2015

Establishing an Information Security Awareness and Culture

Korovessis, Peter

COPYRIGHT STATEMENT

ESTABLISHING AN INFORMATION SECURITY AWARENESS AND CULTURE

by

PETER KOROVESSIS

A thesis submitted to Plymouth University
in partial fulfillment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing, Electronics and Mathematics
Faculty of Science and Engineering

October 2015

Abstract

Establishing an Information Security Awareness and Culture

Peter Korovessis

In today's business environment all business operations are enabled by technology. Its always on and connected nature has brought new business possibilities but at the same time has increased the number of potential threats. Information security has become an established discipline as more and more businesses realize its value. Many surveys have indicated the importance of protecting valuable information and an important aspect that must be addressed in this regard is information security awareness.

The human component has been recognized to have an important role in information security since the only way to reduce security risks is through making employees more information security aware. This also means that employees take responsibility of their actions when dealing with information in their everyday activities. The research is concentrated mainly on information security concepts alongside their relation to the human factor with evidence that users remain susceptible to information security threats, thus illustrating the need for more effective user training in order to raise the level of security awareness.

Two surveys were undertaken in order to investigate the potential of raising security awareness within existing education systems by measuring the level of security awareness amongst the online population. The surveys analyzed not only the awareness levels and needs of students during their study and their preparation towards entering the workforce, but also whether this awareness level changes as they progress in their studies.

The results of both surveys established that the awareness level of students concerning information security concepts is not at a sufficient level for students entering university education and does not significantly change as they progress their academic life towards entering the workforce. In respect to this, the research proposes and develops the information security toolkit as a prototype awareness raising initiative. The research goes one step further by piloting and evaluating toolkit effectiveness.

As an awareness raising method, the toolkit will be the basis for the general technology user to understand the challenges associated with secure use of information technology and help him assess its current knowledge, identify lacks and weaknesses and acquire the required knowledge in order to be competent and confident users of technology.

Contents

List of Figures

List of Tables

Abbreviations

4G	Fourth Generation Networks
ACM	Association of Computer Machinery
ADDIE	Analyze, Design, Development, Implement, Evaluation
BIS	Department of Business, Innovation and Skills
BSI	British Standards Institution
C.I.A.	Confidentiality, Integrity, Availability
CBT	Computer Based Training
CEPIS	Council of European Professional Informatics Societies
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
COBIT	Control Objectives for Information and Related Technology
CSAT	Computer Security Awareness and Training
CSCAN	Centre for Security, Communications and Network Research
CSI	Computer Security Institute
CSO	Chief Security Officer
DSL	Digital Subscriber Line
EBSCO	Elton Bryson Stephens Company
ENISA	European Network and Information Security Agency
GPA	Grade Point Average
HCI	Human Computer Interaction
HEISC	Higher Education Information Security Council
ICT	Information & Communication Technologies

IEEE	Institute of Electrical and Electronic Engineers
InfoSec	Information Security
IoT	Internet of Things
ISACA	Information Systems Audit and Control Association
ISF	Information Security Forum
ISM	Information Security Management
ISO	International Standards Organization
IT	Information Technology
ITGI	Information Technology Governance Institute
LAN	Local Area Network
LMS	Learning Management System
MISSTEV	Model for Information Security Share Tacit Espoused Values
NIST	National Institute of Standards and Technology
PwC	PriceWaterhouseCoopers
SAI	Security Awareness Index
SANS	System Administration, Networking, and Security Institute
SECI	Sociaization, Externalization, Combination, Internalization
STEM	Science, Technology, Engineering and Maths
USB	Universal Serial Bus
WAN	Wide Area Network
WBT	Web Based Training
WiFi	Wireless Fidelity

Acknowledgement

First and above all, I praise God, the almighty for providing me this opportunity and granting me the capability to proceed successfully in this long and lonely PhD journey.

This thesis would never be a reality without the assistance of several people to which I feel compelled to offer my sincere thanks.

My sincere gratitude to my Director of Studies, Professor Steven Furnell for accepting me as a PhD student, for his continuous encouragement, thoughtful guidance, critical comments and endless support throughout this journey. Very deep and special thanks to my other supervisors, Dr. Maria Papadaki and Dr. Paul Dowland for their trust, their insightful discussions and for their guidance during the writing process.

My former undergraduate professor, Dr. Theodore Lyras, who recently passed away. My spiritual father who always urged me, never to give up studying. He will always be, by my side…..

This research has been made possible by a studentship awarded to me by my employer, The American College of Greece, for which I am very grateful.

Finally, I dedicate this thesis to all my colleagues at the Information Resources Management department at ACG and all the anonymous people who work hard and expect nothing but a ‘Thank you’.

Authors Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Graduate Committee.

Work submitted for this research degree at the Plymouth University has not formed part of any other degree either at Plymouth University or at another establishment

This study was financed with the aid of a studentship from The American College of Greece.

Relevant scientific seminars and conferences were regularly attended at which work was often presented; external institutions were visited for consultation purposes and papers were prepared for publication.

Word count of main body of thesis: 76,580 words

Signed: 

Date: **October 28, 2015**

Chapter I – Introduction

In today's business environment all business operations are enabled by technology. The use of technology is invaluable for businesses to carry out their daily tasks since it helps them make strategic decisions by processing data and transforming it into information which is then stored or transferred in various forms.

The always on and connected nature of today's environment has brought new business possibilities but at the same time has increased the number of potential threats. Information is a vital component for every organization and needs to be protected in a proper way. Companies and organizations in order to cope with the increased number of everyday threats have employed information security measures in order to ensure the confidentiality, integrity and availability of their systems and data. These measures include physical components such as guards and cameras, technical components such as electronic devices dedicated to protection (e.g. access controls, firewalls, etc.) and administrative components which involve policies, procedures and guidelines on how technology is to be used securely by those who operate it. In fact, the last 20 years, physical and technical controls have reached a very high level of sophistication but at the same time sophistication of malware and data breaches accelerate at a similar manner which brings an increased number of pressure to IT professionals to secure their organizations (Trustwave, 2014b). Also there is a shift of interest of potential intruders to more vulnerable information system components like the people who manage and use information technologies. Examples of such breaches caused by staff include IT related ones through viruses and malware or company and personal data theft through social engineering attacks (ENISA, 2010). Indeed security surveys indicate that end-users may be completely unaware of their exposure to security risks. Breaches may have occurred days, weeks or even

months ago, before the users become actually aware of it, and when finally detected, the associated costs to the organization may be very high to cope with (Ernst & Young, 2013; Trustwave, 2014a).

There are numerous stories from all industry sectors where data was exposed due to staff related breaches (Privacy Rights Clearinghouse, 2014). The human component has been recognized to have an important role in information security since the only way to reduce security risks is through making employees more information security aware. This also means that employees take responsibility of their actions when dealing with information in their everyday activities. Such an understanding of the importance of information security also achieves employee accountability and works in conjunction with technical aspects in order to achieve a successful security environment.

The protection of critical information is not the sole responsibility of the IT department, and is essentially an interdisciplinary team approach where a large number of non-IT related people must act in an appropriate way. There is an increasing interest in information security, especially for people outside the IT learning area. Also, there are a lot of non-computing disciplines that are closely related with the protection of information (Bishop and Frincke, 2005). Since the use of information technology is an essential requirement for all businesses today, appropriate awareness efforts should be designed in such a way to support the needs of employees outside the IT department who are interested in learning how to protect their personal and corporate information resources.

1.1 Research Aim and Objectives

The aim of the study is to investigate the issues affecting the establishment of effective information security awareness, and to propose a novel prototype that can be used as a model to help an organization move forward from a security awareness raising initiative towards security culture establishment.

In order to achieve this aim, the following objectives have to be addressed:

a. Understand the current information security landscape, and appreciate the importance of the human factor.
b. Investigate the changing trends in the domain of Information Security that lead to the importance of security awareness.
c. From a thorough literature review, understand the issues surrounding effective information security awareness and the establishment of an appropriate security culture.
d. Investigate the potential of raising security awareness within existing education systems as a first step towards a wider security awareness initiative for the online population.
e. Propose, define and develop a novel Information Security Toolkit in an effort to raise the level of security awareness.
f. Evaluate the toolkit validity by piloting a prototype implementation and assessing its effectiveness.

1.2 Thesis Structure

The thesis is comprised of seven chapters. Following this introduction, Chapter 2 introduces information security concepts and how these concepts apply in today's environment. The current state of information security awareness and culture is

examined by referencing internationally accepted security surveys and reports. Further to that the human factor and its relation to information security is examined through issues and topics from social psychology in order to determine the reason behind inexplicable behavior that could lead to security mistakes. Corporate culture, as a concept, is studied along with its relationship with information security in an effort to foster a culture in which users are aware of security issues and have the required knowledge to respond appropriately.

Having established the basis surrounding effective information security awareness, Chapter 3 proceeds with a thorough literature review, in order to understand the issues surrounding effective information security awareness and the establishment of an appropriate security culture. Further to that, the chapter moves one step forward by addressing the importance of embedding Information Security in the society and the role that education has to play towards this effort.

Chapter 4 investigates the potential of raising security awareness within existing education systems by measuring the level of security awareness amongst the online population. For this reason sample data from a university environment is used in order to examine the state of information security awareness in the academic sector and investigate the awareness needs of students in order to (1) support them during their time of study, (2) prepare them for the workplace, and (3) protect them in their wider personal use of IT systems. In fact, two separate surveys are conducted in order to investigate not only the awareness levels and needs of students in order to support them during their time of study and their preparation towards entering the workforce, but also whether this awareness level changes as they progress in their studies. The analysis of the results of the

two surveys then form the foundation for the design and development of an Information Security Toolkit.

Chapter 5 investigates the foundation behind the creation of the Information Security Toolkit, along with the theoretical framework on which it was actually developed. The chapter also presents elements of information security learning in order to get an understanding of its meaning and importance and then proceeds with the rationale behind the development of the toolkit along with its content and distinct areas.

Having developed a working prototype of the toolkit, Chapter 6 proceeds with the implementation and evaluation of its effectiveness. The process of putting the toolkit prototype in action is presented along with aspects of the development work behind it. Consideration is also given to the toolkit evaluation in terms of effectiveness and usability utilizing the various methods.

The final chapter presents the main conclusions derived from the research, its key achievements along with its limitations and potential for further research. The thesis also includes a series of relevant appendices to support the discussions and observations of the previous chapters. These are referenced at appropriate points during the main discussion.

Chapter II – The Information Security Landscape

2.1 Introduction

The purpose of this chapter is to introduce information security concepts and how these concepts apply in today's environment – an environment that has significantly changed and evolved over the last few years. The current state of information security awareness and culture is examined by referencing internationally accepted security surveys and reports. Further to that the human factor and its relation to information security is examined. Issues and topics from social psychology will be presented in order to determine the reason behind inexplicable behavior that could lead to security mistakes. The concept of corporate culture is studied, and its relationship with information security examined in an effort to foster a culture in which users are aware of security issues and have the required knowledge to respond appropriately. Finally the changing trends in information security that have resulted from the explosive changes in information technology are considered in an effort to understand that it is no longer possible to maintain effective information security by using physical and technical controls alone. There is a necessary to educate users on everyday issues concerning information security.

2.2 Information Security Concepts

In today's global economy, business operations are enabled by technology. At all levels of operation, business today make deals, provide goods and services, track client accounts, make financial and strategic decisions, all through the implementation of systems made possible by information technology. IT enables the storage and transportation of information from one business to another. This information is often considered the company's most valuable resource and needs to be protected at all times. Many believe that technology people are in place to

handle technology problems. This idea might have been valid in the days when technology was confined to the climate-controlled rooms of the data center and information processing was centralized. During the early years all IT operations handled by end users where through the use of standalone mainframe computers. These mainframes were usually protected by physical controls and no user intervention in terms of security was needed (Thomson and von Solms, 1998). In the past 20-30 years, however, technology has infused every facet of the business environment. The day-to-day operations of the typical end user have changed, since today end-users operate all aspects of computer systems ranging from critical enterprise applications to network infrastructures. IT has become a commodity through the delivery of generic applications through the Internet as "web services" and the homogenization of customized IT applications through the transformation of customized applications to generic ones (Carr, 2003). Despite the numerous reactions on Carr's controversial article, what that has been correctly predicted was the rapid price deflation of IT. The most cutting-edge technologies and IT capabilities are now available to all. To that extend, most of today's end-users can be seen as working in an IT environment. Since businesses today have become more fluid, the concept of computer security[1] has evolved into the idea of information security.

Information security has been traditionally defined by many sources as the protection of information of unauthorized access, disclosure, disruption, modification or destruction (Whitman and Mattord, 2004; International Organization for Standardization (ISO), 2005; Killmeyer, 2006). Its main goals

[1] Computer Security: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications). NIST Security Handbook, 1995.

have to do with the preservation of confidentiality, integrity and availability, also known as the C.I.A. triad. These basic components of information security can be further summarized as follows:

- Confidentiality: data has confidentiality when it is disclosed only to authorized individuals. When an unauthorized employee is able to view payroll data or when an attacker is able to access a customer database including names and credit card information, both these are examples of a loss of confidentiality.
- Integrity: data has integrity when it is accurate and complete. Data or an IT system loses its integrity when it has been modified or destroyed by an unauthorized entity. For example, integrity loss occurs when a file is modified due to malware infection, or an e-mail message is modified while transmitted.
- Availability: availability has to do with ensuring that information and vital services are accessible for those authorized to use them when required. Loss of availability indicates that either data or a system are not available when needed. For example, an e-shop is not operational when a customer wants to purchase a product.

The C.I.A. triad has been the industry standard for computer security since the development of the mainframe. This definition (inherited from the definition of computer security), was developed to address an environment characterized by: (1) the presence of mainframes located in a centralized data center making the security of such an environments an easy task, (2) hackers as being the primary threat of computer breaches and (3) military and government agencies as being

the primary sources of establishing computer security standards (von Solms, 1998; Whitman and Mattord, 2004).

Since these early days, the environment (both technical and business) has changed significantly resulting in an increased use of personal computers, the revolution of networking technologies and the Internet, and the decentralization of computing assets. As businesses have learned, “unless security technologies are supported by strong corporate security policies and procedures, even the most robust solutions fall short of providing adequate protection against today’s rapidly evolving threats”(Egan, 2005). Policies and procedures complement security technologies. They represent the guidelines and how-to procedures that identify the steps that must be followed so unsafe practices that would endanger the confidentiality, integrity and availability of data are avoided.

Although the existing C.I.A. principles still need to be maintained, what tends to happen is that organizations focus primarily on the technical approaches to maintain them without adequately incorporating employee and organizational aspects of information security (Spears, 2006). The environment has changed significantly and this has strong implications on information security. Among others, these implications include:

- The increased numbers in security breaches as a result of employee responsibility (Ponemon Institute, 2012a).
- Related legislation associated with information security.
- Increased need for justification for spending on information security through a means of measuring the effectiveness of security efforts.

- Potential loss of market share, damaged reputation and even legal implications which elevate information security to an issue of corporate strategic importance (Spears, 2006).
- The proliferation and penetration of mobile technologies and the ease of data access and distribution through them has placed a greater need for policies and procedures for safe computing.

With the extended scope of information security, the C.I.A. definition does adequately address the current scope nor has it evolved to adapt in today's demands placed on information security. Although technology and processes represent foundational pieces of a corporate information security framework, a third component is needed to complete the picture: people.

Security continues to be a major concern not only for companies that provide their services through information technology but also for computer users that use and take advantage of such services. A high number of Internet penetration is reported for both Europe and the US with a growth rate expected at least until 2017 (European Travel Commission, 2014; Pew Research Center, 2014). The World is moving towards a more sophisticated use of technologies like engaging with social networks and Internet on the move through mobile devices. However, the number of cybercrime incidents has also increased in the last few years. More specifically, in the US as of July 2014 the data breaches reported to authorities or covered by the media are 21% higher as compared with the same period last year (ITRC, 2014).

As mentioned before the increase in information technology usage resulted from worldwide Internet penetration, online and credit card payment increases, and market penetration of mobile devices has also increased the information

technology security incidents. While companies and organizations significantly invest on the improvement of information security technologies, hackers' interest has shifted by targeting the weakest link: the uneducated computer user (Aloul, 2012). Although all computer users have heard about attacks that can threaten their computers or violate the confidentiality of their data, the majority of them remain unsure about how to make their computers safe and keep data secure. Similarly, most users are still uninformed about how their system can be compromised due to their insecure behavior and continue to visit unsecure websites, respond to phishing e-mails, create weak passwords or store them at non-secure locations or give out sensitive information through exposure to social engineering. This brings into the scene the concept of Information Security Awareness.

Information Security Awareness has received varying definitions by leading authorities and organizations. The European Network and Information Security Agency (ENISA) define awareness as the "what" component of an organization's education strategy (ENISA, 2010). The goal is to change the behaviors and patterns in how a specific audience uses technology and the Internet. Awareness is considered as a distinct element from training and its objective is to turn information technology users into the organizations' first line of defense. That's why awareness activities occur on an ongoing basis using a variety of delivery methods in a less formal setting than training.(ENISA, 2010)

According to NIST Special Publication 800-16, awareness is not training and its purpose is to focus attention on security (National Institute of Standards and Technology (NIST), 1998). Through a series of presentations awareness efforts allow individuals recognize IT security concerns and respond accordingly. In

awareness raising activities, the learner is the recipient of information while in training the learner has a more active role. The objective of security awareness efforts are to change user behavior and reinforce good security practices.

ISACA defines security awareness in relation to the understanding that every member of an enterprise or every individual has in respect to (1) security and its appropriate levels to the enterprise, (2) importance of security and consequences of a lack of security and (3) individuals responsibility and accountability regarding security (ISACA, 2014).

All the above definitions of security awareness are comprised of two very important components:

- The knowledge component: individuals understand the importance of information security, the level of security required by their organization along with their individual security responsibilities.
- The behavioral component: knowledge and understanding of risks evolves into user accountability and results in change of behavior.

The effectiveness of any information security program depends on the behavior of people. Behavior on the other hand depends on what people know, their feelings, and what their instincts tell them to do (Schein, 2004). Although a security awareness program can establish a baseline and foster information security knowledge, a significant impact on people's feelings concerning their responsibility in the information security function is not always the case (Stahl, 2006). There are cases that a gap exists between what security policies dictate and how actually people behave. It is the role of the culture to change this gap. Taking into consideration that culture is a critical factor for organizations to

continue living, a change in organization security culture will directly affect security practices. The objective is to foster a culture which is synchronized with policies, which in turn lead to acceptable actions.

2.3 The state of Security Awareness and Culture

Information is an organization's most critical business resource and risks associated to that information should be managed as a standard part of their business processes (Broderick, 2001). Posthumus & von Solms realize the vitality of an organization's business information assets and suggest a framework to aid an organization in its information security governance efforts (Posthumus and Von Solms, 2004). Streff & Zhou stress the growing importance of securing information assets of organizations, since the dependency on information systems to support business operations continue to grow (Streff and Zhou, 2006).

Little doubt remains that information security protection is paramount to business success. Information is therefore a valuable resource and it should be protected and secured accordingly. If, for any reason valuable information is compromised, the organization could lose time, manpower, money and/or business opportunities. There are also cases reported where valuable information has been compromised. As a result this has damaged the firm's reputation so badly which led to the disintegration of the organization.

Pentasafe Security Technologies (now acquired by NetIQ Corporation), conducted the Security Awareness Index (SAI) Survey with the support and sponsorship of both ComputerWorld and Computing (Tucker, 2002). Although the survey results may be considered rather old, it is one of the first serious attempts to measure awareness among organizations and identify its importance. The

survey was based on the responses from 1,348 workers from 583 organizations worldwide with an effort to measure how organizations improve security awareness and understanding, and how well employees understand and act upon information security policies, threats and issues in their respective organizations. It represents a major effort on measuring how organizations improve security awareness and how well employees understand and act upon information security policies, threats and issues in their respective organizations. According to the survey:

- Most workers score poorly when it comes to security awareness. Excluding the workers in the information security department, the score for all business units represented by the survey is less than satisfactory. (less than satisfactory is considered any score below 70%).
- More than 25% of employees have not read any of their organization's security policies in the past year, and almost half of the workers are not fully aware of the consequences of failing to comply with organization's security policies.
- A cumulative 67% of the workers rate the security awareness in their organization as "inadequate" or "dangerously inadequate".

Ernst & Young's 2008 Global Information Security Survey, take a closer look at how organizations are specifically addressing their information security needs identify ten potential opportunities for improvement along with trends that will continue to drive information security in the coming years (Ernst & Young, 2008). According to the survey, among others, people still remain the weakest link in information security. It is important that those responsible for information security

must take more active measures concerning the changing of the organizational culture through developing training and awareness programs for employees. At the same time, organizational awareness was cited by 50% of the respondents to be the most significant challenge to delivering successful information security initiatives. This number was recorded significantly higher than the availability of resources (48%), adequate budget (33%), and addressing new threats and vulnerabilities (33%). According to the survey, technology plays a pivotal role in information security but there must also be focus on security training and awareness for information security to operate effectively. People must be viewed by organizations as equally critical as any other information security component.

The CSI 2008 Computer Crime and Security Survey, reports that although the vast majority of organizations view security awareness training as important, the last two years expenditures as a percentage are very low (Richardson, 2008). About 42% of the companies spent less than 1% of their security dollars on awareness programs. Although this number is somehow lower than the previous year, it clearly identifies that relatively little money are pushed into information security awareness efforts. Despite the fact that most respondents do not believe that their organization invests enough on awareness programmes, most of these programmes are not automatically approved by senior management unless they are adequately justified in economic terms.

When examining the state of security awareness amongst organizations as it has been reported by the 2010 CSI Computer Crime and Security Survey (Richardson, 2010), no significantly improved figures are observed (Table 1) and it is obvious that still does not receive the appropriate attention.

Security awareness:	Percentage
Is not used at all	15%
Accounts for less than 1% of the security budget	35%
Is considered to receive too little investment	50%
Was an appropriate action after an incident	42%

Table 1: Observations on security awareness amongst organizations as it has been reported by the CSI 2010 Computer Crime and Security Survey (Richardson, 2010)

Back in 2003, the US National Strategy to Secure Cyberspace realized that information security needs have to be addressed at all levels, from the individual user to an organization and beyond that to the Government and the Nation (White House, 2003b). The end users are emphasized as a key factor in securing the cyberspace and they should know the "simple things" that they could do to behave in a secure way and at the same time held responsible not just for their own security but also for the overall security. This document recognizes that the lack of familiarity, knowledge and understanding of security issues is a major barrier to users acting to improve cybersecurity. Among the priorities to overcome this are the promotion of a national awareness program to empower all users and fostering adequate programs to support the nation's cybersecurity needs. The key idea to a national effort to enhance cybersecurity should be a national effort to raise awareness.

