. 2 cells (33,3%) have expected count less than 5. The minimum expected count is 2,37.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,110	,647
N of Valid Cases		71	

Years of Seniority * Significant Security Responsibility

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	19,603[a]	2	,000
Likelihood Ratio	21,206	2	,000
Linear-by-Linear Association	6,453	1	,011
N of Valid Cases	71		

a. 3 cells (50,0%) have expected count less than 5. The minimum expected count is ,79.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,465	,000
N of Valid Cases		71	

Years of Seniority * Participation in ISA program

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	4,245[a]	1	,039		
Continuity Correction[b]	3,046	1	,081		
Likelihood Ratio	4,047	1	,044		
Fisher's Exact Test				,058	,043
Linear-by-Linear Association	4,186	1	,041		
N of Valid Cases	71				

a. 1 cells (25,0%) have expected count less than 5. The minimum expected count is 4,73.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,238	,039
N of Valid Cases		71	

Years of Seniority * Reason for not participating

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2,850[a]	3	,415
Likelihood Ratio	3,667	3	,300
Linear-by-Linear Association	1,141	1	,285
N of Valid Cases	47		

a. 4 cells (50,0%) have expected count less than 5. The minimum expected count is 1,02.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,239	,415
N of Valid Cases		47	

Years of Seniority * Entering company's building

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	8,405[a]	2	,015
Likelihood Ratio	7,084	2	,029
Linear-by-Linear Association	4,196	1	,041
N of Valid Cases	71		

a. 2 cells (33,3%) have expected count less than 5. The minimum expected count is 2,37.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,325	,015
N of Valid Cases		71	

Years of Seniority * Behavior to a stranger

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	11,083[a]	3	,011
Likelihood Ratio	13,988	3	,003
Linear-by-Linear Association	2,144	1	,143
N of Valid Cases	71		

a. 5 cells (62,5%) have expected count less than 5. The minimum expected count is ,39.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,367	,011
N of Valid Cases		71	

Years of Seniority * Data Center access

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	3,873[a]	1	,049		
Continuity Correction[b]	2,787	1	,095		
Likelihood Ratio	3,957	1	,047		
Fisher's Exact Test				,073	,047
Linear-by-Linear Association	3,818	1	,051		

N of Valid Cases	71				
a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 6,70.					
b. Computed only for a 2x2 table					

Symmetric Measures			
		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,227	,049
N of Valid Cases		71	

Years of Seniority * Locking working station

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1,255[a]	2	,534
Likelihood Ratio	1,241	2	,538
Linear-by-Linear Association	,327	1	,568
N of Valid Cases	71		
a. 2 cells (33,3%) have expected count less than 5. The minimum expected count is 3,55.			

Symmetric Measures			
		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,132	,534
N of Valid Cases		71	

Years of Seniority * IS security techniques

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4,611[a]	5	,465
Likelihood Ratio	5,425	5	,366
N of Valid Cases	71		
a. 9 cells (75,0%) have expected count less than 5. The minimum expected count is ,20.			

Symmetric Measures			
		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,247	,465
N of Valid Cases		71	

Years of Seniority * Reason of not reporting incident

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	8,426[a]	3	,038
Likelihood Ratio	6,421	3	,093
N of Valid Cases	71		

a. 5 cells (62,5%) have expected count less than 5. The minimum expected count is ,79.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,326	,038
N of Valid Cases		71	

Years of Seniority * Experience of security related incident

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1,287[a]	1	,257		
Continuity Correction[b]	,699	1	,403		
Likelihood Ratio	1,303	1	,254		
Fisher's Exact Test				,372	,202
Linear-by-Linear Association	1,269	1	,260		
N of Valid Cases	71				

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 6,90.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,133	,257
N of Valid Cases		71	

Years of Seniority * Report the incident

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	,267[a]	1	,606		
Continuity Correction[b]	,000	1	1,000		
Likelihood Ratio	,286	1	,592		

Fisher's Exact Test				1,000	,525
Linear-by-Linear Association	,259	1	,611		
N of Valid Cases	36				

a. 2 cells (50,0%) have expected count less than 5. The minimum expected count is 1,50.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,086	,606
N of Valid Cases		36	

Years of Seniority * Use of different passwords

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	5,418[a]	1	,020		
Continuity Correction[b]	4,118	1	,042		
Likelihood Ratio	5,708	1	,017		
Fisher's Exact Test				,035	,020
Linear-by-Linear Association	5,342	1	,021		
N of Valid Cases	71				

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 6,90.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,266	,020
N of Valid Cases		71	

Years of Seniority * Remember the password

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	,863[a]	1	,353		
Continuity Correction[b]	,307	1	,579		
Likelihood Ratio	,805	1	,370		
Fisher's Exact Test				,454	,279

Linear-by-Linear Association	,851	1	,356		
N of Valid Cases	71				
a. 1 cells (25,0%) have expected count less than 5. The minimum expected count is 2,76.					
b. Computed only for a 2x2 table					

Symmetric Measures			
		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,110	,353
N of Valid Cases		71	

Years of Seniority * Number of password characters

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1,998[a]	3	,573
Likelihood Ratio	3,343	3	,342
Linear-by-Linear Association	,015	1	,903
N of Valid Cases	71		
a. 5 cells (62,5%) have expected count less than 5. The minimum expected count is ,39.			

Symmetric Measures			
		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,165	,573
N of Valid Cases		71	

Years of Seniority * Frequency of password change

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	10,634[a]	2	,005
Likelihood Ratio	9,555	2	,008
Linear-by-Linear Association	7,080	1	,008
N of Valid Cases	71		
a. 3 cells (50,0%) have expected count less than 5. The minimum expected count is ,20.			

Symmetric Measures			
		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,361	,005
N of Valid Cases		71	

Years of Seniority * Content of password

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	34,958[a]	25	,089
Likelihood Ratio	35,908	25	,073
N of Valid Cases	71		

a. 49 cells (94,2%) have expected count less than 5. The minimum expected count is ,20.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,574	,089
N of Valid Cases		71	