It appears that information security has become synonymous with national security since computer networks form the backbone of the critical infrastructures of a nation's banking, power, communication network, etc. The above dated reports indicate that the importance of the human factor in information security at an individual, corporate and national level, and the consequences that may occur as a result of not investing in security awareness training have been identified

from a very early stage. But has the state of information security in terms of security awareness needs changed since then?

Ernst & Young titles their 2013 Global Information Security Survey as “Under cyber attack” (Ernst & Young, 2013). The report identifies that security breaches of an organization’s security perimeter occur on a continuous basis. Those attacks not only have increased exponentially over the last few years but also have emerged in complexity. At the same time infiltration could have occurred days, weeks or even months before actually detected and when the degree of the breach does surface, the associated costs of recovery for the organization can be shocking. Although organizations are moving towards the right direction there are still actions that need to be taken urgently. Organizations although are reactive in addressing the threats they know, are not seeking to understand new threats that may occur. The steps already taken to combat cyber threats have risen the degree of proactivity in determining both known and unknown risks but there is still room for expansion of security measures. This can be done through a continuous review and potential redesign of an organization’s entire information security framework in order to be better prepared against both the known and the unknown risks in the cyber environment. Although information security is seen as a vital component to the ongoing health and success of the organization, only 35% of security professionals of organizations present information security to the board. At the same time information security professionals report insufficient budgets and lack of skilled resources. Among the top priorities for information security over the coming twelve months, security awareness and training is considered either first or second key priority only by 23% of the respondents (Ernst & Young, 2013). An amazing 31% of the respondents ranked it last from a list of 21 pre-defined priorities! A significant paradox is observed here. During the

last twelve months the vulnerabilities that are the result of careless or unaware employees are reported as increased by 24% of the respondents or stable by 58% of them. Only an 18% reported a reduction. At the same time phishing, malware and spam threats are on the rise (Figure 1).

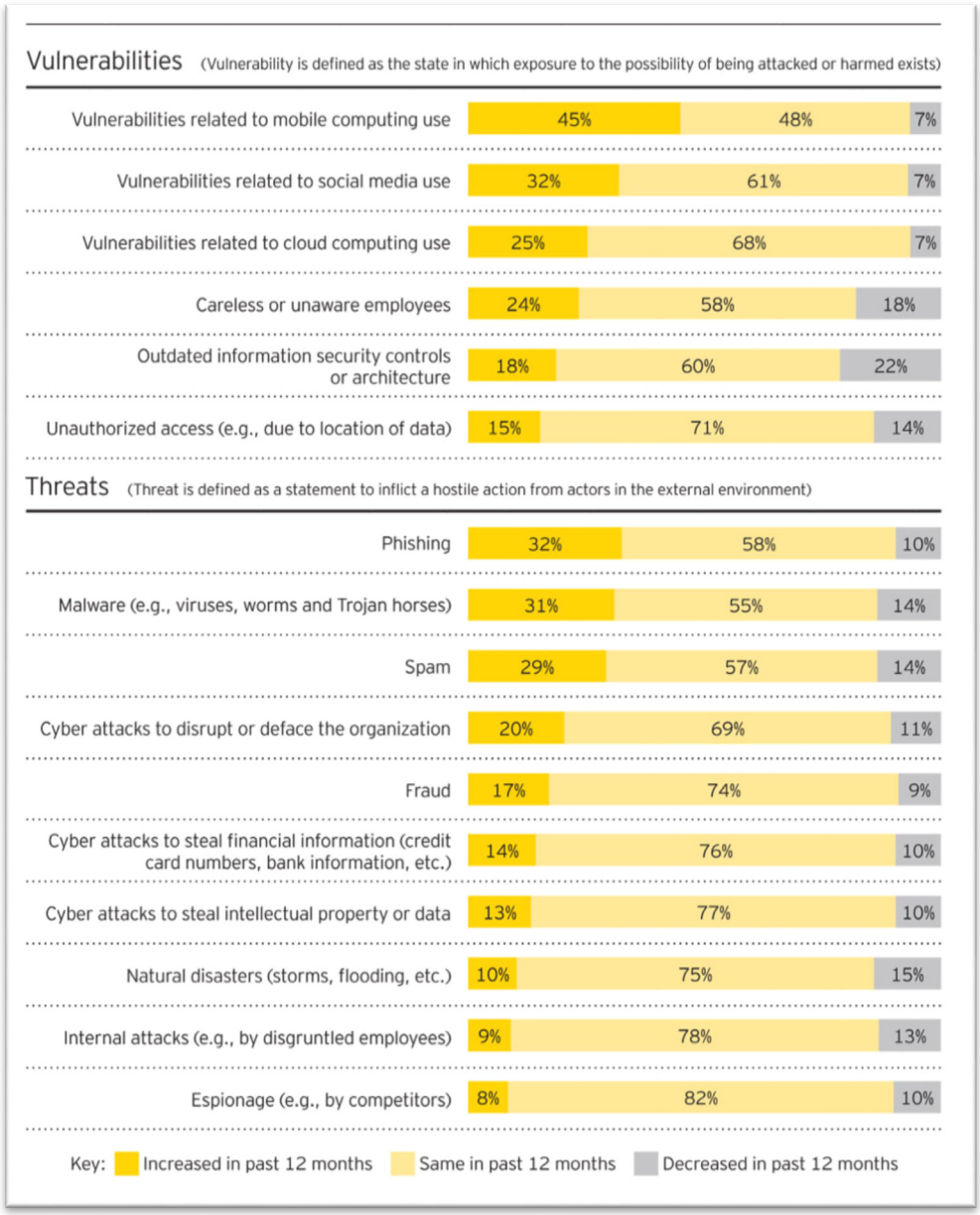


Figure 1: Threats and vulnerabilities that have most changed respondents' risk exposure over the last 12 months (Ernst & Young, 2013)

The following table (Table 2) summarizes notable observations from the Ernst &Young 2013 Global Information Security Survey in respect to information security awareness among the organizations surveyed.

Security awareness is:	Percentage
Undeveloped or nonexistent	29%
Within the top 3 priorities for the next 12 months	43%
A barrier at the executive level	31%

Table 2: Security awareness observations amongst as reported by the E&Y 2013 Global Information Security Survey

Among the leading practices that will enable improvement is fostering an information security culture throughout all levels of the organization. This can be achieved by raising employee awareness concerning their level of knowledge, security responsibilities and appropriate use of organization's technology assets and making information security as part of the employee's performance assessment.

PriceWaterhouseCoopers in their 2014 Global State of Information Security Survey identify that there is a need for a new model of information security with an understanding that knowledge is power (PwC, 2013a). In their yearly survey conducted in cooperation with CIO and CSO magazines, more than 9,600 responses were received from high executives from 115 countries. The results were analyzed in terms of different industry sectors. According to the report although information security risks have dramatically evolved, security strategies do not follow a similar pace. Security incidents have increased despite the fact that many organizations have raised their security efforts. In fact, fewer organizations are prepared to manage future threats. Despite the high degree of confidence among all respondents who believe their security activities are

effective, security incidents in the US have increased by 33% despite the implementation of security practices. In contrast to the Ernst & Young report above, a gain of 51% over year 2012 is reported in security investment. The report identifies the importance of the human factor in information security since insiders (current and former employees) are cited as a source of security incidents by most respondents. The rise in the use of cloud computing by almost half of the respondents puts an extra degree of potential risk since cloud is not included in the security policies of companies. In an effort to prepare an effective security plan for the future threats, most respondents that hold a leading position understand that security is now a business imperative and not just and IT challenge. But although significant investments have taken place in technology safeguards in order to secure against today's evolving threats, employee security awareness training programs have not received yet the needed attention. In terms of infrastructure security, an employee security awareness training program is considered a top priority by only a 22% of the respondents. From a worldwide perspective, employee security awareness training programs are reported present only by a 64% of respondents in North America. These figures are reported as 54%, 63% and 55% in South America, Asia Pacific and Europe respectively. Finally, an employee security awareness training program is included in a list of ten essential safeguards for effective security. The new approach to security for a new world should include the creation of a security culture that starts with the commitment of top level management and cascades to all employees (PwC, 2013a).

The Information Security Breaches Survey 2014, commissioned by the Department of Business, Innovation and Skills (BIS) in the UK, realizes that there are encouraging steps businesses take to improve information security (PWC,

2014). Still, the costs associated with security breaches are high, fact which underlines that cyber security is a significant business risk and must be taken seriously. Although the number of reported security breaches affecting UK businesses have slightly decreased as compared with the previous year, the overall cost of security breaches of all organizations has increased. There were organizations that a security breach damaged them so badly that they had to change the nature of their business. Still, security incidents are expected to rise in the next year. Breaches that are staff-related although dropped significantly compared to previous year, still play a key role in security breaches since 31% of the worst security incidents were caused by human error and another 20% by a deliberate misuse of systems by staff. In terms of information security spending, IT budgets are reported as increased across all sectors as compared to the previous year. In the overall, confidence about the availability of security resources has increased. Changing trends are reported in the use of information technology. There is an increased number of remotely hosted services with increasing numbers of companies storing confidential data on the Internet. The use of social networks by organizations is believed as important to their business and mobile device use is still an un-stoppable trend. On the other hand businesses are becoming more aware of the importance of education on security and spend time and money on programs that will explain security risks to their staff and ensure the right actions from their part in order to protect the company's vital information. The number of organizations which recognize that staff are a great asset but at the same time the greatest threat are increasing. Similarly, the proportion of businesses that have a program of continuous education for their staff concerning information security matters is on an encouraging rise. However, as the survey reports, this is by no means universal. At the same time, there is a

rise of 2% in the number of reported breaches due to staff misuse of confidential data by large organizations. Indeed, more than half of large organizations have staff that accidentally lost confidential information and one third of them actively misused them.

Similarly, the US government has recognized that national and economic security relies on reliable functioning of critical infrastructures and have issued guidelines and practices for reducing cyber risks. The “Framework for Improving Critical Infrastructure Cybersecurity” published by the National Institute of Standards and Technology (NIST) involves the following parts (NIST, 2014):

- “Identify” which involves the development of an organizational understanding to manage cybersecurity risk.
- “Protect” which involves the development and implementation of appropriate safeguards.
- “Detect” which involves the appropriate activities to identify a cybersecurity event.
- “Respond” involves activities to take appropriate action in regard to a detected cybersecurity event.
- “Recover” involves appropriate activities to restore impaired capabilities and services due to a cybersecurity event.

The framework recognizes the limited awareness of cybersecurity risk at an organizational level and the lack of a structured approach in managing cybersecurity risk. An important component in an effort to address appropriately threats involves the provision of cybersecurity awareness education and adequate training to organization’s personnel in order to perform their information-related duties consistent with related policies and procedure.

Towards this approach, and in an effort to promote awareness on security issues to the general population, the US Federal government has established official websites specifically for that purpose. The Stop, Think, Connect (http://www.stopthinkconnect.org) website and the OnGuardOnline (http://www.onguardonline.gov) website represent a global cybersecurity awareness campaign addressed to all digital citizens in an effort to help them stay safer and more secure online.

The importance of information security awareness has also been addressed in the European Union through its ENISA publication of the "The new users' guide: How to raise information security awareness" (ENISA, 2010). The document represents an update of the original document published two years earlier, and includes new activities and case studies, as well as templates and sample documents that can be used in designing, developing and implementing an effective awareness program. The new guide is considered a valuable tool to prepare and implement awareness programs that are addressed to public and private organizations. Similarly, in an effort to help raise awareness of information security and encourage secure handling of electronic data, the Agency has launched in 2011 a series of free videos in all 23 official EU languages (ENISA, 2011). The video clips promote secure online behavior in a range of areas from how to use strong passwords in order to protect sensitive data to methods for securing your computer. This is an effort to make the greatest impact on security matters and share the word that cybersecurity is everyone's responsibility.

The human factor and its important role in raising the overall awareness level and establishing an appropriate security culture has also been identified by software companies that deal with security products and services. Symantec's 2014

Internet Security Threat Report reports that targeted attacks have increased over the last year (Symantec Corporation, 2014a). Although - 2011 was reported as "the Year of the Data Breach", due to the increased number of breaches and acts of hactivism by the Anonymous group, 2013 has been described as "the Year of the Mega Breach". With a 62% increase in the total number of breaches and eight of the breaches in 2013 exposing more than 10 million identities each, the title given truly represents the picture. Cybercriminals, are used to incorporate zero-day vulnerabilities[2] which even though such vulnerabilities are usually patched within four days, still are able to threaten us all. Attacks where the attacker pretends to be a legitimate public source or law enforcement agency, demanding a ransom fine –also known as ransomware– have grown by 500% over the last year. At the same time, new and more directly profitable methods like Ransomcrypt –an attacker encrypts a user's file(s) and requests a ransom in order to unencrypt these files– have been adopted by attackers. Such threats can cause even more damage for businesses since files are not only used by the attacked victim but are also shared by others on shared network drives. The rise of online payment adoption has also facilitated this type of attack, which is expected to grow further in the coming year. Such attack raises the issue of prevention and backup as important in defending users and critical data from this type of threat. At the same time, a new prevalent ground for attacks seems to be in favor by hackers and this is the mobile with an explosive growth of scams and malware attacks. Despite the fact that mobile malware attacks is comparatively low, 38% of mobile users have already experienced mobile cybercrime. Although lost or stolen devices remain the biggest risk, the behavior of mobile users is the

[2] Zero-Day Vulnerability: a hole in the software that is not yet known to the vendor. Such vulnerability is exploited by attackers before the vendor becomes aware of it and releases a fix. SYMANTEC, PC Tools 1998-2010.

main cause that keeps the door open to attackers. Mobile users are used to store sensitive files online, share logins and passwords with friends and family, and store work and personal information on the same online storage. At the same time only 50% of these users take even the basic security precautions (Norton Corporation, 2013). The explosive use of mobiles phones with smart capabilities had also a direct effect on attacks related to social media where scams have increased over the last year. Although 12% of social media users report that someone has hacked their account and pretended to be them, a change in user behavior has not been observed since a large number of the users still share their social media passwords with others or connect with people they do not know. Finally, it seems that attackers are turning their focus on new and emerging technologies like the Internet of Things (IoT). Such concept which promises a world of connectivity and net presence for every consumer electronic device that has a SIM card is at the “peak of inflated expectations” although it is not expected to be placed in actual production stage for at least five to ten years from now (Hern, 2014). Still the installed base of such devices is expected to grow to 26 billion units by 2020 when at the same time the numbers of PCs, smartphones and tablets is use will only reach about 7.3 billion units (Rivera and Meulen, 2013). By year 2020 the component costs are expected to be so low that connectivity will become a standard feature for everything. This opens the possibility of connecting almost anything but at the same time creates a brand new environment of threats since IoT devices will become points of targeted attacks.

The 2014 Global Security Report published by Trustwave, continuous to identify compromises and weaknesses that results from poor user behavior (Trustwave, 2014b). With data breach investigations increasing by 54% in 2013, the

importance of the victims being able to detect a security compromise is evident. Still a shocking 71% of the victims were not able to detect the breach themselves when self-detection could shorten the timeline from detection to containment from 14 days to 1 day. Unfortunately the median number of days reported from initial intrusion to detection was 87. Similarly as identified by previous report, use of mobile phones pose a serious security threat since an amazing 100% of the mobile applications tested contained at least one vulnerability. The action plan proposed apart from the implementation of additional technological measures, involves also a user centric approach. Security awareness education is considered a priority (Trustwave, 2014a). Users should be protected from themselves and employees and staff should receive appropriate education on best security practices. Taking into consideration that weak passwords contributed to 31% of investigated compromises, it is evident that weak passwords should be eradicated by implementing and enforcing stronger password authentication policies, and users should be educated on this matter more effectively. Finally, users should be aware that securing all of their data is a necessity due to the diversification of data types attackers use to target. Users should be appropriately aware about the criticality of each data they possess, adequately prepared to protect it and ready to recognize a breach on their own so appropriate response and clean-up time is reduced.

Kaspersky Lab's 2013 Global Corporate IT Security Risks report, recognized that maintaining information security is the main issue that IT departments face today since 91% of the surveyed companies had at least one external IT security incident (Kaspersky Lab, 2013). Further to that, internal incidents should receive high attention since 85% of the surveyed companies reported internal incidents. Similarly as with previous security reports, a significant proportion of the incidents

were internal and involved the intentional or negligent actions of employees and the loss or theft of mobile devices. At the same time the personal mobile devices used for work related purposes remain one of the main hazards for businesses. Although the top IT function concern is the prevention of IT security breaches, training users on how to use IT systems receives low popularity the last two years to approximately 20%. In the case of security threats from internal sources, it seems that accidental data leaks by employees and loss or theft of mobile devices by staff, constitute the second and third most common internal threat. Incidents involving the misuse of mobile devices were among the most dangerous threats. The evolution of the “Bring Your Own Device” trend has affected security to such extend that mobile devices now form a separate class of threats with its own subcategories. This inevitable phenomenon has emerged a need for companies to implement additional security policies for mobile devices, however, this is not yet the case in all organizations. Among the actions taken to prevent future IT security incidents among large corporations, have to do with the investment into training existing employees in methods of incident prevention and as a result maintain a high level of employee awareness at all levels, not just among staff whose work is IT related. This will make a significant contribution to the overall security of the company since employees often become the sources of data leaks.

The following figure (Figure 2) summarizes and reports the trends over time in respect to information security awareness initiatives. More specifically the figure shows the percentage of organizations that claim to do awareness raising based on the PriceWaterhouseCoopers Information Security Breaches Surveys. Although the figure presents a steady increase on the awareness raising

initiatives by organizations, still the percentages are low. Also this steady increase seems to be suspended the last four years.

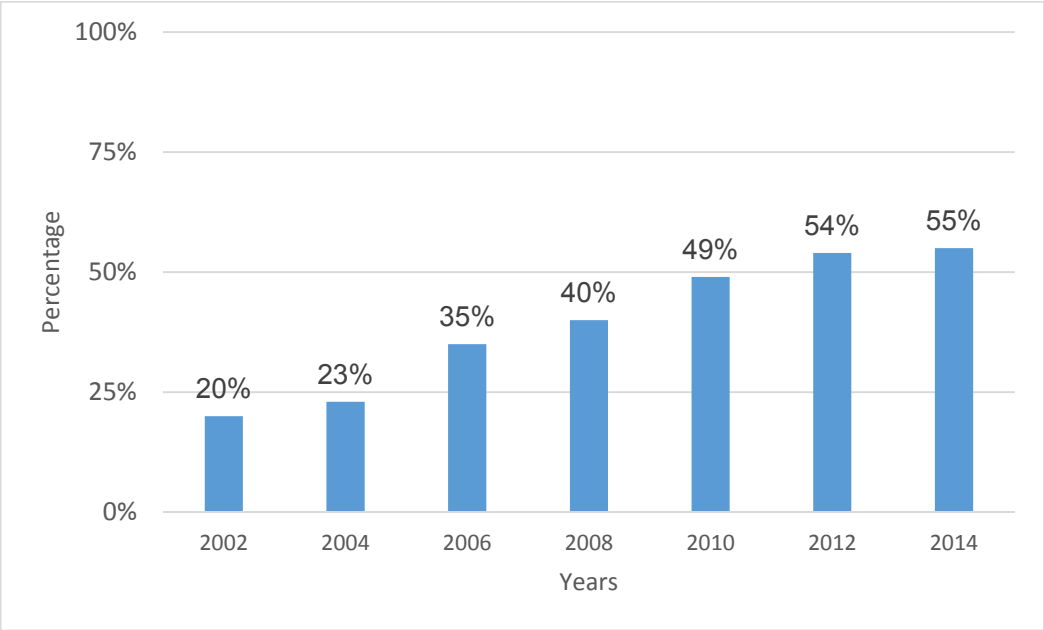


Figure 2: Organizations that claim to do awareness (Source: PwC)

To conclude, the state of information security in respect to Security Awareness and Culture as presented by reports from internationally acclaimed consulting companies, government agencies and software companies that deal with security products and services, can be summarized as follows:

- An increase in information security incidents over the last years is reported worldwide.
- The associated costs of data breach and recovery remain at very high levels.
- Detection levels are very low usually resulting in weeks or months before actual infiltration is detected.
- Changing trends are reported in the use of information technology that involve the use of the cloud, social networks and mobile device use, with emerged threats associated with these trends.

- With companies investing significantly in the improvement of security technologies, the interest of attackers has shifted to uneducated computer users who are still are considered the weakest link in information protection
- Security awareness training is considered among the top priorities for information security and among the leading practices in fostering an information security culture throughout all levels of an organization.

Information security needs have to be addressed at all levels, from the individual user to an organization and beyond that to the Government and the Nation. The massive Internet usage of lots of users either home or company ones with little or no prior knowledge poses a serious security threat. Security awareness education should be a component to companies and government agencies but not only limited to them. It should be spread to include school children, youngsters, teachers, parents and senior citizens and equip them with the knowledge needed to mitigate the threat. Considering young people and their information security habits, research has indicated that they are completely comfortable with using online services and social applications, but rather less informed concerning their safe usage. More specifically, a survey indicated that they are very comfortable in using ICT but lack the foundation knowledge required to protect themselves in the event of threats or abuse (Furnell and Phippen, 2007). Such rather worrying findings indicate that the next generation of adults lacks the skills to engage with online services in a safe manner. In other words the research shows an alarming potential future where a society produces an internet-aware generation which does not have the knowledge about the threat that exist online nor has the ability protect themselves. Further research should be made on the issue in order to identify the causes of such a reality.

2.4 Information Security and the Human Factor

As previously discussed, information security has been traditionally defined as the “preservation of preservation of confidentiality, integrity and availability. The main goal of any IT infrastructure is to achieve this triad by information security implementations and management. Information security is usually associated with three important components: (1) physical, (2) technical and (3) administrative. The physical component involves a wide variety of security related activities such as special buildings, guards, guns, cameras, etc. The technical component involves the use of electronic devices dedicated to protection such as access control systems, system monitors, firewall, etc. The administrative component involves policies, procedures and guidelines and mainly deals with how technology is to be used securely by those who actually operate it.

Through the last 15 years there is a tremendous increase in the variety of physical and technical security controls. Also new tools that improve security are constantly developed. At the same time, due to the increased dependency on electronic information, information security threats are more lethal than before. What someone would expect with such proliferation of security tools is that achieving a suitable level of security would be an easy task and security breaches would be minimum or non-existent at all. Unfortunately this is not the case. The problem lies to the fact that technology is designed to run without people but managed and used by people (Schultz, 2005). This refers to the concept of the “human factor” in information security.

In today's world, security threats can be classified as internal threats and external threats. Internal threats primarily include accidental security breaches caused by employees such as errors during the installation and maintenance of security technology, dishonest employees driven by revenge, shortcuts in the name of improving efficiency (e.g bypassing a firewall rule in order to facilitate a top management request), negligence or non-compliance to policies and procedures. External threats include virus and hacker attacks, technology failures, acts of nature, fraud attacks and spam. External factors usually receive a lot of media attention and are well-known, which makes it easy for an organization to recognize them and act accordingly. While most organizations appear ready to face and prevent external threats, they are inadequately prepared for the threats that originate from within the organization. The 2014 key findings from the Global State of Information Security Survey indicate that most incidents originate from everyday insiders like current employees (31%) or former employees (27%). These insider threats are considered more significant than threats from outsiders (PwC, 2013a).

A new type of employee has emerged and this is the "wired" employee. Most companies provide their staff with a laptop and a smartphone for work and often allow unrestricted personal use (PwC, 2013b). As time passes, these devices filled with important company data as well as with personal data will be subject to external security threats driven by the employee's personal habits.

According to IBM's Security Services 2014 Cyber Security Intelligence Index report, from all of incidents investigated, over 95% recognize that human factor as their main contributor (IBM, 2014). Despite the fact that companies employ a variety of security controls in an attempt to limit their risk of becoming a victim of

a security incident, the human factor is something that cannot be always controlled or relied on. Some of the most common human errors include:

- Opening of infected attachments.
- Use of unsafe URLs.
- Lost laptops of mobile devices.
- System misconfiguration.

Another common human error is the use of default username and password (Northcutt, 2007), or passwords that are easy to guess (CSCAN, 2014; SplashData, 2014). Although in many cases, policies are present that dictate password creation and usage, the strength of a company's security measures is as strong as the passwords that its users choose.

Additional survey findings plead to the same fact that human error if the largest information security risk to organizations (Kroll Advisory Solutions., 2012; Ponemon Institute, 2012b). At the same time, Ponemon has identified risky practices in which employees routinely engage. These include:

- Connecting computers to the Internet through an insecure wireless network.
- Sharing passwords with others.
- Reusing the same password and username on different online services.
- Leaving computers unattended in the workplace.
- Carrying unnecessary sensitive data on a portable device (laptop, unencrypted USB) when travelling.
- Connecting to company owned networks using personally owned mobile devices.

- Losing a device containing company data and not notifying immediately the appropriate organizational authority.

It is evident that information security cannot be seen as a single, discrete entity. It is a whole range of measures and should be viewed as a system, actually a complex one which combines a number of different aspects none of which can be regarded as more or less important. The human factor plays an equally important role.

Despite the presence of the latest technological improvements, it is still the people who are interacting and configuring information systems and services. According to an article by windowsecurity.com “our staff members are the ones who unknowingly contribute to the exposure of sensitive information” (Danchev, 2006). By using the term “staff members” the article specifically refers to system administrators, company executives and end users.

Although the level of information security knowledge is not comparable between these three groups (e.g. system administrators are expected to have much more knowledge on security issues than the other two groups), still mistakes that can compromise the security of systems are often made at all levels. For example, although system administrators are considered the key personnel in terms of information security good practices, it is still possible to make mistakes or engage themselves in unsafe behavior that can enable attackers to succeed. According to SANS Institute some of the worst mistakes information technology people make are (SANS, 2006):

- Connecting systems to the Internet without making sure that they are secure.

- Failing to educate users about how to behave when they observe a potential security problem. At the same time it is common that they give passwords and other sensitive information to users without properly authenticating them.
- Running unnecessary services which may be proven at the end an entry point for attackers.
- Failing to take common everyday security precautions (e.g. maintain regular backups, update antivirus software) or update systems when security holes are found.

Meanwhile, according to the same source, some of the worst security mistakes end users make are:

- Incorrect or inappropriate use of e-mail (e.g. spamming, opening attachments, etc.).
- Failing to take the appropriate measures for protecting their own machines (e.g. installing security patches, taking regular backups, install and maintain antivirus programs, etc.).
- Visiting or downloading from untrusted websites.
- Not adequately protecting sensitive data (e.g. writing down passwords or sharing them with other people).

Finally, according to the same source, senior executives can also be the source of security compromise due to insecure behavior or wrong actions and perceptions. More specifically among others senior executives may:

- Fail to understand that a security breach may have both an economic and reputational impact to their organization.

- Appoint people to positions where security is a serious consideration without providing them with the appropriate training or enough time to learn through on-the-job practice.
- Fail to realize that there is a close relationship between information security and business operations (e.g. business continuity) because they only understand the physical component of security.

To summarize the SANS findings, all groups that are members in an organization may compromise the security of systems but in different ways. Top level executives may compromise the security of systems by failing to understand its strategic importance (e.g. economic and reputational impact, business continuity, etc.). Information technology people through over confidence in the systems they are managing and their security knowledge (e.g. not taking common everyday precautions) and end users through their lack of awareness on how to deal with simple everyday technology issues in a secure way.

2.4.1 Information Security and the insider threat

It is evident that people are the company's greatest asset but at the same time its greatest liability. Most companies are in the dark about the insider threat. Even after the damage has been made the impact usually is unnoticed. At the same time many insider threats are ignored, overlooked or deliberately downplayed. According to the 2013 US State of Cybercrime Survey, Less than 50% of the companies have a formal plan for responding to insider security incidents (PwC, 2013a). To counter these threats it is important to understand the nature of the insider threat.

Events, incidents, even disasters and crises are part of our everyday life and determine the success or failure of a business as well as our life. They cannot be

ignored. The whole information security concept is based on the assumption that we should take measures to prevent, detect or respond to events of one type or another. Organizations review past security incidents in order to determine its cause so countermeasures can be identified for future prevention and avoidance. At most cases, it is the people who are the underlying cause of most security incidents. Nearly two-thirds of the worst incidents have an internal cause (BERR, 2008). But at the same time, people do more than just cause incidents. They can also prevent them, report them, fix them and learn from them. The human factor is the major factor in both the problem and the solution.

The first thing that is important to understand about people is to recognize their differences. Depending on their job objective some people may look more competitive that others, more caring, more wise, more authoritative or more conservative. People might look and act the same on the outside, but they can be very different on the inside (Lacey, 2009). That's why it is usually a shock to managers and staff to discover that one of their colleagues has been dishonest.

Insider threat refers to the behavior of employees who possess substantial access to the organization's information assets. This behavior may be intentionally or unintentionally disruptive, unethical or even illegal (Stanton et al., 2005). According to Schneier "Mathematics is logical; people are erratic, capricious, and barely comprehensible" (Schneiner, 2000). The idea behind this statement is that security can reach a state of perfection by using mathematics but unfortunately security systems are based on people whose behavior many times is neither predictable nor understandable. Indeed as Schneier mentions security is like a chain and it is only as secure as its weakest link. Stanton in his research believes that information security behavior may indeed be

understandable, organized and meaningful and describes both beneficial and harmful behaviors that information technology users within organizations enact that may affect security (Stanton et al., 2005). Categorized according to user intentions and technical expertise Stanton comes with a six-element taxonomy of security behavior:

- Intentional destruction: this malicious behavior involves strong intention to do harm to the organization's information resources but also requires technical expertise.
- Detrimental misuse: malicious behavior that includes intention to do harm through annoyance or rule breaking and requires minimal technical expertise (i.e. sending e-mail spam messages).
- Dangerous tinkering: refers to a behavior that requires technical expertise but with no clear intention to do harm to organization's information resources.
- Naïve mistakes: behavior requires minimal technical expertise and no clear intention to harm the organization's technology and resources.
- Aware assurance: beneficial behavior requires technical expertise together with a strong intention to do good by protecting the company's information resources (i.e. recognition of a security flaw).
- Basic hygiene: beneficial behavior requires no technical expertise but includes a clear intention to preserve and protect the company's information resources (i.e. a trained employee successfully resists a social engineering attempt).

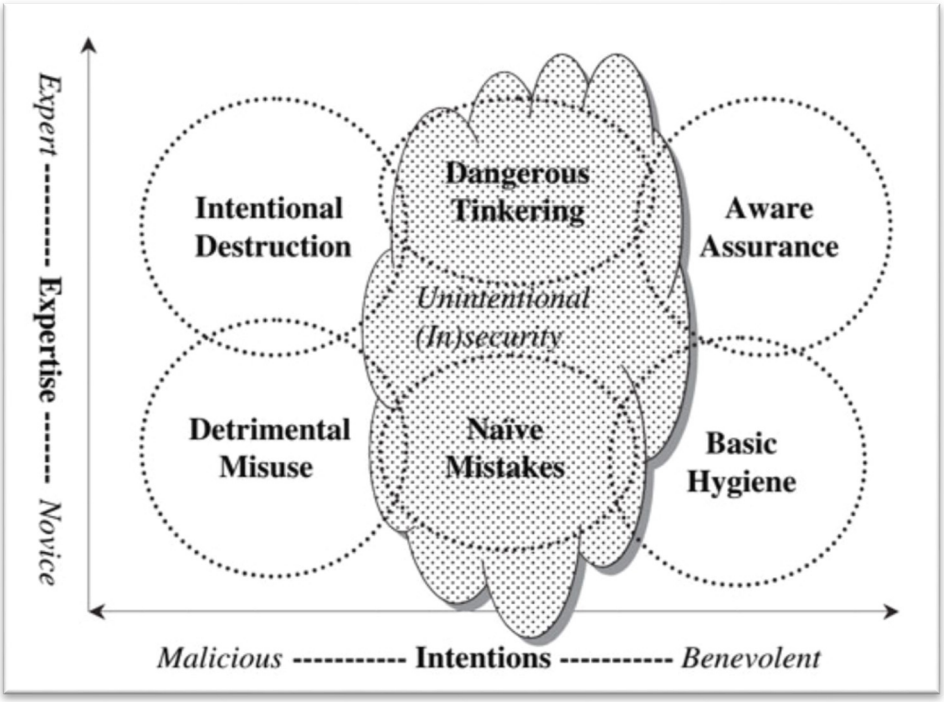


Figure 3: Taxonomy of end-user security behaviors. (Stanton et al., 2005)

If all six elements are placed on an x.y axis (Figure 3) based on intentions (malicious to benevolent) and expertise (novice to expert) it is concluded that sometimes individuals act without explicit intentions either to harm or help information security behavior. There are actually cases where “naïve mistakes” suggest a lack of awareness of basic information security principles rather than intention to do harm. Similarly, the case of dangerous tinkering suggests that an individual with a high degree of technical expertise may affect information security through his ability to setup a complex technology with unintentional consequences. This behavior is still unintentional.

Another issue closely related with the human factor in information security is the ability of users to understand and use security. The issue refers to the usability of the security features offered and how easily end users may benefit and use security options. There are cases where security functionality is presented

inappropriately within end-user applications making them difficult to understand and use (Furnell, 2005). For example, a series of pop-up menus in Internet Explorer asking users whether or not they wish to trust a particular certificate. Another issue that also leads to security usability is the case where a security feature is not immediately visible especially in the case of desktop applications where security is not the main purpose of the software. Common HCI design faults include software security functionality be hidden across different menus and sub-options or being placed under the 'advanced' menu options which will potentially scare the novice user who do not consider themselves to possess advanced knowledge.

2.4.2 Why do people make mistakes?

Many times we usually ask ourselves: "why did I do that?" There are many reasons behind inexplicable behavior, and most of these are based in social psychology. Some behavioral examples may be due to accidental causes some other may be considered as deliberate acts.

The National Research Council Computer Science and Telecommunications Board has made a distinction between deliberate acts and accidental acts that have an effect on information security (Computer Science and Telecommunications Board-National Research Council, 2002). Accidental causes are natural but non-deliberate (e.g. a programming error that causes a computer to crash) and are referred to as human error. Deliberate causes are the result of human choice. In information security literature, deliberate causes are

usually referred as ‘attacks’. Attackers are those who seek to cause damage deliberately.

The field of human factors has developed models and concepts for understanding varying types of human errors. These categorizations do not only explore the cognitive mechanisms involved in human error but also emphasize the role of organizational and management elements in creating conditions that lead to errors (e.g. faulty equipment, unclear procedures, poor management practices) (Reason, 1997). According to Smith and Sainfort, a work system may be conceptualized as having five elements: the individual, task, tools and technologies, environment and the organization (Smith and Sainfort, 1989). These elements may equally contribute in creating conditions that result human error and violations. These errors may result in security vulnerabilities or security breaches if the vulnerabilities are exposed. One of the most widely accepted taxonomy of human errors is the skill-rule-knowledge framework of Rasmussen. According to it errors may be divided into categories based upon an individual’s level of performance (Rasmussen, 1982):

- Skill-based level errors: errors that are made with routine tasks or tasks at which expertise when acquired very little attention is required (e.g. bicycle riding).
- Rule-based level errors: Such errors occur when a change is needed to modify the automatic behavior found at the skill-based level. They take place when rules and procedures are used to select a course of action in a familiar situation.

- Knowledge-based performance errors: when a type of control must be employed in order to resolve a novel or unexpected situation (e.g. repeated failures in a situation without a pre-existing solution).

Kraemer and Carayon conducted a survey in order to describe human errors and violations of end users and network administrators in computer and information security (Kraemer and Carayon, 2007). A total of 16 people working with computer and information security systems were interviewed. Eight network administrators from two academic computer laboratories were interviewed and eight computer and information security specialists from various industry areas (retail, insurance, financial, energy, health care, and manufacturing). Although the sample is rather limited, it may be used as a starting point in describing the security errors that result from the human factor. According to the survey the types of errors contributing to vulnerabilities and security breaches are either intentional or unintentional. Intentional errors are further categorized as mistakes or violations. For network administrators and security specialists most errors done are considered unintentional while intentional ones are mainly classified as mistakes rather than violations. In contrast, for end users (according to network administrators and security specialists), the vast majority of errors are intentional that fall under the violation category mainly because “the people we are trying to protect do not want to be protected, and they don’t see it as important”.

Concerning individual elements contributing to errors, assessment of security is the most frequently cited individual element for network administrators. The second largest subcategory for network administrators is end user perception. This subcategory is considered the largest for security specialists with second option defined as training. For most of the security specialist group, end users

feel that they do not have access to anything important and what they do (or *believe they do*) is just access the system.

For task and workspace environment elements that contribute to error, network administrators state that workload is the most important element that contributes to error (e.g. the frustration in keeping up with patch management), with duties (e.g. security related responsibilities) and structure (the organization of tasks or duties) as second and third elements.

Concerning the technology elements that contribute to error, inadequate hardware/software is the most frequently cited technology subcategory for network administrators.

Finally, concerning the organizational elements that contribute to error, security culture (21 comments) shares the same space in human error for network administrators as communication (20 comments), policy (21 comments) and organizational structure (17 comments). On the other hand, if comments are taken as a whole for both network administrators and security specialists, organizational culture is considered as one of the strongest barriers to organization-wide security (Kraemer and Carayon, 2007).

Coming back to reasons behind inexplicable behavior, and their roots in social psychology, Angus McIlwraith tries to explain “why people do stupid things” in relation to information security (McIlwraith, 2006). The reasons may be summarized as follows:

1. People have selective memory. They tend to forget things because they have a limited capacity for information and usually they try to operate

under stressful conditions. This can make rational people do irrational things. Such problem may be successfully addressed by an awareness program that will encourage people to temporarily stop what they are doing and try to think rationally whether the current situation has a security element to it.

2. Identity issues concerning the use of passwords. People who exhibit good password behavior are usually considered as paranoid by others, or the kind of person who doesn't trust anybody.
3. Resistance to followership. People do not comply with regulations just because they do not want to follow orders.
4. Social issues. Sharing your password is considered by many users to be a sign of trust in their colleagues.
5. Illusion of safety. Many users think that the data stored on their system is not important enough for a hacker to target it.
6. Level of damage caused. Most users think that somebody getting into their account could not cause any serious harm to them or their organization. This is closely related with their opinion concerning the usefulness or regularity of backups.
7. Informal work procedures. Current policies and regulations often contradict with informal work procedures (e.g. an employee on vacation shares his password with a colleague so he can do his work while he is away !!!).
8. Accountability. Although many users are aware that their behavior does not comply with security regulations, they do not feel accountable because such regulations believe are unrealistic and their behavior is considered as common practice.

9. Illusion of security. Many users believe that whatever security precautions they take, if a hacker targets them, their system will be eventually compromised and there is nothing they can do to avoid it.
10. Increased security may cause hacker's interest. Many users believe that a system with strong security mechanisms is more likely to attract hackers.

It is evident from the above that it is part of the human nature to make mistakes. These mistakes are sometimes intentional, or some other times due to negligence. The human factor is identified as the greatest root cause for security breaches but at the same time, the company's greatest assets. Since people are usually part of an organization, it is important to examine the relation Information Security with the corporate culture.

2.5 Corporate culture and its relation to Information Security

In today's modern economy, the reliance of organizations to information technology has increased dramatically. Technology not only continuously develops and evolves but also has become the root cause for the creation of new types of businesses and services. Outsourcing, downsizing and off-shoring are very common practices due to technological advances and as a result enterprises have been extended with different technologies and cultures in an effort to become more efficient (Johnson and Goetz, 2007; Koskosas et al., 2011). Information has developed into a strategic asset for enterprises who now have a growing dependence on their information systems for their smooth operations. Computerized information systems have transformed from everyday commodity tools to ultimate strategic tools for governments and organizations. At the same time, this dramatic increase of organizational dependence in information

technology has brought a similar increase to the number of threats related to the adoption of this technology (PWC, 2014; Symantec Corporation, 2014a).

Due to the continuous increase to the number of security breaches, information security has evolved into a very popular area. Organizations tend to focus their security practices on technical issues like encryption, intrusion detection systems and access controls. But information security problems in organizations are closely related with employee behavior. According to many reports, major security failures are the result of poor security behavior by organizational staff (Danchev, 2006; BERR, 2008; Kroll Advisory Solutions., 2012; Ponemon Institute, 2012b; IBM, 2014). Therefore, information security can no longer rely only on physical and technological controls but focus on employee commitment and understanding of the objectives of information security. The most effective way to protect vital organizational information is to promote security in the daily activities of the organization. In other words, security must become part of the organization's culture.

Technical controls are important but their efficiency is dependent on the competency and behavior of people who implement and use them. So the behavior and actions of people determine the effectiveness of information systems. Since information that resides in an organization's systems is an asset for the whole company, effective information security needs to become part of how everybody conducts daily business and should become second nature to all members of the organization from top management to typical employees. Changing human behavior and attitudes in an effort to enhance awareness among employees about information security tasks are part of what is called organizational culture.

Culture is a concept adopted from anthropology for organization management research and is a critical factor for organizations to continue living. The need to foster a culture in which users are aware of security issues and have the required knowledge to respond appropriately, is more that evident since the lack of awareness of security issues are among the most significant causes to security incidents.

Corporate culture can be defined as:

> *"A pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way you perceive, think, and feel in relation to those problems" (Schein, 2004) .*

Schein further develops organizational culture into three levels (Figure 4):

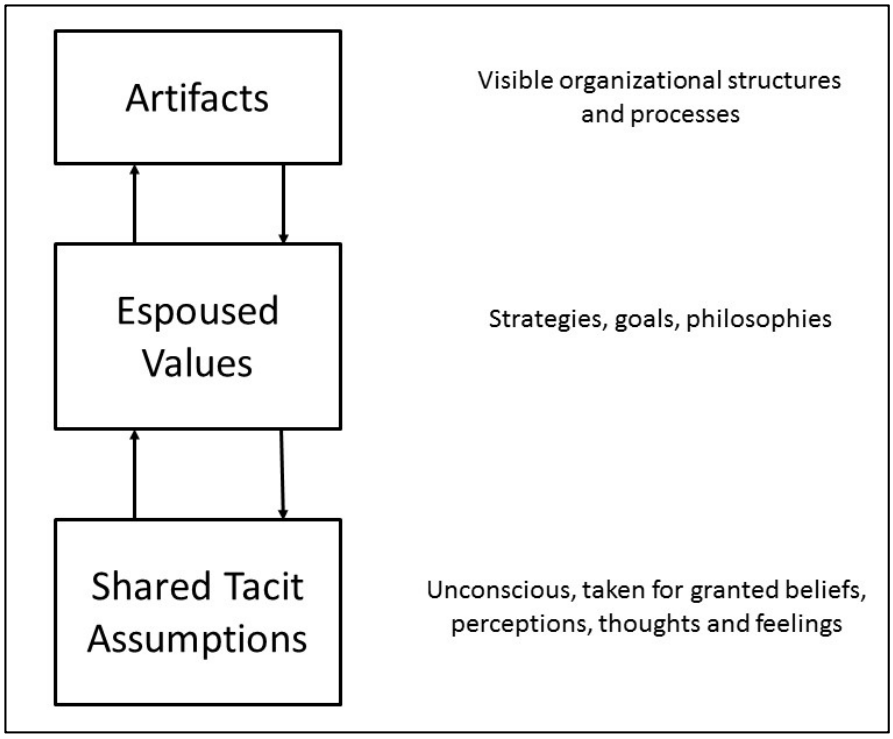


Figure 4: Levels of Culture (Schein, 2004).

- Artifacts: what an individual can see, hear and feel in regard to an organization. It may include the architecture and décor, the clothing of people, organizational processes as well as other tangible expressions of culture like logos, brochures and organizational slogans. All these artifacts are easily spotted by outsiders when in the organization's premises but as far as employees are concerned, these artifacts are part of their conscious thinking. Although artifacts are easily observed they are not considered as a reliable judgment for an organization's culture. In other words although, at the artifacts level, corporate culture is very clear, why employees of an organization behave in a certain way is not and should be further explored by talking to them in order to gain an understanding of their perceptions about the artifacts (Schein, 2004).
- Espoused values: this level results as a continuation of the previous level and is achieved by asking questions about organization's artifacts in order understand the organization deeper. This process refers especially to those artifacts that seem inconsistent with what expected. This is usually achieved by asking employees (referred to as "informants") who will explain their organization. Again further inconsistencies may be observed at this level that is differences observed between visible behavior of an organization (artifacts) and some of the espoused values. In other words what values an organization hopes to endorse may be different from what is actually expressed in the behavior of the organization. For that reason a deeper level is necessary in order to understand the culture of an organization.

- Shared tacit assumptions: the deepest level of culture that must be examined in order to understand organizational culture. It refers to the beliefs and values that key leaders or founders of the organization endorsed and as a result the organization became successful. If these belief and values lead to the success of the organization in the chosen environment then they eventually become shared and taken for granted. In other words, the core of the organizational culture are these mutually learned beliefs and assumptions that are taken for granted as long as the organization continues to be successful. Although these values were the original abstract thoughts of the founders of the organization, they have become shared and taken for granted as new members of the organization realize that these values of the founders must be right since they have led to organizational success.

It is evident that people base their everyday behavior on shared tacit assumptions. So if the shared tacit assumption level of corporate culture can be changed, the behavior of employees would change at the artifacts level. In order to achieve compliance to information security practices, inappropriate actions and behaviors by employees have to be minimized. This can be achieved if information security practices become an internal part of the corporate culture that exists in an organization.

Corporate culture determines what behavior is acceptable in an organization. Once this behavior is learn and understood by all employees they develop beliefs and assumptions that are shared among them and become the rules on how their job should be done. So in order for an organization to establish a corporate culture that is suitable for protecting information assets, the behavior and actions

of employees should evolve in that direction. That is acceptable behavior in an organization should be reflected at the espoused values of the corporate culture. Then employees will develop beliefs regarding the appropriate information security practices which eventually be internalized by becoming part of their shared tacit assumptions. So the espoused level of culture will correspond with the shared tacit assumptions level of culture. In that way the employees' behavior at the artifacts level will support the vision of information security.

The above process can be successful by incorporating the following methods:

- Setting an Information Security Policy.
- Establish and Information Security Awareness program

The objective of the information security policy is to influence the espoused values level of culture in terms of the organizational vision in respect to information security. This is achieved by educating employees (especially non-technical ones) about the risks associated with their daily exposure to information technology. Also the information security policy should describe the organization's vision regarding the protection of information along with disciplinary action in case the policy is violated. Finally the information security policy should foster a positive attitude towards information security by means that security is not about restricting daily operations but an additional mean for organizational success.

Once a corporate information security policy is set, compliance to this policy must be ensured. This is achieved by making employees aware of the policy its objectives and importance. The establishment of an ongoing information security awareness program not only will help employees understand the importance of

the information security policy but also provide them with the necessary knowledge to overcome the daily threats associated with the use of information technology. In that sense, a security awareness program works as a mechanism to cultivate the behavior of employees towards information security.

2.6 The changing trends in Information Security

The use of information technology has dramatically changed over the last ten years. Not only we have a wide adoption of information technologies among all types of businesses worldwide but also the profile of end users who use this technology has also changed. We have moved from a situation where all users of technology were technology specialists working in a centralized computing environment, to a situation where most company employees are considered end users who operate all aspects of computer systems as well as critical data and networking infrastructures. (Thomson and von Solms, 1998; Boshoff and Van Niekerk, 2011).

The significant developments in the area of information technology are one of the reasons why the profile of the end user has changed so significantly. More specifically the following technological advances have been observed over the years, which have also played a major role in the changing trends in information security:

- Decommission of the standalone computing environment: this form of computing was used by the first computers introduced in business. Large machinery susceptible to environmental conditions were housed in separate buildings under a controlled environment. These computers were protected by physical controls without the necessity of

security knowledge from the part of the end user. At the same time, these machines were operated by one user at a time as stand-alone devices with no networking capabilities and very limited options for portable storage. So the threats to this form of computing environment were physical in nature (e.g. floods, earthquakes, fires, etc), and the precautions taken to minimize them were considered easy and effective.

- Multi user environment evolved: under this form of computing more people are able to work on a machine at the same time and not necessarily within the computer center. In other words, physical access control to the computer room is no longer a physical measure that is taken into consideration since users are allowed to access data electronically through various locations within the organizations network environment. Also many components (e.g. hardware devices) can now be shared among many people. Security precautions under this computing environment were largely implemented through user authentication with a username and a password. Also workstations were operating as dump terminals again with very limited capability for portable storage and as result it relatively easy to implement security restrictions.
- (R)evolution of personal computers and networks: the wide availability of personal computers, their continuously increased computing power and at the same time their decreasing price have completely phased out the previous multi-user environment in favor of a more flexible environment. Also the tremendous expansion and reliability of LANs, WANs and the Internet has brought new and more productive

environments not only for the enterprise user but also for the home user.

These advances along with new technologies that evolved as a result of networks and Internet proliferation, have brought great challenges in the area of information security. As referred previously in this chapter, the rise in the use of cloud computing puts an extra degree of potential risk since cloud is not included in the security policies of companies. Also, there is an increased number of remotely hosted services with increasing numbers of companies storing confidential data on the Internet. The use of social networks by organizations is believed as important to their business and mobile device use is still an un-stoppable trend. At the same time attackers are turning their focus to technologies that emerged for the explosive growth of connectivity like the Internet of Things (IoT). The promise of a world of connectivity made possible for every electronic device that has a sim card or network capability is at the peak of the industry expectations although not yet in full production stage.

This explosive growth in connectivity and information sharing has changed the security landscape making information security a challenging and difficult to manage task (IBM, 2013a). Similarly this growth will drive cybercriminals into investing further resources in developing more sophisticated attacks. Given this rising complexity and volume of threats, organizations should consider approaches to information security that integrate not only technology and processes but also people. (PWC, 2010; Jarvis, 2013).

Recent research indicates that among many factors which made such incidents possible more than 70% can be attributed to end-user error and misconfigured systems or applications (IBM, 2013b). The origin of these incidents indicate that

it is no longer possible to maintain effective information security by using physical and technical controls alone. It is necessary to educate users on everyday issues concerning information security. A change is user behavior has to be achieved to such degree that not only they carry their day-to-day operations in a secure manner but also that this behavior is subconscious and natural. For example as locking your household door in order to avoid burglars is a natural instinct the same should apply in the case of locking your computer or signing off when not in the office.

Although in the next years security technology will continue to evolve in order to cope with the increasing number of security threats, building a risk-aware culture where zero tolerance concerning carelessness is allowed, is considered a more effective practice for cyber security defense. Also this enterprise's culture of security must be extended beyond company walls to include not only contractors and suppliers but also individuals where best security practices should be incorporated into their everyday lives.

2.7 Chapter Summary

In the past 20 years, technology has infused every facet of business operations. Moving from the typical mainframe environment to personal computers and network revolution, IT with cutting edge capabilities has become a commodity for everyone. As a result the concept of computer security has evolved into the idea of information security. The purpose of this chapter was to introduce information security concepts and how these concepts apply in today's environment. Information security surveys and reports have indicated that the information security scene has significantly changed. Increased numbers of security breaches as a result of employee responsibility are observed resulting in loss of

market share, damaged reputation and even legal implications. At the same time new IT trend has receive an exponential growth. Adoption of cloud computing, remotely hosted services, mobile device use, social network adoption and the Internet of Things are only a few examples that indicate that information security can no longer be achieved by technological means alone but also involve those who actually operate these systems. The human factor and its relation to information security has been examined with issues and topics from social psychology in order to determine the reason behind inexplicable behavior that could lead to security mistakes. Finally, the concept of corporate culture has been studied along with its relation with information security as an effort to foster a culture in which users are aware of security issues and have the required knowledge to respond appropriately.

The next chapter continues by examining the current state of the art in terms of actually fostering security awareness and culture. Conclusions will be drawn from the existing research and the scope for further research will be determined. More specifically, emphasis will be drawn on the concept of embedding and understanding InfoSec concepts as early as possible and certainly before people reach the workspace. The role of educational institutions towards supporting this effort will be examined.

Chapter III – The Importance of Information Security Awareness

3.1 Introduction

Information security is a vital component at all aspects of our everyday lives, and is considered a critical success factor for today's businesses since technology is an integral part of all our endeavors. The purpose of this chapter is to examine the importance of information security awareness focusing also on its interdisciplinary nature in an effort to prepare a workforce capable not only of protecting business information assets but also personal user information. A study of the existing literature is presented in order to determine the current state of the art in terms of efforts towards fostering security awareness and culture. Emphasis is given to the concept of embedding and understanding information security concepts as early as possible and definitely before people reach the workspace. Towards this effort, the role of educational institutions is examined.

3.2 The importance of Information Security Awareness and its interdisciplinary nature

Given the rising level of breaches, it is more critical than ever for organizations to raise the level of security awareness by turning their users into the first line of defense.

The National Institute of Standards and Technology (National Institute of Standards and Technology (NIST), 1998)in their article "Information Technology Security Training Requirements: A Role- and Performance-Based Model, Special Publication 800-16" use the following definition for security awareness:

> "*Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities the learner is a recipient of information, whereas the learner in a training environment has a more active role.*

Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate job performance."

Rebecca Herold (2005) at her book "Managing and Information Security and Privacy Awareness and Training Program", defines awareness as"

"*a learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure*."

According to Information Security Forum (ISF), security awareness is:

"*the degree or extend 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." (Information Security Forum, 2002)

All of the above widely accepted definitions have a lot of similarities. Awareness has to do with realization of information security threats so people are aware of what may happen as a result of poor information security. It also has to do with willingness to accept appropriate behavior to counter take the various threats and attacks. So awareness by itself has no value unless a desired change in security behavior is achieved.

In summarizing the above definitions, security awareness is a proactive measure and has to do with making end users and employees aware of how to protect personal and organizational information by applying information security practices. According to NIST, information security in terms of learning is a continuum which starts with awareness, build into training and finally evolves into education (National Institute of Standards and Technology (NIST),

1998). Awareness being at the bottom of the continuum is required by all employees. Training is required by those individuals with specific roles in the organization that require special knowledge of security threats and vulnerabilities. Finally, education applies to those individuals who have IT security as their profession. NIST clearly separates awareness from training by defining the purpose of awareness presentations as “simply to focus on security” with an objective to allow individuals recognize IT security concerns and behave accordingly.

Information security has to be managed effectively and such process requires a combination of technical as well as procedural controls in order to protect information assets. However these controls can be bypassed or abused by employees who have appropriate elevated access to information systems and who will neglect to comply with the organization’s security policy. Such behavior may also be observed on home users of information systems and is usually the result of the lack of awareness in regard to information security threats. Such incidents caused by employee mistakes result in far more damage to businesses every year than external attacks.

In order to safeguard a company against all IT threats requires adequate attention to many aspects of security Among others it is important to maintain a high level of employee awareness among all levels and not just among staff whose work is IT related (Kaspersky Lab, 2013). Ernst & Young’s Global Information Security Survey 2013 recognizes that organizations are moving towards the right direction concerning information security but “more still needs to be done – urgently” (Ernst & Young, 2013). Awareness of security threats and risks is a crucial step since it is recognized as a method that drives

improvement. Taking into consideration that companies do not have the skilled resources to support their needs (only a 30% of the companies according to the report are considered mature or very mature in terms of security awareness, training and communication), the establishment of an information security awareness program that will foster the appropriate security culture throughout all levels of the organization is one of the leading practices that will enable InfoSec improvement (Ernst & Young, 2013).

Finally, information security awareness as a preventive measure is considered as an important prerequisite by several international standards. BSI's self-assessment questionnaire concerning ISO/IEC 27001:2013, recognizes that everyone within the organization must be aware of the importance of information security policy and adhere to it through proper awareness, education and training (BSI, 2013). Also COBIT 5 realizes the importance of a knowledge-sharing culture through an information training and awareness program as a prevention measure for data loss (ISACA, 2012; ISACA, 2013).

It is evident that the protection of confidential information from unauthorized access along with secure online behavior, is very important for every organization and individual. As it is important to invest in technology to protect your assets, it is also equally important to invest in the education of employees. Since the company's information security team cannot provide all the necessary security measures for all kinds of threats, an overall enterprise awareness plan is required in order to cope with the wide variety of incidents an organization might face and such plan requires the active participation of every employee (Olzak, 2006).

Herold (2005) also realizes that an information security awareness program not only adds an extra level of strength in coping with today's threats and attacks but can also be an important component of an organization's business success. More specifically, corporate reputation can be severely damaged because of the lack of a security awareness program due to the following reasons:

- Regulatory requirements compliance: There is an increasing number of laws and regulations that require some form of training and awareness activities to occur within the organization. Examples of these training activities include frequency of organizational communication concerning personnel policies and procedures, ongoing and constantly updated awareness initiatives with appropriate measurement of desired results, training on ethical work practices, etc.
- Customer trust satisfaction and corporate reputation: Customers and organizational partners are bombarded everyday with privacy breaches from the media. Protection of customer privacy is one of the most important issues companies are facing today. Providing a personnel awareness program on how to deal and safeguard personal identifiable information will establish customer trust for existing customers and attract new ones. Also it will ensure the successful building of a good corporate reputation since personnel and business partners follow the right security precautions to reduce the risk of compromising personal information.
- Due diligence: Due diligence has to do with the assurance that management adequately protects corporate assets such as confidential information. There are laws and regulations that require

organizations to have established internal controls that support the privacy and security of sensitive information. Such laws and regulations can be a powerful motivator for the implementation of an employee awareness program.

- Accountability: Employee accountability is a crucial component for the success of an information security program. It is generally the norm that personnel performance is measured by certain activities which eventually impact career advancement. If information security and privacy is connected with personnel performance, then personnel accountability is more clearly understood and are more likely to comply. Such accountability can be achieved through well-organized security awareness programs.

From the above it is evident that the purpose of information security is to protect organizational assets that are critical for its success and business continuity and at the same time reduce business damage by preventing and minimizing the impact of security incidents. Information security can be achieved by both technical and non-technical aspects. As part of the non-technical aspects, the human component has been recognized to have an important role in information security since the only way to reduce security risks is through making employees more information security aware.

3.3 Assessing the state of the art in building security awareness and culture

The purpose of this section is to cover relevant literature on the current state of the art in terms of efforts towards fostering security awareness and culture, as well as some of the barriers and challenges in the area has been identified. In

this effort, information systems and information security journals and articles were explored through the aid of digital databases (i.e. ACM Digital Library, Elsevier Science Direct, Emerald digital library, online publications, IEEE electronic library, EBSCO, etc.). Additionally, conference proceedings were examined and information security textbooks were explored.

3.3.1 An Overview of existing information security awareness approaches

Anttila et al (2007), identify different levels of needs for information security awareness and learning (e.g. ordinary citizens, business leaders, experts), and argue that it is impractical to require that everybody needs to know everything about information security. Different levels require different knowledge and the different deepness-levels of intellectual behavior in awareness and learning are categorized according to Bloom's Taxonomy[3]. Traditional training and education approaches are not enough in our current modern society. Based on the increasing degree of connectivity, the degree of interactivity, and the degree of sharing information between experts, business leaders, and ordinary citizens, new learning theories and new practical web 2.0 applications have been proven effective and useful in learning. Also, according to the authors, although professional certifications in information security are widely recognized today, they are used as a method to convince others that the hold of the certification is capable to carry out tasks in information security. However, the level of knowledge of these certification programs is very basic. The European Network and Information Security Agency follows a similar (maybe broader) categorization

[3] An approach to educational psychology developed by Benjamin Bloom, according which classifies levels of intellectual behavior important in learning. Six levels are identified within the cognitive domain, from the simple recall or recognition of facts, as the lowest level, through increasingly more complex and abstract mental levels, to the highest order which is classified as evaluation.

approach concerning the different levels of needs for information security awareness and learning (ENISA, 2010). The categorization is as follows:

- Home User: citizens with varying age and technical background who use ICTs for personal use anywhere outside their work environment.
- Employee: all organizations' personnel.
- Mid-level manager: managers throughout the organization responsible for personnel performance. Usually non-technically oriented need to be educated on the importance of information security in order to implement relevant security policies within their unit.
- Executive management: decision maker for investment in security.
- System administrator: IT related personnel responsible for the technical aspects of security within the organization.
- Third party: partners, suppliers and consultants contracted to work in an organization.

In addition, several other partners or bodies can be used to help deliver the awareness messages as part of an initiative such as community centers, ISPs, leading academics, governments, etc. Different groups require different levels in terms of security awareness and training. For example, home users between 7 and 15 years old need to be taught of what is right and wrong in respect to technology borders while adults of the same group needs to be aware of relatively new threats. SMEs must realize that information security management fits into the overall company strategy and clearly understand the effects of a security breach to their business.

Cox et al (2001), state the importance and the criticality of user behavior to IS security. Their study examines three approaches which can have an impact on

IS users' behavior in an academic setting: (1) a discussion session, (2) a checklist, and (3) a web based tutorial. All approaches seem to be valid, whether the objective is to raise awareness generally or to support the introduction of relatively novel technologies such as the encryption of e-mail. However, the study does not give practical guidance on how to set up these approaches. According to the same study, security determines the requirements of both technology and users. Although good technical solutions can establish a baseline for secure information systems, human behavior is equally important. Therefore, users must understand IS security issues and organizations must make sure that their employees understand their role in respect to security. This approach with respect to technical and social matters expresses a socio-technical perspective.

Denning (2006)argues that since people are considered one of the major points of vulnerability, training is an important part of defensive information warfare. She proposes IS security awareness training programs as a means to inform employees at different levels (staff, systems administrators, etc.), students and partners with respect to security policies, make them aware of the risks and potential losses and teach them proper utilization of IS security practices and technologies. The issues addressed by Denning suggest a social view of IS security since it includes people's motivation, societal and cultural aspects. In addition, technology and technique is considered important in ensuring IS security. This indicates a technical viewpoint. Guidance is given on how to design and implement such training in practice.

Desman (2003) identifies as the most frustrating aspect of creating a solid program of information security within any installation, the effort to gain cooperation of the staff who use the organization's assets on a daily basis. The

teaching of information security awareness must be directed towards persons who use the PC for their day-to-day duties and will not spend time on something they deem not to be worthwhile. In reaching the audience, ten tips (commandments) are presented with an attempt to encapsulate them in an organized manner so they can be applied in a program on a step-by-step basis. These ten "commandments" are the following:

1. *"Information security is a people, rather than a technical, issue.*
2. *If you want them to understand, speak their language.*
3. *If they cannot see it, they will not learn it.*
4. *Make your point so you can identify it and so can they.*
5. *Never lose your sense of humor.*
6. *Make your point, support it, conclude it.*
7. *Always let the recipients know how the behavior that you request will affect them.*
8. *Ride the tame horses.*
9. *Formalize your training methodology.*
10. *Always be timely, even if it means slipping schedules to include urgent information".*

These commandments realize among others that information security is a people as well as a technical issue and if you want them to understand you, you must effectively communicate with them understanding their different backgrounds. Extra effort should be made in order for the security awareness message to reach the majority of the intended audience in such a way so its purpose is readily identified. Despite the seriousness of the message a sense of humor can be proven helpful in making and supporting your point.

Desman clearly claims that IS security is not a technical but rather a human issue. Although the technical countermeasures (e.g. Encryption) must be in place, security always starts from an organizational and human-related basis. His perspective is definitely socio-technical.

Dodge et al, (2007) reinforce the need for security education and training using security exercises on a regular basis. In their research they evaluate a users' propensity to respond to email phishing attacks and describe the considerations in establishing such a process as an evaluation of an information assurance education program. This indicates a social viewpoint of information security.

Forcht et al, (1988) raise an important issue to IS security that is the awareness in computer ethics and emphasize the role of the human factor (attitudes, actions, sense of right and wrong) in addressing issues of security. The study proposes that building a strong base in terms of ethical awareness and constantly reiterating this base, can help organizations increase their IS security.

Furnell et al, (2002) present a prototype tool for IS security awareness training. The tool enables individuals pursue self-paced training by providing an environment that permits the use of simulation in order to introduce the use of security in a number of pre-defined scenarios. According to the authors, this familiarizes employees with security situations they will face and the types of countermeasures available. This tool is evaluated as extremely useful in small organizations where specialist knowledge is scarce and issues need to be addressed by existing staff. IS security is seen as having a socio-technical role. The importance of technical and organizational sub-systems is emphasized, and both are working in mutual balance.

Hansche (2001b), focuses on the first step on providing computer and information system security, that is developing and implementing an effective security awareness program. The goal of the program is to heighten the importance of information systems security and it is achieved through the following five stages: (1) setting the goal of the program, (2) deciding on the content of the program, (3) selecting delivery options, (4) program implementation, and (5) program evaluation. Although she sees IS security as having a technical role, she also claims that users who are aware of IS security issues, are the single most important asset in detecting and preventing security incidents. Seeing an employee as an asset to ensure security emphasizes the social view of IS security. At a following study, Hansche describes a framework to help develop an information system security training program. Before the design and development of course content, Hansche presents as a major challenge of a training program the support from all levels of the organization, especially senior management, and suggests methods to help persuade senior management of the importance of sponsoring training. The framework contains the following phases: (1) establishing the information system security training needs, (2) developing the program plan, (3) training design and development, (4) implementation, and (5) program evaluation.

Hudson (2006), tries to identify the framework of a successful security awareness program, and it includes examples of techniques (like themes and slogans, seminars, new employee orientation, etc.) that can be used in a program. The building blocks are broken down into five major areas (corporate culture, company awareness level, security policies, budget and time constraints, and leadership support), and numerous awareness raising techniques are presented,

stating clearly at all times that security awareness is an ongoing and not just a one-time event.

ISO/IEC standard 27002:2013 2nd edition, “Information technology – Security techniques - Code of practice for information security controls”, argues that providing appropriate awareness, training, and education is considered a critical success factor to the successful implementation of information security within an organization (International Organization for Standardization (ISO), 2013). Among the responsibilities of top level management is to ensure that all employees and contractors are motivated to fulfill the information security policies of the organization and achieve an appropriate level of awareness on information security relevant to their roles within the organization. Furthermore, all employees of the organization should receive appropriate awareness training and regular updates in organizational policies and procedures. The standard recommends that IS security awareness training is used to introduce new employees the organization’s security policies and expectations before access to information or services are granted. It also claims that ongoing training should include security requirements, legal responsibilities and business controls, correct use of information processing facilities and information on the disciplinary process for employees who have committed a security breach. The considerations on organizational, technical and human aspects of information security are rather balanced and indicate a socio-technical viewpoint. Furthermore, according to the standard, new employees should attend IS security awareness training before they are granted access to information or services.

According to Kruger and Kearney (2006), since information security awareness is a dynamic process, it can be made even more difficult in an environment where

risks continuously change. Awareness programs need to be continually measured and managed to keep ahead of changes in risk profiles. The authors of this journal article have developed a prototype awareness measurement tool that may assist a great deal in providing feedback to senior management on what is happening to the company in terms of information security and assist them in their function of controlling and directing strategic objectives set for information security. The tool methodology includes a description of what is to be measured in terms of awareness and how is to be measured (presentation of mathematical formulas, weight analysis, questionnaires in order to produce a regional and a global awareness map). It is important to mention at this point that the implementation of a security awareness program does not guarantee that the employee participants understand their role in the security function. Awareness training can convey information security knowledge but a change of culture will reduce the gap between what and information security policy dictates and how actually the people behave (Stahl, 2006). The issue of employee commitment is raised here. A structured approach needs to be followed in order for the awareness program add value to the organization and at the same time make a contribution to the field of information security.

Mellor and Noyes (2006) also raise the issue of personal commitment and accountability in security training. They argue that personal accountability can be added into the security training process and play a valuable role in increasing the overall strength of the human factor in information security. A baseline training and assessment instrument is created to cover ten domains of information security (proposed as: passwords, social engineering, email, physical security, locking or logging off your computer, unauthorized programs, handling confidential data and material, internet usage, phishing, and handling storage

media and portable computers), and consists of five phases according to the NIST SP800-16 proposal (needs analysis, goal formation design, development, implementation and evaluation). The study showed that a great deal of personal learning has occurred as individuals were personally instructed in each of the ten information security domains. Also, raised awareness, is strongly correlated with security accountability.

Similarly, according to Peltier (2002), a strong security architecture will be effective if there is a process in place to make certain that employees are aware of their rights and responsibilities. According to the study, an IS security awareness program should have the following stages: (1) segmenting the audience (by job function), (2) establishing the roles expected of the employees, and (3) delivering the message. At all cases, the goal of the program is to explain in business terms why something is needed. Peltier also suggests a wide range of means in order to convey the awareness message (training sessions, videos, brochures, newsletters, booklets, and practice with the help of an instructor). In addition, he claims that IS security represents a cultural change. The considerations of Peltier of organizational and user-related matters represent a social viewpoint.

NIST (1995), identifies that an effective computer security awareness and training (CSAT) program requires proper planning, implementation, maintenance, and periodic evaluation. The report presents the following seven-step approach for developing an IS security awareness training program: (1) identify program scope, goals, and objectives, (2) identify training staff, (3) identify target audiences, (4) motivate management and employees, (5) administer the program, (6) maintain the program, and (7) evaluate the program. In addition to

technical and organizational IS security measures, NIST considers also end-users a critical factor in guaranteeing the security of computer systems. This represents a socio-technical viewpoint.

NIST Special Publication 800-16 (1998), presents a conceptual framework for providing IT security training. It introduces a model where learning starts with awareness, builds into training and evolves into education. Because employees acquire over time different roles relative to the use of information systems, their needs for information security training change. This is recognized by segmenting the training level into six functional specialties: (1) manage, (2) acquire, (3) design and develop, (4) implement and operate, (5) review and evaluate, and (6) use. The above mentioned specialties are examined relative to three fundamental training content categories: (1) laws and regulations, (2) security program, and (3) system life cycle security. The study, since it describes a methodology that is based on each employee's specific role in the organization, takes a social view of IS security.

NIST Special Publication 800-50 (2003), provides guidelines for building and maintaining a comprehensive awareness and training program as part of an organization's IT security program. This guidance is presented in a life-cycle approach. According to the document, the critical steps in the life cycle of an IT security awareness and training program are: (1) awareness and training program design, (2) awareness and training material development, (3) awareness and training program implementation, and (4) post-implementation. The document provides assistance towards different aspects that occur throughout the awareness and training program like: identification of need for awareness and training, development of strategy and plan, establishing training

priorities, obtaining funding to the training program, selecting awareness topics and finding sources of material, implementing training material using a variety of methods, and evaluating the effectiveness of the program.

Schultz (2004), like many of the previous scholars, stated the importance of security training and awareness, but at the same time raised the issue whether they really yield to more return on investment (ROI) than other important areas of an information security practice. A common decision is to reduce the budget from these areas during a period of budget crisis. At the same time, an evaluation that characterizes a security training program as successful does not necessarily correlate with actual on-the-job security behavior. The question raised is how security awareness and training efforts are aligned with business drivers and how the really needed security knowledge is imparted to appropriate personnel.

Siponen has published numerous articles on the area of security awareness and training as well as approaches to motivational aspects relating to human errors. He argues that IS security awareness programs should be grounded upon behavioral theories and provide users with answers as why following security guidelines is necessary (Siponen, 2000). The aim of such a program should be to achieve a situation where users' internalize and follow IS security policies. In this respect, Siponen presents a framework for persuasive approaches based on morals and ethics, well-being, a feeling of security, rationality, logic and emotions. The matters addressed are end user-related and organizational related. Also the human nature in enhancing IS security is stressed as well as the necessity of employees' commitment to IS security. Furthermore, he presents a "persuasion framework" to be used in security education (Siponen, 2000). The study recognizes the human component in IS security and has a social perspective.

However, punishment is proposed in order to achieve users' compliance with IS security policies. At another study, the importance of information security awareness as a result of the continuing use of IT and computerization is stressed (Siponen, 2001). Thus, other dimensions are needed in addition to organizational ones. The general public dimension has as main objective to increase public awareness of relevant security issues, the socio-political dimension involves increasing people's information security awareness with respect to the socio-political nature of IT, the computer ethical dimension includes moral thinking in terms of IT usage and the institutional education dimension refers to a society-driven process of education that is aimed at making individuals proper members of society.

Siponen and Kajava (1998), focus their study on the motivational aspects relating to human errors, with particular attention paid to the actual form and content of an awareness program when building any approach. The authors examine motivation and attitude, how people respond to awareness and the different methods used to increase awareness. Common to all approaches that affect the behavior of people (logic, emotions, morals and ethics, feeling of security, etc.) is the fact that they should satisfy the requirement of intrinsic motivation[4], explaining why they should follow security guidelines. Techniques from the field of social psychology (although previously have been largely ignored), are borrowed in order to improve the effectiveness of awareness programs. Thomson and von Solms, in their effort to highlight the reasons why an information security awareness program should enjoy more attention in all organizations, investigate

[4] Intrinsic motivation is when people are motivated by internal factors, as opposed to the external drivers of extrinsic motivation. Intrinsic motivation drives people to do things just for the fun of it, or because they believe it is a good or right thing to do. For example, most people's hobbies are intrinsically motivated.

the evolution of computing with specific reference to the new threats that technological advances have brought to systems (Thomson and von Solms, 1998).

Von Solms and von Solms (2004a), identify the ten most important aspects – called the 'deadly sins of information security'- which if not taken into account in an information security governance strategy, will cause the strategy to fail. Similar approaches have been identified by other scholars in the area. Wood recognizes that even the best technical information security solution is doomed to failure if the people involved do not support it (Wood, 1995), similarly Desman (2003) identifies ten directives (called commandments) for information security awareness training necessary in order to gain the cooperation of the staff who use the organization's information assets on a daily basis. Without any order of importance among others, information security awareness is realized as of core importance amongst users, and although such a 'sin' is apparent it is still committed by many companies. As a result of committing this sin, many information security related intentions will fail to materialize.

Spurling (1995), discusses promoting users' security awareness and commitment. He presents a case study in order to prove that commitment to security requires a process that fits into the culture of the organization. According to the case study, the company involved, based its IS security awareness efforts on three principles: (1) promoting the best "product" (in this case a high quality IS security plan), (2) involving people in order to get easier commitment, and (3) constantly reminding people about IS security issues. Presentations and training, involvement, work instructions, booklets, e-mail messages, newsletters and a problem management reporting system were used in the example organization

as means to emphasize the importance of IS security to employees. Spurling's approach presents IS security as having a social role. He emphasizes that users' commitment to IS security must also involve a process that fits in with the organizational culture.

A White House document (2003b), describes a program developed by the US government in order to promote a nationwide security awareness and training program with the objective to protect the nation's information technology infrastructure. The components of the program are: (1) awareness (addressed to home users, small businesses, large enterprises, institutions of higher education, the private sector and the state and local governments), (2) training (fostering adequate education and training, and increasing the efficiency of existing education programs), and (3) promote private sector support for well-coordinated widely recognized professional certifications. Furthermore, the document "White House: The National Strategy to Secure Cyberspace, Appendix: Actions and Recommendations (A/R) Summary.", presents several actions and recommendations that may be used in a national training and awareness program including awareness campaigns, securing networks and network components, training of IS security professionals, and certification programs (White House, 2003a). Both studies address societal and organizational issues of IS security in respect to private sectors, organizations, individuals and the United States as a whole. Similar studies by ENISA, give consideration to the role and responsibilities of home users, small businesses, large enterprises, institutions of higher education, the private sector, state and local governments (ENISA, 2010).

The following table (Table 3) summarizes the common factors identified across the different studies in respect to information security awareness. More

specifically the table recaps the different studies according to the following factors:

- Awareness Definition/Goals: whether the study includes or refers to a definition of security awareness along with its goals and objectives.
- Awareness needs/levels: whether the study identifies the different needs of security awareness in respect to different user levels.
- Awareness surveys/assessments: whether the study refers or conducts specific surveys on the level of security awareness concerning specific user groups.
- Models, tools and/or areas of learning: whether the study proposed specific tools for raising security awareness and/or the areas of learning that should be involved.
- Awareness approaches/steps: whether the study proposes specific approaches or steps that could be followed in order to achieve an appropriate level of awareness.
- IS Security Perspective: whether information security is perceived from a social, technical or sociotechnical perspective.

Author	Awareness Definition/Goals	Awareness Needs/Levels	Awareness Surveys/Assessments	Models, tools. areas for Learning	Awareness Approaches/Steps	IS Security Perspective
Anttila, Savola, Kajava et al (2007)		x		x		Social
ENISA (2006, 2010)	x	x	x	x	x	Social
Cox, Connolly and Curral (2001)		x			x	Socio-technical
Denning (2006)	x	x			x	Socio-technical
Desman (2003)					x	Socio-technical
Dodge, Carver and Ferguson (2007)		x	x	x		Social
Forcht, Pierson and Bauman (1988)		x		x		Social
Furnell, Gennatou and Dowland (2002)		x		x		Socio-technical
Hansche (2001)	x	x		x	x	Socio-technical
Hudson (2006)		x		x		Social
ISO (2013)		x	x	x		Socio-technical
Kruger and Kearney (2006)			x	x		Social
Mellor and Noyes (2006)		x	x	x	x	Social
Peltier (2002)	x	x	x	x	x	Social

Author	Awareness Definition/Goals	Awareness Needs/Levels	Awareness Surveys/Assessments	Models, tools. areas for Learning	Awareness Approaches/Steps	IS Security Perspective
NIST SP 800-12 (1995)	x	x			x	Socio-technical
NIST SP 800-16 (1998)	x	x	x	x	x	Social
NIST SP 800-50 (2003)	x	x	x	x	x	Social
Siponen (2000)	x	x		x		Social
Siponen (2001)	x	x		x		Social
Siponen and Kajava (1998)	x			x		Social
Thomson and von Solms (1998)	x	x	x	x		Social
Von Solms and von Solms (2004)		x			x	Social
Spurling (1995)				x	x	Social
Wood (1995)				x	x	Socio-technical
The White House (2003)	x	x		x	x	Socio-technical

Table 3: Common factors identified across the different studies in respect to information security awareness

In addition to the above mentioned studies, there are numerous websites that can be identified as valuable resources towards protecting information assets and raising the information security awareness level. Some representative websites are described below.

The SANS Institute website (SANS, 2014) provides a dedicated section called “Securing the Human” in recognition of the need for training on awareness and compliance for non-technical users, if security is to be achieved across an entire organization. The objective of the site is to provide with training and testing tools in order to ensure that security compliance requirements are met and at the same time a change in human behavior is achieved. A wealth of resources are available in various formats (e.g. training videos, awareness posters, screensavers, etc.) and for different types of audiences like end users, developers, engineers, healthcare professionals and people working at utility organizations. In the case of end users, there is foundation training that can be addressed to organizational staff as well as employees and contractors. Training is divided into approximately 43 different modules averaging 3 minutes in length with availability in 28 languages, plus necessary support materials for each module. Area coverage is broad and includes the most common topics like social engineering, email and messaging, social networks, data security, use of WiFi, use of passwords, etc. The selection of training modules is based on SANS’s “critical security controls”, which represent an effort to prioritize a list of the controls that would have the greatest impact in improving risk posture against real-world threats.

Figure 5: SANS's Securing the Human, end user security awareness training topics.

All these awareness resources are offered for a fee and are generally addressed to corporations that need to prepare and distribute awareness training materials to their employees with minimal effort. At the same time, from the way the approach is presented at their site, it seems that a structured learning framework is not followed. Topics are presented without any order of preference and existing participant knowledge does not appear to be taken into consideration. Although the computer-based training approach will allow participants to take training at their own pace from any location, the passive presentation of each topic using 3-minute videos and accompanying them with support materials does not guarantee neither coverage nor retention of topic knowledge.

The WiredSafety.org website (2014), contains security resources provided by volunteers among different age groups and different personalities (e.g. teachers, TV personalities, executives, writers, PhD's, etc.) and is generally addressed to teenagers and their parents. Most of these resources are provided free of charge and visitors are able to find resources on the following major areas:

- Help and support for victim of cybercrime and harassment.
- Advice, Training and Help for law enforcement worldwide on preventing, spotting and investigating cybercrimes.
- Education for children, parents, communities, law enforcement and educators.
- Information and awareness on all aspects of online safety, privacy, responsible use and security and
- Resources that can be downloaded or printed and used for offline presentations, community events and classroom activities.

Main subjects include topics like privacy, safety, security, child protection, etc. Most topics follow a very common presentation pattern that is text with very limited amount of graphics and no interactivity at all while others, although are considered serious issues in a modern society, cannot be directly related to information security awareness and efforts towards change in security behavior (e.g. sexting, distracted driving). Also some other subjects (e.g. cyberbullying) seem to follow a completely different structure and presentation approach which may confuse the reader. The site as a whole does not follow a structured approach making it very difficult for a visitor to either follow it or find easily information on related security topics.

The website named Stay Safe Online (NCSA, 2014), developed and maintained by NCSA, provides information on how to be safe when online and gives the opportunity to the public to take part in awareness initiatives such as the information security awareness month, celebrated every year during October. The website provides free resources to promote awareness like posters, templates, banners, letterheads and security videos.

Figure 6: StaySafeOnline.org resources related to the National Cyber Security Awareness Month.

From the way material is presented, topics are divided into specific broad categories:

- Information for those that want to “Stay Safe Online” with subareas about how to keep a machine clean, protect personal information, work with mobile devices, and information specifically addressed to parents.
- Information for people responsible to teach online safety categorized into different age groups (e.g. middle & high school, higher education).
- Information for people already in a working environment that want to find information on how to protect their businesses.

At each of the following areas, information is presented in the form of text-based material and in many case there are references to the stopthinkconnect website which also presents the same material in a similar way. Although some visual content is presented in the form of videos, still material is presented in an unstructured way without clear guidance on the steps or the sequence of topics that someone must follow in order to have an overall idea on how to get prepared so awareness for online safety issues is assured.

The Security Awareness Toolkit developed by Microsoft (Microsoft Corporation, 2014), provides a number of resources that can help users understand security and help security managers plan, develop and deliver their own awareness and training program, Tools included in the toolkit include a planning guide, templates, reference materials, a customizable awareness presentation and example awareness campaigns. Generally from the way these are prepared, they are addressed to security managers that want to have a starting point on how to build an awareness program for their company environment so additional work is needed so this approach is suitable and complete. There is no awareness content available so, it cannot be used as it is from an end user that seeks information on how to be prepared for online safety.

The Stop Think Connect website (stopthinkconnect.org, 2014a), represents a global effort aimed at increasing the understanding of cyber threats and empowering the public to be safer and more secure online. The site explains how average Internet users can protect themselves and their families against fraud, identity theft and other online threats. Information is presented in the form of various resources like:

- Tip sheets, which contain brief text-based information on how to be protected at various information security topics (e.g. mobile devices, privacy, games, social networking, etc.). Some of them are addressed to specific age groups (e.g. teens, parents, etc.).
- Posters ready to be used in order to raise awareness levels at specific topics.
- An online quiz that can be used to test the participant's knowledge on online safety, security and ethics. It contains 26 questions which are divided into two areas: (1) safety and security and (2) Privacy and being a good online citizen.
- Memes on specific security topics (e.g. email safety, WiFi usage, shopping online, etc.), in an effort to mimic an information security topic in a humorous and easily transmitted way.
- Videos on a wide range of information security issues.

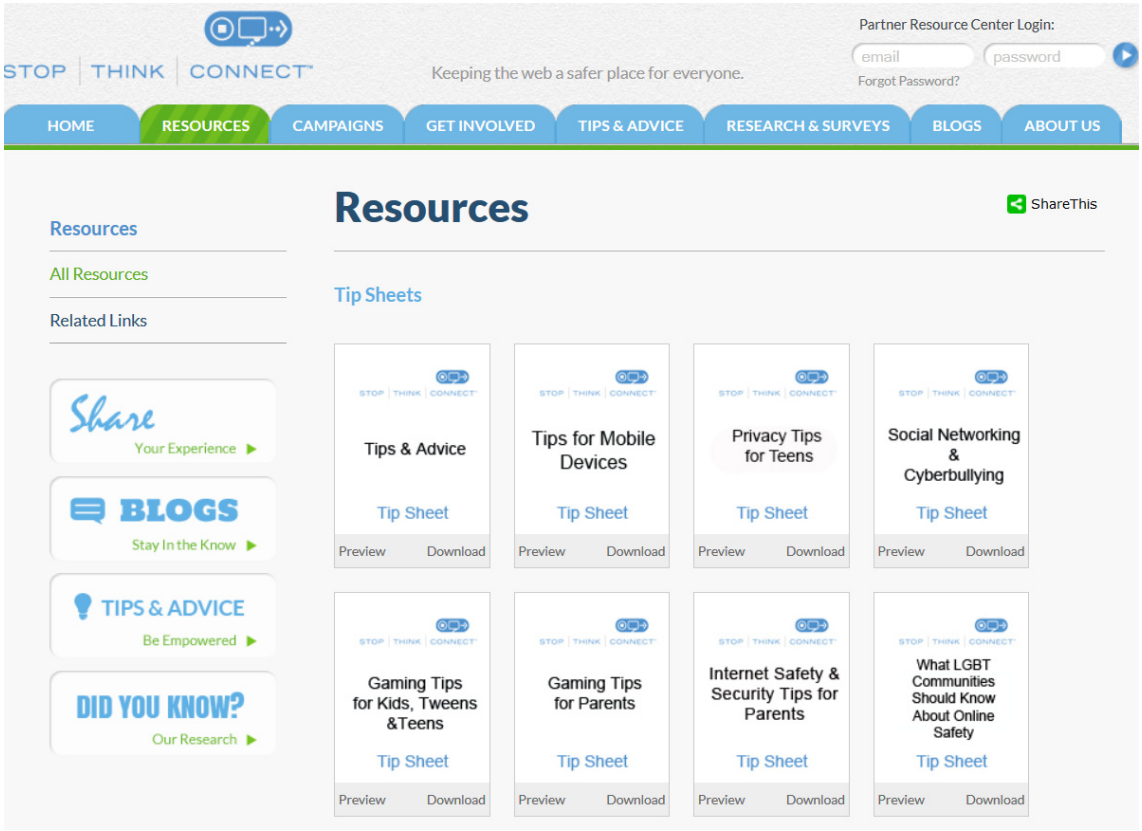


Figure 7: Resources page of the Stop Think Connect website.

The wealth of materials presented, makes stopthinkconnect.org one of the most valuable websites towards protecting information assets and raising the information security awareness level. The visitor can find almost everything in terms of information security issues. Still, like the websites considered previously, information is not presented in a structured way making the site aiming towards a user who is already security aware and wants to learn more on each subject or wants to use materials for an awareness campaign addressed to others. From the sites examined previously, it is the only one that introduces the concept of examining user knowledge through the use of a quiz. Still, the way the quiz is presented (use of PowerPoint) could be further enhanced to include additional interactive elements that could facilitate learning retention. On the other hand, if

this wealth of materials was structured, was integrated in a structured and guided package, it would easily achieve a more complete learning outcome.

The website of the Internet Corporation for Assigned Names and Numbers (ICANN, 2015), which has the responsibility for Internet Protocol address space allocation, has developed a security awareness section dedicated to prevention through threat awareness, preparedness, collaboration and information sharing. The materials available are addressed to all stakeholders in an effort to learn how to protect themselves, their families or their organizations against online threats. Most resources redirect to already known security related sites (e.g. Stay Safe Online, Stop Think Connect, SANS), sites concerning security of other countries or organizations (e.g. Australia, Malta, ENISA) and sites containing infographics, presentations and videos. Still, like the previously described websites, despite the wealth of resources, it does not follow a clear and guided approach which a novice individual can easily follow.

The above described websites are representative examples of efforts towards protecting information assets and raising the information security awareness level. Despite the wealth of information addressed to different population groups, most websites do not follow a clear and structured way on how someone can be informed and prepared about various information security topics. In fact, it can be concluded that the resources available can be an excellent basis for security professionals that are entitled to create awareness materials but can cause confusion to individuals that want to be informed and protected about potential threats. Also, most resources do not offer the ability to test someone's existing knowledge or the knowledge acquired by using the web resources. In many instances, such testing and knowledge verification is desirable before being faced

with the task of applying security precautions in a real world situation (Furnell et al., 2002). All of the above justify the need for a more structured learning approach that could combine all these valuable resources in a more efficient way. Such approach can make a valuable contribution and can provide a context in which users can learn about security concepts in a more active manner.

3.3.2 An Overview of existing information security culture approaches

Culture (a concept adopted from anthropology for organization management research) is a critical factor for organizations to continue living. Many corporate security articles state that security is primarily a management issue and not a technology issue. But without a significant change in organization security culture (which affects security practices and behavior), security implementation is doomed to failure. Since numerous surveys continue to argue that the lack of awareness of security issues are among the most significant causes to security incidents, the need to foster a culture in which users are aware of security issues and have the required knowledge to respond appropriately, is more that evident. An effective security culture represents the cornerstone for information security and can be achieved only with the appropriate attention to security awareness, education and staff training.

Schein (2004), an organizational pioneer, explains how to transform the abstract concept of culture into a practical tool that managers and students can use to understand the dynamics of organizations and change. Schein defines culture as:

> *"A pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way you perceive, think, and feel in relation to those problems".*

Schein divides organizational culture into three levels: (1) artifacts which are at the surface and refer to aspects (such as dress) which can be easily recognized, yet are hard to understand, (2) espoused values which lie beneath artifacts and represent conscious strategies, goals and philosophies, and (3) basic assumptions and values which are the core, or essence, of culture and are represented by the basic underlying assumptions and values, which are difficult to discern because they exist at a largely unconscious level. Yet they provide the key to understanding why things happen the way they do.

Ashenden (2005), argues that although there is an increased focus on the security processes because of the new and emerging regulatory environment, a lot of research is still to be done on the "people issues". A sociological perspective has to be taken on IT security risk assessment. Since most information security professionals come from a science or engineering background, they tend to see security rather as a process than a change of culture. With organizations now maturing in how they see security, there is a need for it to get pushed away from the IT professionals and apprehended as part of a change management process.

Chang and Lin (2007), examine the influence of organization culture on the effectiveness of implementing information security management (ISM). Based on a literature review, a model of the relationship between organizational culture and ISM effectiveness were measured in order to investigate how various organizational culture traits influenced information security management principles. The study was conducted by administering questionnaires to

respondents in organizations with significant use of information systems. According to the study, the control oriented organizational culture traits, effectiveness and consistency, have strong effect on the ISM principles of confidentiality, integrity, availability and accountability. On the other hand, the flexibility oriented organizational culture traits, cooperativeness and innovativeness are not significantly associated with the ISM principles with one exception that cooperativeness is negatively related to confidentiality. Since the human dimension of information security cannot be totally solved by technical and management measures, a culture conducive to information security practice is extremely important to organizations. For understanding and improving the organization behavior with regard to information security, organizations must look into organizational culture and examine how it affects the effectiveness of implementing ISM.

Finch et al (2003), address the problem of achieving security within modern organizations. According to his survey, a company cannot simply rely on the security message to spread itself. Even where appropriate measures are in place, it is clear that the users do not fully understand security. This comes from the realization that although a security policy is present and (in some cases) users have to sign indicating their acceptance, which is considered an inadequate means of ensuring that it means something to them. Instead appropriate training should be in place in order to teach the organizational IS security policy to employees. In addition, training should emphasize employees' role in adhering to the policy. The issue of promoting security amongst end-users goes far beyond having simply a security policy. Ongoing reinforcement of the security issues should be given more attention.

Furnell and Clarke (2005), recognize the fundamental role of security awareness in order to establish a successful security culture within an organization and examines the applicability of techniques to employees at all levels. According to the study, security culture will only be achievable if the concept is supported by the top level of the organization. A generic security program addressed to everyone is not the answer, and employers need to determine the level of understanding of their employees in order for the desired security culture to be fulfilled. Although awareness will help end-users understand their part in the security culture, this is only part of the process. It is also necessary to ensure that people have the knowledge and capabilities to do what is expected of them. Security training supported by a wide range of initiatives (i.e. job training, training on the use of systems and applications, internal training programs, specialist training courses), can fill this gap. Concerning the knowledge and skills of individuals with key responsibilities, organizations seeking to recruit, are often faced with a confusing situation concerning what skills they should look for. Usually a wide range of skills is available such as (Furnell, 2004):

- Academic qualifications: obtained by attending educational programs at academic institutions leading to a general or more specialist security related degree.
- Professional certifications: may be broadly based, or more specifically focused around individual technologies and security roles (e.g. CISSP certification).
- Vendor specific: relate to an individual's proficiency with a specific vendor's range of products (e.g. Cisco certifications).

According to the study, it is important to understand the type of expertise that your business requires and ensure that security knowledge is regularly reinforced and updated.

Gaunt (2000), discusses practical approaches for creating a security culture in the healthcare environment. He argues that although awareness of policy and observance of a code of conduct is important, their existence do not guarantee acceptable behavior by staff which is identified as the most significant threat to the security of information. For this reason the behavior of employees plays a vital role in good IS security practice. Hence, all employees should be aware of, agree and observe the procedures established for preserving the security of information. Gaunt also argues that the demonstration of the commitment to security by key opinion formers is the most important influence. Finally, in order to achieve wide acceptance, user participation in the development of an organizational IS security policy is necessary.

May (2003), states the important reasons of a security business certification as a means to demonstrate to potential customers that extra care to safeguard information is taken. According to the study, standards and adoption of them are one of the best methods for companies to develop a proactive strategy for information security. By meeting the standard required principles, it can help to improve and measure existing processes and procedures, while strengthening a security-focused culture. Furthermore, creating a culture of awareness will often lead to a more productive work environment, which can only have positive implications on the business as a whole.

Ruighaver et al (2007), addresses the concept of information security culture and argues that the investigation of security culture should also have a management focus. According to the paper, it is a mistake to follow the belief that information security is mostly a technical problem but rather understand that it is a management problem and the security culture reflects how management handles it. A framework of eight dimensions of security culture is presented as follows:

1. The basis of truth and rationality (explains the degree to which employees believe something is real or not real and how truth is discovered).
2. The nature of time and time horizon (refers to whether an organization adopts long-term planning and goal setting or reacts on a short-time horizon).
3. Motivation (a fundamental management principle – how actually people in an organization “do” things).
4. Stability versus change/innovation/personal growth (stability and change are very closely linked to motivation. It applies to whether individuals/organizations are open to change or tend to be less innovating and risk-takers).
5. Orientation to work, task, co-workers (the concept whether we work in order to achieve productivity or we work in order to have a comfortable life and developing social relationships).
6. Isolation versus collaboration/cooperation (focuses whether employees can work, either alone, or do collaborative work).
7. Control, coordination and responsibility (deals with whether control is concentrated so rules and procedures are set by few in order to control the majority or shared so flexibility and autonomy of workers is present, with fewer rules and shared decision making).

8. Orientation and focus – internal and/or external (the relationship between and organization and its environment and whether an organization controls or is controlled by the environment).

Each dimension is discussed in terms of how they relate specifically to security culture based on a number of previously published case studies. Although specific aspects of a security culture such as attitudes, norms, shared expectations, etc. do not fit nicely within a single dimension of the framework (due to the complex concept of security culture), the described framework is considered an essential step in ensuring that we have a comprehensive view of how the different dimensions of an organization's security culture relate to that particular aspect we are interested in.

Von Solms and von Solms (2004b), argue that defining a series of policies does not ensure that all employees will necessarily obey them and that policies must manifest in some company culture in order to ensure appropriate behavior. In this paper, the process of integrating policies, education and culture is addressed and a suggested framework of how culture is synchronized with polices that lead to acceptable actions is presented. According to the framework, policies and procedures should be properly communicated to all parties, regularly refreshed, posted to noticeable places to be seen and become part of every individual. Only then there is a chance to properly influence the behavior of employees to such extend that might manifest in a company culture. At the same time, a continuous information security awareness program should be in place to ensure initial education and also regular updates and reminders.

Stahl (2006), identifies the importance of peoples' behavior in an effective information security program and recognizes the gap between policies and the

behavior of people. It is the role of the culture to close this gap. According to his paper, the behavior of people depends on what they know, how they feel, and what their instincts tell them about, which leads to the fact that today's organizations are dynamic entities where different types of cultures coexist. The only way to transfer to the larger organization the correct way to perceive, think and feel in relation to information security problems, is to embed the information security subculture into the culture of the organization. This is a challenge that the CISO is facing today, and recent work in the area of behavioral sciences has discover six specific persuasion triggers that the CISO may use in his effort to persuade people (Cialdini, 2001). These triggers are:

1. Liking: people respond positively to people they like or to people who they perceive like them.
2. Reciprocity: people feel obliged to give to people who have given to them.
3. Social proof: people tend to follow what other people, similar to them, are doing.
4. Consistency: people fulfill written, public, and voluntary commitments.
5. Authority: people tend to rely on those with superior knowledge and expertise for guidance.
6. Scarcity: people value what is scarce and difficult to be replaced (i.e. an information security breach can result in lower revenues and revenues may be translated into fewer jobs).

These triggers if taken together open up the spaces in which information security learning can take place.

Von Solms and Thomson (2005), examine the relationships that exist between the fields of corporate governance, information security and corporate culture and highlight the role that senior management should play in cultivating and information security culture. In their paper the four pillars of corporate governance are identified (accountability, responsibility, fairness and transparency) and through these the board of directors is both accountable and responsible to their organization. One of the challenges that corporate governance and information security are facing, is to convince senior management that security should be treated as an investment rather than as an overhead. Furthermore, corporate culture is recognized as an important element in the actions of employees in an organization and its levels are presented according to the study of Schein. The relationship that should exist between information security and corporate governance is highlighted by the fact that senior management (who is accountable for the organization's success), is responsible for the protection of information (the organization's most valuable asset). The relationship that should exist between information security and corporate culture is highlighted by the fact that corporate culture should be used to influence the behavior of employees towards information security in a positive way. The relationship between corporate governance and corporate culture is highlighted by the fact that senior management should make an attempt to shape the corporate culture into one that will help in the achievement of the organization's goals. Finally, the relationship between the three levels of information security, corporate governance and corporate culture is recapitulated in the introduced term of "information security obedience". Information security obedience implies that a policy should be implemented in an organization in such a way that it affects the behavior of users and facilitates behavioral changes towards security practices.

In other words, staff actually understand and accept security as a second nature behavior in daily activities. The term binds all three levels by recognizing the fact that the actions the employees must comply are the ones that are required by senior management in terms of information security.

Thomson et al (2006), address that knowledge creation is necessary in order for employees to become more knowledgeable and more committed to the protection of information. This is possible through the integration of Nonaka's "Modes of Knowledge Creation" and the stages of the "Conscious Competence Learning Model" into the Model for Information Security Share Tacit Espoused Values (MISSTEV). Through this MISSTEV model, employees should be informed about the information security vision of senior management and their roles and responsibilities as part of this vision. Further to that, by following the MISSTEV model, employees become aware of and trained, of the skills necessary to protect an information asset, and these skills should become part of the everyday job practices of employees. By following the MISSTEV model, corporate information security obedience is becoming evident in an organization and the vision of top level management concerning information security is realized.

The following table (Table 4) summarizes the common factors identified across the different studies in respect to information security culture. More specifically the table recaps the different studies according to the following factors:

- Culture Definition/Goals: whether the study includes or refers to a definition of security culture along with its goals and objectives.

- Principles/Categories: whether the study refers to principles or different categories associates with either security culture or culture establishment in general.
- Framework: whether a framework is proposed for culture establishment.
- Culture levels: reference to the different levels of culture.
- Culture change methods: methods examined that can lead to an effective cultural change.
- Culture assessment: methods that can be used to assess the resulting cultural change.

Author	Culture Definition/ Goals	Principles/ Categories	Framework	Culture Levels	Cultural change methods	Culture Assessment
Schein (2004)	x	x		x	x	
Ashenden (2005)					x	
Chang and Lin (2007)		x	x	x		x
Finch, Furnell and Dowland (2003)					x	x
Furnell and Clarke (2005)	x	x	x			x
Gaunt (2000)	x				x	
May (2003)			x		x	x
Ruighaver, Maynard and Chang (2007)	x	x	x	x		
Von Solms and von Solms (2004)			x	x	x	
Stahl (2006)	x			x	x	
Thomson and von Solms (2005)	x	x		x	x	
Thomson, Von Solms and Louw (2006)	x		x	x	x	

Table 4: Common factors identified across the different studies in respect to information security culture

3.3.3 Literature review conclusions and further research objective

From the study of numerous literature, the importance of information security awareness and training in order to secure critical organizational or personal information resources, is clear and beyond any doubt. Security awareness is aimed at improving human security behavior. If human behavior is improved security awareness is also improved. Developing and implementing an effective security awareness program is the first step on providing computer and information security, and is considered a critical success factor. At the same time, information security is presented with different viewpoints:

1. Social: when the focus is mainly on the human aspects of information security.
2. Technical: when the focus is mainly on the technical aspects of information security and,
3. Socio-technical: when the focus is rather balanced between the human and the technical aspects of information security.

Furthermore, many approaches indicate the different needs for security awareness based on different population categorization. Different levels require different knowledge. The most common level categorization include students, parents and educators, young professionals, small businesses, industry and the government, law enforcement and older citizens (stopthinkconnect.org, 2014b). Because information security is considered not a technical but rather a human issue, the user behavior to IS security is critical. People are considered one of the major points of vulnerability. Still they must be seen as an asset in order to ensure security. It is evident that good technical solutions must be in place for secure information systems but without taking into consideration the human

element, technical solutions will fail. So people must understand their role in respect to security. Awareness training may come in many different forms (i.e. training sessions, security exercises, videos, brochures, newsletters, booklets, practice with the help of an instructor), although, self-paced training through simulation and pre-defined scenarios may be proven highly effective. Many research publications and famous security websites described before, have identified different awareness approaches along with the steps that should be followed in order to achieve the required awareness level. Antilla et al (2007) identify the role that end user awareness plays to the society and the importance that that information security education becomes a fixed part of the educational programs and not just rely on the activity of a few observant educators. The distinct characteristics though that such an educational program should have remains to be seen. Desman (2003) presents information on how to reach the required audience in an effort to achieve a successful information security awareness training but his approach is limited to set a set of tips without going into greater detail on the actual process of putting it into action. But, despite the fact that a wealth of information and resources is provided, most resources describe the problem – need for information security awareness establishment through an appropriately designed education program – without actually putting in action such a program or establishing a prototype. Also many resources especially from publicly available websites, are either offered for a fee (e.g. SANS) or do not follow a structured approach or guidance, except the fact that information is classified by different population groups. That adds an additional level of burden and confusion to people that want to have more clear guidance on how to protect effectively their information assets and at the same time have a tool readily available to help them through a modular approach.

Employee cooperation and commitment to the information security function is also very important. Implementation of a security awareness program does not guarantee that the employee participants understand their role in the security function and act accordingly. Employee accountability increases the overall strength of the human factor in information security and is strongly correlated with raised awareness. Commitment to security requires a process that fits into the culture of the entire organization. At the same time, a structured approach needs to be followed in order for the awareness program add value to the organization and at the same time make a contribution to the field of information security.

Many scholars believe that IS security is relevant to people's motivation, societal and cultural aspects. At many instances, people's motivation towards security is not internalized. That is they do not follow security procedures because they are good and right but because a policy is enforced. This is because, unfortunately, positive security performance is rarely rewarded while security failures are often punished. This may result in a negative reinforcement. Some good examples of security motivators may include: (1) rewarding, (2) punishment, (3) protection of personal investment, (4) protection of employer's reputation (5) desire to excel among peers, etc. At this point, the discipline of social psychology has conducted research into the area of changing successfully the behavior and attitude of people and may help make any security awareness program effective.

Finally, a critical success factor of any security awareness program is to gain support not only from all levels of the organization but specifically from senior management. Numerous methods in order to help persuade senior management of the importance of sponsoring training are suggested. Although awareness goals are difficult to quantify and measure, some evidence on return of

investment due to security training and awareness must be present. Senior management must understand that security should be treated as an investment rather than as an overhead.

Security culture in general is considered one of the major building blocks of a security awareness program. Significant organizational culture change is a necessity for security implementation as it affects many security practices and behavior. A study of the existing organizational culture is considered necessary in order to provide a key understanding why things happen the way they do. Unfortunately, due to the fact that most information security professionals come from a science or engineering discipline, they tend to see security rather as a process than a change of culture. Since the human element of information security cannot be totally solved by technical and management measures, a culture contributing to information security practice is extremely important for the organization. A security message cannot automatically spread itself within a company unless ongoing reinforcement of security issues is given more attention.

The fundamental role of security awareness in order to establish a successful security culture is beyond doubt but it is only achievable if the concept is supported by top level management of the organization. The existence of awareness programs, policy documents and well document code of conduct does not guarantee acceptable behavior or obedience by staff. Policies, education and culture should be synchronized together in order to lead to acceptable actions. In today's business environment organizations are dynamic entities where different cultures coexist and it is usual to experience a gap between existing policies and the actual behavior of people. The management focus on security culture may help greatly in taking corrective action towards this situation.

Finally, strong relationships exist between the fields of corporate governance, information security and corporate culture. The relationship that should exist between information security and corporate culture is emphasized by the fact that corporate culture should be used to influence and change the behavior of employees towards information security in a positive way. Corporate governance and corporate culture are related by the fact that senior management should attempt to shape the corporate culture into one that will help the organization achieve its mission. The term “information security obedience” is used to imply that policy is implemented in the organization in such a way that affects the behavior of users and facilitates behavioral changes towards security practices.

Evidence has been presented up to now that users remain susceptible to information security threats, illustrating the need for more effective user training in order to raise the level of security awareness. The primary aim of (ICT) is making the lives of citizens more efficient through its provided services. In regard to that, all members of the society today are more interconnected than ever and at the same time Internet supports critical infrastructures of and plays a major role on how governments provide services to its citizens and how companies do business. So there are different levels of needs for security awareness for different levels of users (e.g. ordinary citizens, nosiness leaders, experts, etc.). Taking into account the challenges for security for organizations and the society at large it is essential to focus efforts towards an information security aware society (Anttila et al., 2007). Research will continue by examining the importance of embedding information security concepts as early as possible and definitely before people reach the workplace. At this stage the role that the academic sector has to play in establishing an appropriate level of security awareness will be examined. Further emphasis will be made on the importance of security

awareness in academia and how the lessons learnt there are applied in both the personal and professional lives of students.

3.4 Embedding information security in our society

The number of users using a computer at home is rapidly increasing. With more than one billion PCs in use worldwide in 2008 and an expectation to reach more than two billion units by 2015 (Gartner, 2014), this large number of individual home users represents a significant weak point in an effort to achieve an appropriate information security level. The importance of embedding information security in the society has been identified by many scholars and research bodies. Since many functions of our society are now dependent on information and communication technologies, citizens should be security aware to the necessary extend. Since end users are using ICT services both in their private life and as part of their employment commitments, end user security awareness is one of the most important issues in our society and everyone should have at least some basic literacy (Anttila et al., 2007).

ENISA (2010), recognizes that citizens (and businesses) extensively use ICT to carry out their day-to-day tasks and because of that the number of security breaches have increased. Although most of these breaches are IT related, there is still a considerable number of breaches that are caused because end-users are unaware of information security threats. The increasing number of staff related breaches across all industry sectors raise the need for security awareness in order to turn users into a first line of defense. Recognizing that nowadays information security is more aligned with the business than with IT, the document published features a step-by-step advice to help design, develop and implement an effective information security awareness program. Moreover, among the

typical groups where security awareness programs are usually addresses, namely employees, mid and high level managers, system administrators and third parties, the importance of the “home user” as a target awareness group is realized including many different categories like kids, teenagers, youths and adults.

The Council of European Professional Informatics Societies (CEPIS) realizes the importance of security awareness for citizens of all ages since they are used to share sensitive information for both personal and professional reasons but they often lack awareness of the important security risks that are derived from sharing such information (Council of European Professional Informatics Societies (CEPIS), 2014). These security breaches do not necessarily involve criminals or criminal organizations but may also involve questionable data collection efforts from companies and government organizations. For example service providers may be forced to collect user data by state and country laws or software companies developing operating systems or applications for their own benefit. Such actions make clear the need for an adequate level of ICT security for the protection of the European citizen’s data and interests.

The idea behind both these reports is that security awareness raising methods should not be focused only on the professional or organizational level but take into serious consideration the home user. Companies and organizations usually spend substantial resources in order to develop technology and processes that can help safeguard the security of their information assets. Employees at a work setting are in many cases exposed to security training or are protected by special security software and dedicated staff, but this does not apply in the case of home users. Home users are no motivated to take the necessary security precautions

in order to secure their own computer and the Internet in a home setting (Anderson and Agarwal, 2010). In fact, infected computers of home users can be the ideal ground for hackers attacking organizations (Li and Siponen, 2011). The concept of embedding and understanding information security concepts should be emphasized as early as possible and definitely before actually described at the workspace. In this effort people, organizations and bodies that are already involved in cyber security could help reaching out end users with information on how to protect themselves against risks. Several practices have been employed in this manner like the so called cyber security awareness month designed to educate and raise awareness not only to the public and private sector but also to all US citizens. Since the goal of such efforts is to achieve a cultural and behavioral change, home users should be aware on how technical precautions and policies available usually in a company setting can also be applied on an individual basis. Such messages and efforts can find a friendly ground on young users and their parents. Academia can play a significant role in these endeavors by engaging educational efforts as early as possible in order to achieve a stronger effect on users' Internet behavior (Council of European Professional Informatics Societies (CEPIS), 2014).

The research will continue by examining how security awareness initiatives are addressed during early stages of education and the role that educational institutions can play in addressing security.

3.4.1 Addressing security issues in early stages of education

The Internet plays a vital role in everyone's everyday lives. Ranging from young children to adult home users and professionals, it offers a wide range of opportunities as a learning, communication or even entertainment tool. In fact

research has shown that approximately 75% of the children in Europe are online engaging themselves in such opportunities (Livingstone and Haddon, 2009). The figure for the Internet use of parents is even higher (84%). Although studies including very young children are quite rare, it is safe to assume that internet use for children nowadays starts at an ever younger age. From a study carried out in Finland involving families with children aged 0-8 years, it was reported that there is a dramatic rise for 7-8 year olds in the use of digital games, the Internet and mobile phones. Similar studies from other countries reports that the most common online activity for 9-16 year olds is (Ólafsson et al., 2013):

- Using the Internet for school work even without being told to do so by teachers. Google and Wikipedia dominate most of the sites accessed and pupils usually copy from the Internet and use a variety of methods to cover up their plagiarism.
- Playing games,
- Watch video clips (usually through YouTube),
- Social networks and
- Instant messaging as a communication tool with classmates and friends which often accompanies schoolwork.

At the same time, as exposure to online services brings a significant number of risks for adults, such risks are also encountered by young users with similar negative consequences. More specifically young users are exposed through internet to content that is inappropriate for their age. Such content is reached by children either by an active search by young users or by coincidence. Following the risks classification used by the EU Kids Online network (Hasebrink et al., 2008), the risks can be summarized as follows:

- Content risks: Involves what is found on the web. A study involving the 40 most popular websites in the UK for young users reported that less than one third of the sites popular for this age group are designed specifically for them. In fact age inappropriate content may include illegal content such as child pornography, gambling messages, hateful or violent content (Fielder et al., 2007). The same study revealed that 95% of the popular sites for children contain some form of commercial content which poses a risk for children since they do not possess yet the skills to assess the appropriateness of such content.
- Contact risks: Involves someone else making contact. Social networking sites have an increased popularity not only among adults but also among children as well. Through their provided services such as instant messaging and chat, children are potentially at a greater risk of receiving unwanted and questionable messages from strangers and cyber bullies. Specifically in the case of cyberbullying research has identified that it is not a passing "phase" but indeed is having a significant impact on the lives of children. In fact a survey conducted in a sample of approximately 10,000 young people aged 13-22 mainly from the UK, the US and Australia (Ditch the Label, 2013) identified that:
    - 7 out of 10 young people are victims of cyberbullying.
    - 37% of young people are experiencing cyberbullying on a highly frequent basis.
    - 20% of young people experience extreme cyberbullying on a daily basis.
    - The main sources of cyberbullying are social networks and mobile phones.

Further to that, the use of social networking sites and their associated services expose young people to the risk of putting personal information on the Internet. Two thirds of the sites most frequently visited by children in the UK ask for personal information (Fielder et al., 2007). Such personal information may not only involve the children itself but also ask for family personal information and children do not yet possess the necessary knowledge of the risk associated with disclosing such personal information

- Conduct risks: involves children contacting someone. As explained above such activity involves children bullying or harassing other children.

- Security risks: The risks associated with the use of the Internet also apply to young users in the way they apply to adults. This means that young users may also be exposed to a range of internet risks such as viruses, phishing, spam, spyware, etc.

From the above it is evident that internet risks are not any more associated with professional and home users or necessarily adults. In fact, more and more young users who are associated early with the Internet may be victims of threats. Although these threats are not similar as the ones that adults are exposed, still the result is the same. We have moved to an era where viruses do not just play a tune on the computer or display a harmless graphic but instead even the looking innocent online computer games can pose a significant threat. Adult users can benefit from a formal awareness program either at home or at the workplace. In the case of young users although this can be more complex or time consuming, it will pay dividends in the future since it will prepare a security aware workforce

from an early stage. It is necessary that security issues should be addressed from an early stage in order to change young people's current behaviors and highlight good security habits. That said building a security aware society should start very early and should be driven by an appropriately designed educational curriculum. Adopting safe computing practices from an early stage will change behavior and promote a good security practice. A security awareness program introduced in the early stages of education not only will make young users aware of the online risks they face but also will familiarize them with the countermeasures they can utilize to protect themselves.

3.4.2 Addressing security issues at a higher education level

The proliferation of Internet in our everyday lives and the risks associated with its use have made security something that everyone has to worry about. Moreover, security has become a business issue since all elements of critical infrastructures ranging from governments and telecommunications to typical businesses now have an IT backbone. In fact, understanding and acceptance of IT security issues is now regarded as an essential requirement for every modern business (Finch et al., 2003). The availability of technical security measures to prevent data breaches can be proven inefficient if the irreplaceable human element is not taken into serious consideration. For that reason, many businesses and organizations have established security awareness and training programs for their employees. While security awareness efforts at the industry level are advancing, only few awareness programs direct their focus to higher education recipients (Chun-I Lin, 2009). The problem is focused on the availability of security awareness programs before employees enter the workforce. It is promising that there is a growing number of businesses that have established security awareness programs for their staff, but in order to achieve the main goals of information security, educating

the future workforce well in advance is considered a top priority. Institutions of higher education can play an important role on that.

The academic sector has a critical role to play in leading the effort for a security aware society. As one of the sectors that commonly address information security awareness, it consists of academic institutions with primary goal to provide learners with the necessary skills and knowledge for future occupations. Such occupations may include information security as a primary or secondary focus and it is the role of the academic institutions to ensure that learners are aware of information security issues that are relevant to their field of study. It is important that the growing need for information security aware professionals is appropriately addressed by academic institutions (Bishop, 2000; Streff and Zhou, 2006).

A few researchers and organizations have understood the importance of creating a security aware workforce by introducing security awareness topics to higher education recipients. One of these initiatives involve the establishment of the Higher Education Information Security Council (HEISC) by EDUCAUSE and Internet2 in an effort to improve information security, data protection and privacy programs across the higher education sector (Educause, 2014). In order to pursue projects and security initiatives in higher education, the council has established several working groups and committees with one of them being responsible for awareness and training. The objective of this group is to implement and make public methods by which awareness of security issues are raised among university and college communities.

Institutions of higher educations are responsible not only for preparing a workforce with the appropriate knowledge for today's demanding business environment but also have the responsibility to equip this workforce with the necessary skills to protect the valuable information assets of such businesses. For that reason, information security should be incorporated in the curricula of the institutions of higher education in an effort to raise security awareness of citizens and influence their security behavior. Unfortunately, although efforts are available through institutions of higher education, research indicates that there is still an ongoing need for information security courses in the academic sector (McGettrick, 2013). In fact there are numerous recommendations for near-term and short-term curricular guidance in cybersecurity for colleges and universities. It is important to incorporate information security at all levels of the curriculum in institutions of higher education. Indeed, incorporating security topics is not just seen as an area of academic study but as a public good in need of a large and expert workforce. For that reason everyone, and in particular all students should have some form of cybersecurity education.

More specifically, a workshop comprised by cyber security experts in government, industry and academia gathered in Atlanta in February 2013 made the following recommendations in respect to cybersecurity curriculums for colleges and universities:

- In the case of undergraduate computing majors and related programs, each student should be required to take at least one technical course in a security related area. Such courses should be taught by faculty with an appropriate comfort level in teaching security topics. Also institutions should enhance such programs by introducing industry credentials or

certificates in security related topics in order to equip their graduates with an extra competitive advantage with employees.

- At all levels of undergraduate curriculum there is a need for understanding and practicing cybersecurity in a human context. In this view, institutions of higher education should make every effort in raising security awareness of citizens through their curriculum.
- Information security curricula should include both technical and non-technical issues. It is widely recognized as technical as well as non-technical subject and definitely not strictly a computing discipline (Martins and Eloff, 2002; Bishop and Frincke, 2005; McGettrick, 2013). However, it is common that technical information security issues overshadow the non-technical issues.
- Information security should be treated as a multidisciplinary topic which is relevant not only to computing and information system disciplines but also to a variety of other study fields. There are many disciplines like law, medicine, international studies and business that have related cybersecurity issues that should be part of their curriculum. In fact, as Davidson suggests, among the graduates of liberal arts majors, there are many who are likely go into politics and deal with legislation so it is imperative for those people to understand what they are legislating about (Davidson, 2005).

In the same manner, the UK government recognized the need for a workforce with the necessary cybersecurity skills (UK Department for Business Innovation and Skills (BIS), 2014). This is a challenging objective not only for the UK but also globally since recent reports identified that the global demand for people with cyber security skills is expected to grow at about 13.2% each year till 2017 (Frost

& Sullivan, 2013). In fact the presence of highly-skilled cyber specialists and cyber-aware professionals will help countries ensure adequate responses to the growing cyber threats.

Towards this effort initiatives have taken place in order to increase cyber security skills at all levels of education and amongst the cyber security workforce both in the public and private sector. More specifically the following activities are suggested:

- Develop the workforce of the future by inspiring young people to pursue STEM and cyber security related careers.
- Develop the workforce of today for people in mid-career by developing cyber security pathways.
- Increase cyber security research.
- In order to meet the growing demands for competent cyber security professionals, develop a cyber-security profession through standards, certification and training and
- Influence associated professions and the wider workforce since appropriate cyber security knowledge is part of the daily activities also for non-cyber security professionals.

From the above, it is evident that information security issues should be addressed at the level of higher education in an effort to prepare a security aware workforce. In the following chapters, the research will continue by examining the state of information security awareness in an academic setting. More specifically the research will examine how/if the level of security awareness among students, changes as they progress in their academic life till they reach graduation and become ready to enter the workforce.

3.5 Chapter Summary

In today's environment, the use of technology is essential for businesses in order to carry out their daily tasks. It helps businesses make strategic decisions by processing data and transforming it into information. This information is a vital component for every organization and needs to be protected in a proper way. The purpose of this chapter was to examine the importance of information security awareness focusing also on its interdisciplinary nature. It was identified that security awareness is an essential proactive measure that has to do with making users of technology aware of how to protect personal and organizational information systems by applying security practices. The decentralization of information sharing has increased the number of people that are accessing and handling critical information. Since these people are not necessarily employees of the IT department but still handle critical data, the protection of vital information has an interdisciplinary nature.

The chapter examined the existing literature, in order to determine the current state of the art in terms of efforts towards fostering security awareness and culture. This literature determined that developing and implementing an effective security awareness program, is the first step on providing computer and information security and is considered a critical success factor.

Further to that emphasis was drawn on the concept of embedding information security concepts in the society and definitely as early as possible. Security awareness raising methods should not be focused only on the professional or organizational level but take into serious consideration the home user. Moreover, home users should be motivated to take the necessary security precautions in order to secure their own computer and the Internet in a home setting. Also

security issues should be addressed in early stages of education. The fact that a large number of children are online using the Internet as a learning, communication or even an entertainment tool supports this approach. Finally the role of the academic education in leading the effort for a security aware society was examined.

The next chapter continues by examining the potential of raising security awareness within the existing education systems. As a first step towards this goal, the current level of security awareness is investigated by using sample data from a university environment in order to examine the state of information security awareness in the academic sector.

Chapter IV – Measuring Information Security Awareness

4.1 Introduction

One of the major challenges of managing an information system and its resources is to provide appropriate measures to protect these systems. Information security has become an established discipline as more and more businesses realize its value. Life has become more interconnected than ever as recent surveys indicate. There are almost more cell phones than people and the Internet expansion has facilitated connectivity at any part of the world at almost no cost. At the same time, technology is generating a global convergence and has played an important role in improving, connecting and saving human lives (Mahbubani, 2012).

The volume and nature of information security threats have evolved targeting mainly the weakest link, which is the end-user (Schneiner, 2000; Hinde, 2004; ENISA, 2010). It is understood that good security cannot be achieved by technical means alone. Online users, in order to protect themselves, must have a solid understanding of the required security measures (Talib et al., 2010).

The purpose of this chapter is to investigate the potential of raising security awareness within existing education systems and as a first step towards this goal, the level of security awareness amongst the online population will be investigated. For this reason sample data from a university environment is used in order to examine the state of information security awareness in the academic sector and investigate the awareness needs of students in order to (1) support them during their time of study, (2) prepare them for the workplace, and (3) protect them in their wider personal use of IT systems.

4.2 Research Rationale

There are several sectors where information security awareness has received increased attention, namely government, industry and academia (Bishop, 2000; Siponen, 2001; Yasinsac, 2002). The academic sector is one that should regularly address information security awareness. Research has shown that a significant percentage of children in Europe are online engaging themselves in the learning, communication and entertainment opportunities that Internet provides (Livingstone and Haddon, 2009). A similar study has shown that young users between 9 and 16 years old are using the Internet for school work even without being told to do so by teachers (Ólafsson et al., 2013). Such exposure although it facilitates learning, it brings also a significant number of risks for young users. Schools can be the centers that will initially address and educate young users on how to use the Internet in a safe way. In the case of higher education institutions, exposure to security awareness concepts can be beneficial for students. Since the objective of higher education is to provide students with the necessary skills and knowledge for future occupations, it is important that the growing need for information security aware professionals is also equally addressed (Bishop, 2000; Streff and Zhou, 2006).

Information security has become a business issue since all elements of critical infrastructures now have an IT backbone. In order to protect these critical infrastructures, many businesses have established technical security measures, employed IT security staff and established security awareness and training programs for their employees. Considering that academic institutions are responsible for preparing the future workforce, their role in information protection is also vital but has not received the required attention. While security awareness

efforts at the industry level are advancing, only few awareness programs direct their focus to higher education recipients (Chun-I Lin, 2009).

The use of information technology is an essential requirement for all university students, and for this reason the information security curriculum must also be designed to support the needs of students undertaking non-IT courses who will similarly need to learn how to protect the information assets and resources of their future occupations (Hentea et al., 2006). There are many non-computing disciplines that are closely related with the protection of information (Bishop and Frincke, 2005). Because many successful security intrusions are the result of either social engineering or user complacency, there is a need for students in non IT-related disciplines to become as security literate as possible. Therefore, it is important to investigate the potential of raising security awareness within the existing education systems. Because of its multidisciplinary nature, information security should be integrated with a variety of other study fields (e.g. the legal environment). At the same time, extra care should be taken to the design of awareness curriculum when it is built into different study fields so the needs of every particular field are properly suited (Gritzalis et al., 2005).

Information security curricula should include both technical and non-technical issues since it is widely recognized as technical as well as non-technical (von Solms and von Solms, 2004a). However, along with the feeling that information security is strictly a science or engineering discipline, there are many instances where technical information security issues overshadow the non-technical ones. Many non-technical security issues (e.g. security policy and procedures, ethical and legal issues) are identified as missing from the information security curricula (Bacon and Tikekar, 2003).

The rapid growth of information technology makes important for the academic sector to identify new trends and developments in information security and adapt the curricula appropriately. Because of the need to integrate security awareness into education, the first step towards this process is to investigate the level of awareness amongst the online population. This will ensure that learners are kept up to date with new developments and trends in information security.

4.3 Information Security Awareness in a University Environment

The primary purpose of this research is to identify ways of establishing an appropriate information security awareness level. An important first step towards this goal is considered the analysis of the existing awareness level among relevant user population. Experts in computer security agree that, computer security tends to be weaker at universities (Identity Theft 911, 2009; Whittaker, 2010). One of the most commonly identified problems as obtained by audit reports by The Chronicle of Higher Education, is that colleges are not doing enough to encourage students as well as other campus users to protect their campus accounts (Foster, 2004). Among other issues, passwords are not changed periodically, are too short, or are not always required in order to gain access to sensitive information. Audits of university security systems reveal a large number of weaknesses including a lack of student awareness of computer security and ethics. As such, it was considered that a relevant and achievable focus for the project would be to investigate the security awareness level of students, at different periods of their academic life. More specifically the objective was to investigate:

- The level of security awareness when they enter the university environment.
- The level of awareness when they are considered established university students and,
- The level of awareness when they have reached the stage before graduation and are ready to join the workforce.

For that reason two separate surveys were conducted in order to investigate not only the awareness levels and needs of students in order to support them during their time of study and their preparation towards entering the workforce but also whether this awareness level changes as they progress in their studies.

At this stage of research, using surveys was considered more suitable than other data collection methods (e.g. interviews, focus groups) mainly because:

- The data that needs to be collected is not already available and cannot be obtained using other data sources or collection methods (e.g. existing records using the university's student information system),
- Surveys provide an effective method of gathering data from a large population sample and are also perceived to require less of the participants' time.
- Surveys can provide statistically significant results through the analysis and cross tabulation from multiple answers (e.g. comparison of answers that come from similar questions presented with different wording approaches).
- Surveys can provide participants with a standardized stimulus, with little or no researcher bias thus providing a high degree of reliability.

The first survey was conducted using a sample size of one hundred and sixty (160) students who have registered for CS1070 – Introduction to Information Systems course at The American College of Greece. It is important to note here that this group of students is a representative sample of students just entering the university that would be used to assess how well pre-university education had prepared them in relation to information security. Related studies on the level of security awareness of high school students from other European countries (ENISA, 2013) have determined important risk factors such as:

- Minimum knowledge about the risks of online communication and online delinquency.
- Immature personal, social and moral competences concerning the use of the Internet.
- Absence of education on the safe and ethical use of the Internet in the high school curricula.

Concerning the current study and the group of students chosen, although the CS1070 course contained a chapter related to computer security, ethics and privacy, such material had not been covered yet so students had not been formally introduced to any information security education and related ideas as part of their higher education engagement. Course sections were selected from both the undergraduate divisions of the American College of Greece that are Deree College and Junior College. The College offers baccalaureate degrees in the liberal arts and in business administration. The main entrance requirements are sufficient level of English plus average or above average academic

performance at the high school level. The Junior College offers two year associate degrees with an option for students to transfer to Deree College after the end of their associate degree studies. Junior College accepts students with a lower level English language or lower high school GPA provided that they attend special preparation courses through a carefully designed advising system. The reason behind choosing this module is that the CS1070 – Introduction to Information Systems course is a general education requirement for all students and is co-taught for both Deree and Junior College students. Most students are required to register for this course during their first semester of studies irrespective of their chosen area of study, in order to get an understanding of IT concept at an early stage. The course is complemented by a lab and has the objective to teach students basic information systems concepts like computer hardware and software, data acquisition, storage and manipulation, data communications, the Internet and the Web, present and future trends in information technology and the social impact of IT.

The second survey came out of the results of the first survey and its objective was to examine if/how the level of security awareness of students change as they progress in their academic life. Taking into account that academic institutions are the starting point in producing professionals who are security literate, the focus has to be placed upon what can be achieved and the critical question that arises is whether the level of awareness of students changes as they progress to their studies. In other words the objective of the second survey is to examine whether academia plays a role in the effort to raise the awareness level of the online population.

It should be noted here that the hypothesis whether the security awareness level of students changes as they progress in their academic life could be proven by examining the course requirements at each curricular area (i.e. whether security issues are addressed as a formal part of their study). However, with the exception of students majoring in Information Technology and/or related subjects, it could be concluded in advance that since other areas have no security awareness courses in their curriculum, the awareness level of students will remain pretty stable or at least will not be directly determined by their educational experience. However, the essence behind the second survey was not to see the effect of something they had been taught, but rather to see whether they simply became naturally more mature in terms of security practices as a result of a few years of additional experience and their general college interactions. As mentioned before, our hypothesis might reasonably have been that such maturity does not cultivate, but the need for such hypothesis to be proven was still relevant in order to determine whether there is a need for a more structured approach in order to achieve an acceptable security awareness level.

In the case of the second survey, we have continuing students who have completed up to thirty credit hours, in other words they have completed their first year of studies and students with ninety or more credit hours completed, in other words students towards graduation.

4.4 Presentation of Results – Pre-university awareness level

A concise questionnaire of 28 questions (see Appendix I) was used consisting of three sections. The purpose of the first part was to collect demographic information from the student participants (e.g., gender, college year, academic discipline, age, and employment status). The second part was the main part of

the survey measuring the level of security awareness of students by examining opinions and habits like the use of Internet, level of security knowledge, password usage, methods used for protecting computer and electronic data, use of e-mail, awareness of the various threats to computer assets, etc. Most questions were multiple choice with some allowing the user to choose more than one answer. The last part of the questionnaire included true/false questions where students were asked to indicate their level of agreement with a specific information security issue/statement.

The results are presented and interpreted in the following four sections:

- Background Information.
- Use of IT and the Internet.
- Security Knowledge and Perceptions and Security.
- Practices and Behaviors.

4.4.1 Pre-University Survey, Background Information

Although this was not intentional, the participants of the first survey were almost equally distributed between males (46%) and females (54%).

The majority of survey respondents are students who have just entered the college (63%) with the second biggest category being students with at least one semester enrollment (28%). All other categories have non- significant values, and no senior students have actually participated. Therefore the survey results represent the level of security awareness at the start of higher education.

Almost one third of the survey participants are currently employed (31%). Since information security has become a business issue for all modern enterprises,

businesses today employ technical measures in order to prevent data breaches. At the same time because they understand the significance of the human element in information security, many of them have established security awareness and training programs for their employees. It would be interesting to measure at a later stage the awareness level of this group of students and examine whether their employment status has a significant contribution to their awareness level.

Students majoring in Business Administration represented the highest percentage of those that participated in the survey (36%) with the second largest category being students who have not declared their major yet (30%) (Figure 5). This is in complete accordance with the US National Center of Education Statistics which reports that among the bachelor's degrees conferred, the greatest numbers are in the fields of business (U.S. Department of Education, 2013). Also this follows the enrollment trend of students in the last ten years at the American College of Greece. In the case of undecided students, again the percentage follows the norm since it common for the American educational system a student not to declare a major upon entering the college. In fact most college students declare their major toward the end of their second year of college and most faculty members and department encourage them to explore their interests by taking courses not even offered at most high schools so they discover new fields of interest.

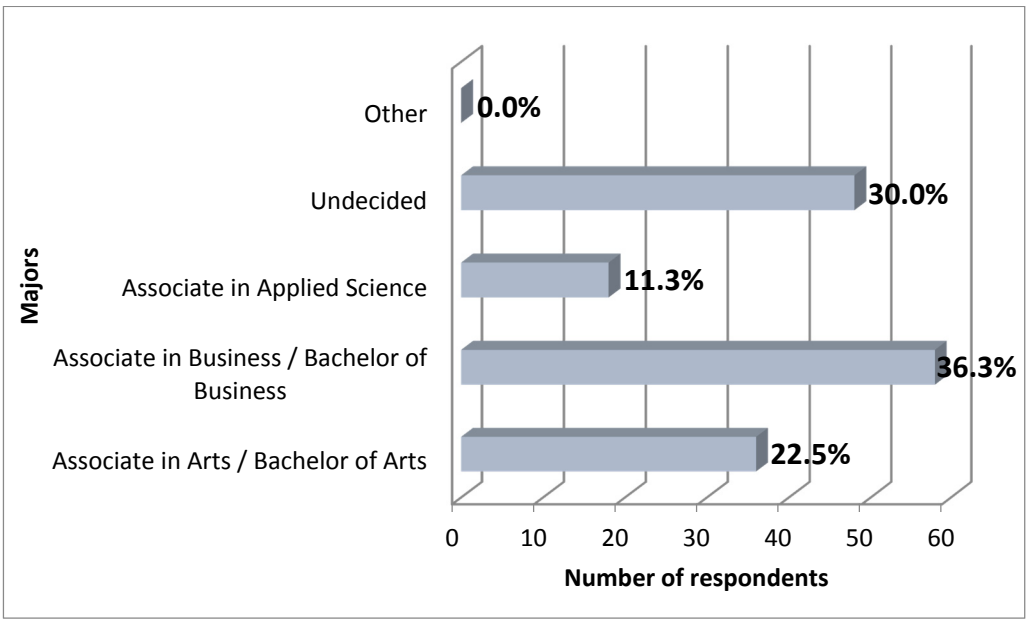


Figure 8: College year respondents

The last question from the background information section indicates that most survey participants (88%) are under 21 years old. This is an expected outcome taking into consideration that most students enter the college immediately after they finish normal high-school.

4.4.2 Pre-University Survey, Use of IT and the Internet

The following section presents the first survey findings related with the use of IT and the Internet. Concerning computer usage, the two most dominant answers are at home (96%) and at school (71%) (Figure 6). A significant portion of these groups have chosen both at home AND at school (72% of the students that use a computer at home, also use it at school). Significant lower numbers use a computer either at an Internet Café (33%) or at work (14%).

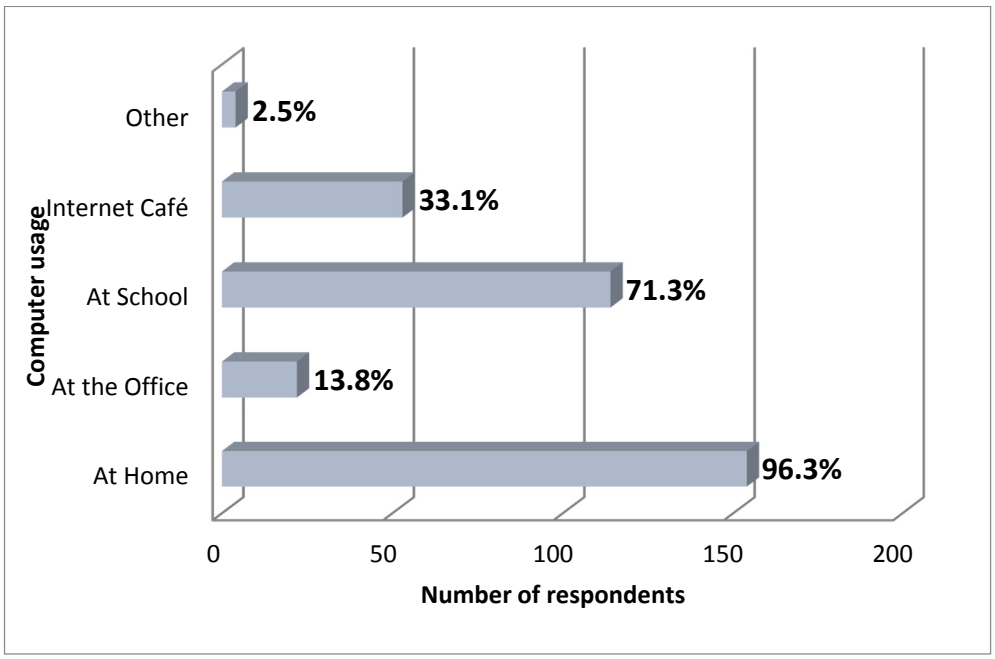


Figure 9: Respondents' computer usage

Most users access the Internet using a DSL broadband connection (84%). A significant portion of the respondents access the Internet using either the school or the company Internet connection (58%). At the same time, the users that access Internet both using a DSL line and a school/office connection are 59%. It is important to mention that 15% of the respondents access Internet using a mobile device (e.g., mobile phone) and a very small and insignificant percentage (13%) use a dial-up connection. In the case of respondents that access the Internet using a mobile device, the low reported figure is quite normal taking into consideration the time the survey was conducted (September 2008). Although during that time, mobile communication providers were offering Internet services through a mobile device, this was not offered as part of the normal contract plan but as an add-on feature mainly addressed to business and corporate users. At the same time the mobile technology developments and the use of smartphones was not that significant in order to make such an add-on service attractive to students.

Concerning Internet usage (Figure 10), 54% of the respondents spend one to three hours on line per day. A smaller percentage (but still significant) spend four to five hours per day (20%). Internet speed plays an important role on the time that users spend online every day. From the users that spend between one and three hours per day, 89% use a broadband connection. The same applies for the users that spend four to five hours online per day (almost 100% use DSL broadband).

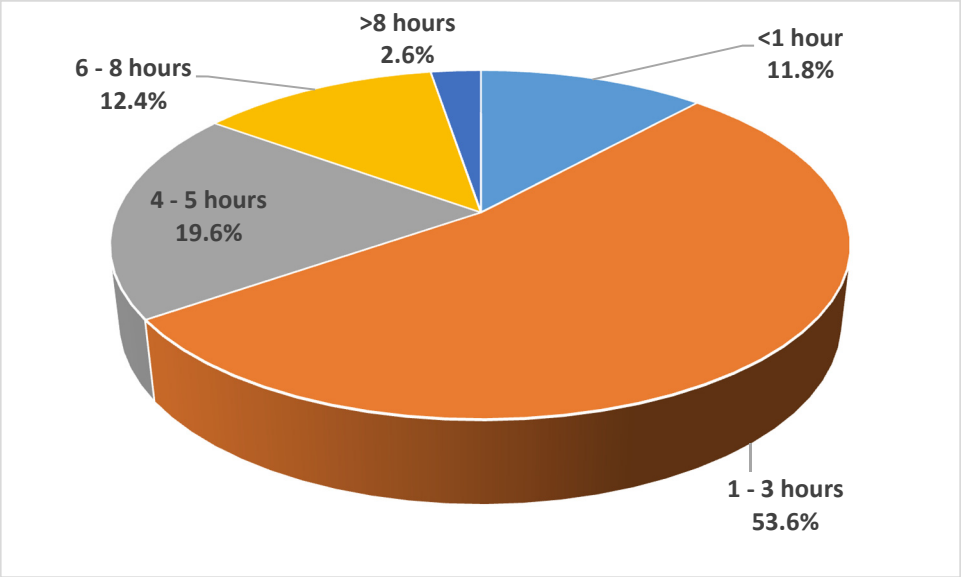


Figure 10: Time spent online per day

By comparing the survey findings with the European Union (EU) Internet usage, where at least half of the EU population consists of regular internet users (European Commission, 2009) we conclude that the sample is well above the EU average and that the sample population are the most intensive internet users.

To measure respondent's use of the Internet they were asked to choose three answers from a list of common Internet applications. The essence behind this question was for respondents to focus on what Internet applications they use most and for that reason were asked to record their three most common Internet

uses without any ranking or prioritization. Asking them to rank all choices in such a big list was considered inefficient since it may result in forcing users to rank usages that use very rarely or do not use at all. A significantly low number in a specific usage example does not necessarily mean low usage but rather non main usage.

Internet Usage	#	ALL	Employed	Unemployed
E-mail	110	69%	59%	73%
Educational purposes	62	39%	29%	43%
Chat rooms	31	19%	29%	15%
Games	49	31%	49%	23%
Web browsing (excluding social networking)	50	31%	37%	29%
Shopping	9	6%	8%	5%
Banking/Paying Bills	3	2%	2%	2%
Instant messaging	66	41%	27%	48%
Social Networking (e.g. MySpace, Facebook)	77	48%	39%	52%

Table 5: Internet usage

It can be seen from Table 5 above that the most popular use of Internet among students is e-mail (69%) with social networks (48%), instant messaging (41%) and education (39%) being the other most popular choices. It sound strange that web browsing is ranked fifth (31%) among the most popular choices. At the same time, and since we are referring to students, the number of people that use Internet for educational purposes (39%) may be considered low. This may be explained by the fact that the sample involved mostly incoming college students who are not yet familiar on how to use the Internet for educational purposes. It is likely though that this will change significantly as students' progress with their studies and register in courses that require them to do independent literature reviews and assignments. An additional distinction is made between employed

and unemployed students. The reason behind that is because business users usually have different Internet habits as compared with users not yet entered at the workforce. Such habits are usually derived from how companies and organizations are using the Internet for business purposes. Such distinction is also made at other questions in this survey in an effort to check whether employment affects the habits and behavior of respondents. In this question, the comparison between these two groups does not show a significant difference although some variances are observed in the case of games and instant messaging.

It is useful at this point to compare the answer to this question with the answers to relevant true/false questions presented later at the survey.

Although 31% of respondents reported that web browsing is one of their main Internet usages, at a later T/F question, (not surprisingly) almost all (92%) report that they have used the Internet in order to download music and programs from file-sharing programs or file repositories, which often requires web usage. This does not contradict at all with the user's perception on downloading music, videos, or programs without permission presented later on this report.

It should be also clarified here that the very low percentage of respondents that buy things online (6%), represents that this option is the least favorable internet usage among the options presented at this question. It does not necessarily mean that students do not at all buy things online which is clearly represented at a later question where half of the respondents report that they have been engaged in such activity (50%). The same case appears with the use of instant messaging programs (90%).

From the results presented above (how students use IT and the Internet, where they use their computer, the way they access Internet and for how long and the most common Internet usage applications), there is a clear need for safe and secure Internet usage.

4.4.3 Pre-University Survey, Security Knowledge and Perceptions

The next question is actually the first attempt that deals with respondent's security knowledge and perception (Figure 11). Approximately 64% of the respondents were concerned about the safety of their information assets (combined percentages of those who answered agree or strongly agree), 28% were neutral while the number of people who are least concerned is almost 9%.

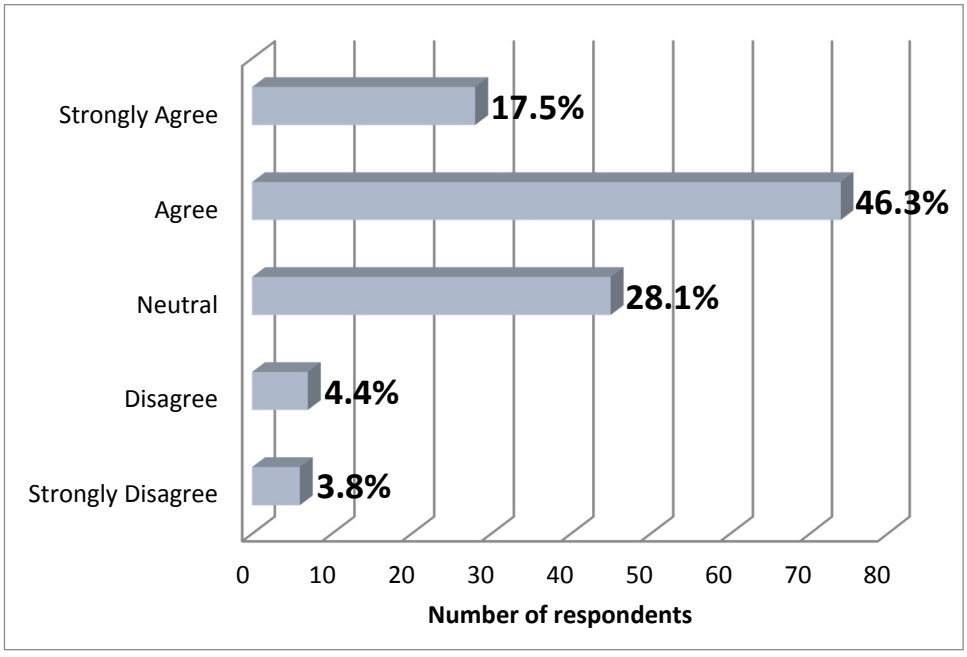


Figure 11: Responses to the statement 'I am concerned about the safety of my information assets'

The next question tried to identify whether the respondents felt that they possessed the necessary knowledge in order to protect their information technology assets. The question is rather subjective and does not ask the

respondent to justify their answer. The question tried to measure their feeling based on a subjective judgment of whether their knowledge of information security issues was enough to protect their technology resources. Approximately 66% of the respondents felt that they possessed the necessary knowledge to protect their information resources (combined percentages of those who answered agree or strongly agree). 8% did not feel comfortable with their information security knowledge.

The next question tried to measure the respondent's confidence in recognizing security incidents (Figure 12). Again this question was rather subjective and did not ask the respondent to justify their answer. 51% of the respondents felt that they would easily recognize a security incident. Another 33% were neutral. The figures do not significantly change if we isolate the employed students from the non-employed ones.

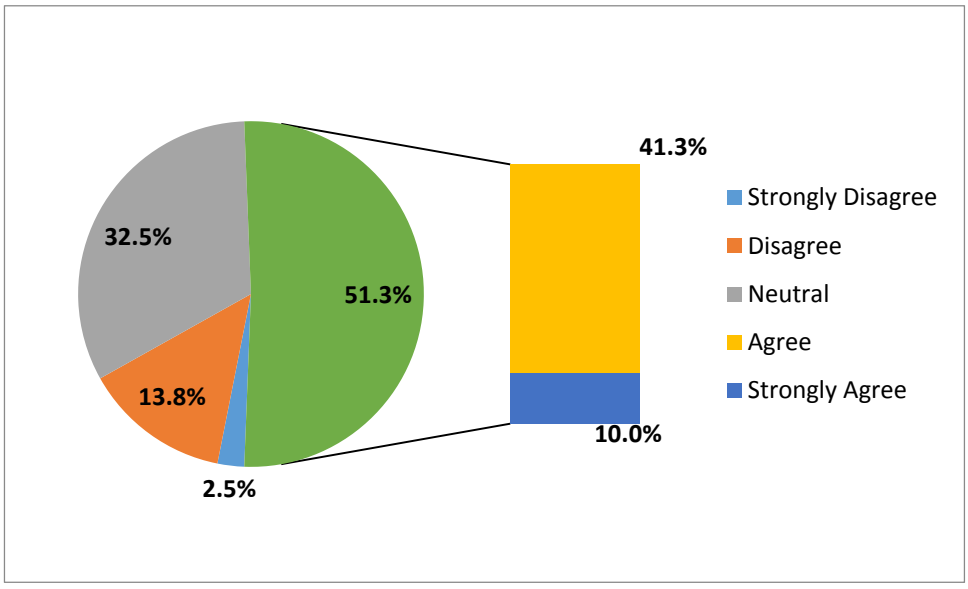


Figure 12: I am confident that I would recognize a security incident if a saw one

Up to this point the survey considered issues of information security like password selection and use, e-mail usage habits along with the subjective opinion of users

about their level of information security literacy. The next question presented the respondents with a list of information security terminology and asks them to indicate their level of familiarity. The list also contained an option that did not exist (whooping) in order to measure whether the respondents were providing considered responses. From Table 6 below, it is clear that most respondents were very familiar with traditional malware terms, like "virus" (80%), "trojan" (60%), "spyware" (54%), "spam" (54%), and "worm" (44%). However, it seems that other serious information security terms like "phishing", "social engineering" and "shoulder surfing" are not recognized by the survey respondents.

IS Terms	1 **Not at all Familiar**	2 **Least Familiar**	3 **Somewhat Familiar**	4 **Familiar**	5 **Very Familiar**	**Sum of 4 and 5**
Spyware	12.4%	17.6%	15.7%	22.9%	31.4%	54.2%
Phishing	61.4%	23.5%	7.2%	2.6%	5.2%	7.8%
Dumpster Diving	69.9%	19.6%	4.6%	4.6%	1.3%	5.9%
Shoulder Surfing	54.2%	19.6%	13.7%	9.2%	3.3%	12.4%
Whooping	60.1%	19.0%	8.5%	8.5%	3.9%	12.4%
Identity Theft	28.1%	13.7%	20.3%	15.0%	22.9%	37.9%
Spam	14.4%	11.8%	20.3%	16.3%	37.3%	53.6%
Trojan	20.3%	9.8%	9.8%	13.1%	47.1%	60.1%
Virus	5.2%	2.6%	12.4%	18.3%	61.4%	79.7%
Worm	24.8%	14.4%	16.3%	16.3%	28.1%	44.4%
Adware	29.4%	18.3%	17.0%	13.1%	22.2%	35.3%
Social Engineering	34.0%	20.9%	20.3%	20.3%	4.6%	24.8%
Content Filtering	28.8%	13.1%	24.8%	19.0%	14.4%	33.3%

Table 6: Perceived level of familiarity with specific information security terminology

As far as the imaginary term is concerned ("whooping") a small number of respondents (12%) claimed to be familiar (or very familiar) with the term. In order to identify how this group of respondents affects the results of the survey, their answers to main questions were reviewed separately. More specifically the

questions that were examined were the ones that deal with methods of protecting their data, perceived knowledge in identifying a security incident, password habits and habits concerning e-mail attachments. It was found that those students do not significantly affect the survey results and their opinion was therefore included in the survey findings.

The next question, asked respondents where they obtained their information security knowledge and how they protected their computer assets from potential dangers (Figure 13).

Respondents were allowed to choose more than one answer from a list of the most popular sources available for information protection. It is evident from the survey responses that participants are more confident in using informal and more "personal" sources of advice, such as friends, colleagues and college professors (73%). Other sources of information for protection of information assets included Internet news feeds (43%), newspapers and magazines (35%) and received e-mails (31%).

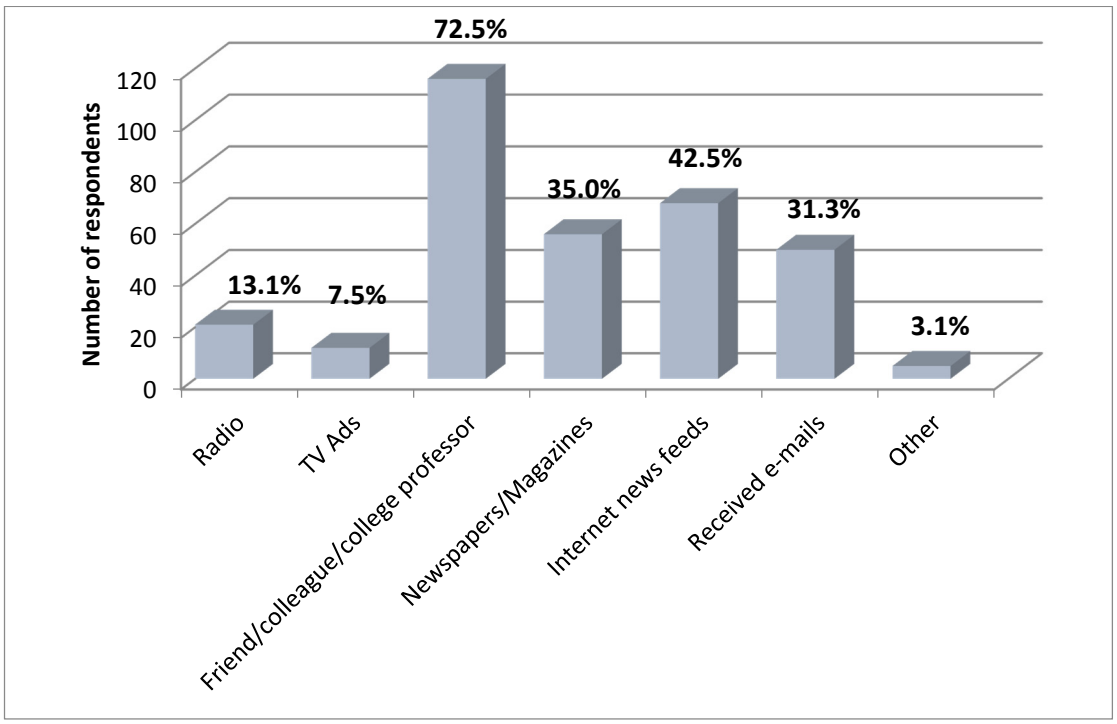


Figure 13: Sources of information for protection of computer assets

The last question concerning knowledge and perceptions asked the respondents to indicate their level of agreement with specific statements that concern information security threats from hacking/hackers (Table 7).

A high number of respondents believe that data encryption (45%) and the use of a firewall (37%) is not sufficient protection against hackers. Half of the respondents believe that:

(1) Hacking is not rare,
(2) A hacker's invasion is of considerable importance (63%) and
(3) The greatest threat to electronic information comes from hackers (54%).

IS Statement concerning hacking	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1-If my data is encrypted, it is safe from hackers	8.5%	36.6%	32.0%	19.0%	3.9%
2-If my computer is behind a firewall, it is safe from hackers	11.8%	25.5%	34.0%	26.8%	2.0%
3-Despite its popularity, hacking is very rare	19.6%	29.4%	17.6%	26.1%	7.2%
4-I have very little to lose if a hacker invades my computer	32.7%	30.1%	15.0%	15.7%	6.5%
5-The greatest threat to electronic information comes from hackers	7.2%	15.0%	24.2%	34.6%	19.0%

Table 7: Opinions concerning hacking

User's opinions and perceptions about hacking seem imbalanced. A significant number of respondents (almost half) that believe that hackers is the greatest threat to electronic communication, but seem to overestimate what hackers are capable of doing and whether this is strongly related to users' security behaviors and choices. For example choosing a weak password, dealing with email attachments in an insecure way or using social networks without any security precaution may open the door to a potential hacker but it is the users' poor choices that have resulted in this and not the hackers ability. Also in the case of using technology measures in order to protect data (like encryption) still a significant number of users believe that technology safety measures alone are sufficient for intrusion protection.

Finally using T/F questions, it appeared that the opinion of respondents concerning the importance of backups is equally balanced. Almost half of the students (53%) did not keep important information in more than one place. Also, 33% of the students believe that they will understand if a website is secure to give information but at the same time very few (less than 2%) could provide accurate answers about what constitutes a secure site.

4.4.4 Pre-University Survey, Security Practices and Behaviors

The last section of survey findings dealt with users' security practices and behaviors.

By presenting a list of common information security procedures, the next question tried to identify what type of protection was preferred by students in order to

protect their computer and electronic data (Figure 14). The participants were able to select more than one answer.

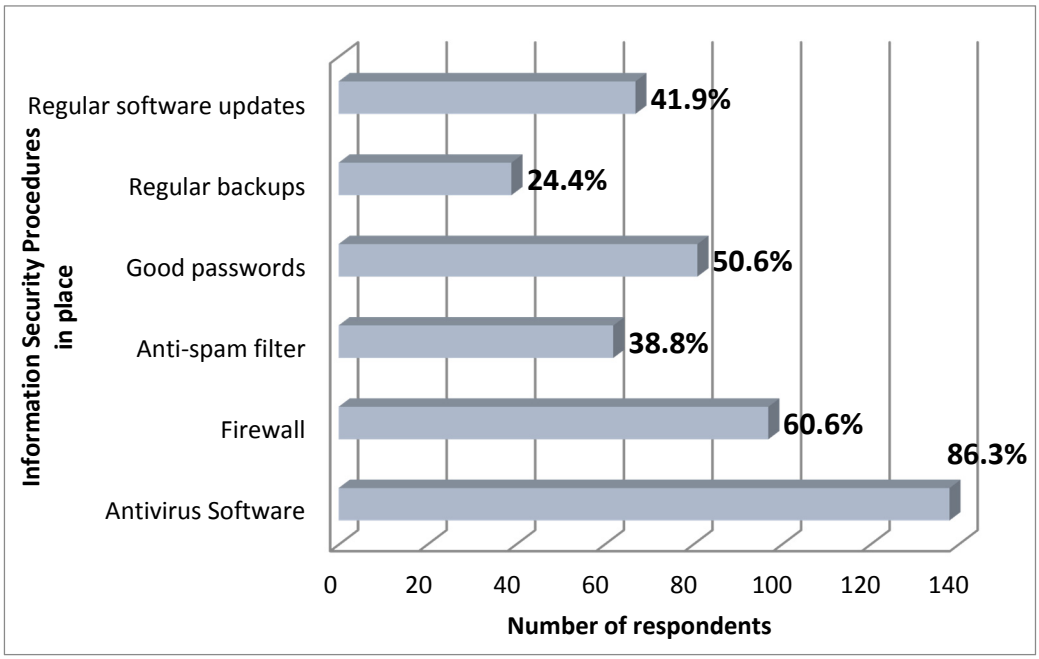


Figure 14: Do you have any of the following in place in order to protect your data and electronic data?

It is clear that antivirus software is considered the most popular protection mechanism used by students (87%). Second and third most popular choices were the use of a firewall (61%) and the use of good passwords (51). At the same time 65% of the students who chose antivirus as their means of protection also chose the use of a firewall as additional protection. Furthermore, 38% of the students who chose antivirus as their means of protection complemented it with the use of firewalls and implementation of good passwords. It seems from the respondent data that regular backups were not considered as a popular method of protection. Taking into account that more than one answers could be selected it is important to go one level deeper in the analysis of the options that users prefer in order to protect their data.

From the findings it seems that adherence to good practice is at best sporadic. Despite the fact that the options presented are of major importance in order to protect data, only 8 respondents have chosen all options. Among the total number of 154 students that chose to provide an answer to this question, those who selected between 3 and 5 of the total 6 options were very few in number (between 26 and 34).

Taking into consideration that the use of e-mail has been previously identified as the most popular Internet application, the next question tried to identify their security habits concerning e-mail attachments. Although one third of the respondents (31%) chose the "correct" answer (if the e-mail successfully passes the security checks of my computer), a significant number of students would always open the e-mail or will open it if it originated from an authority that they know (e.g., university, government), or if it originated from a person they knew (54% in total). This clearly indicates that a large number of students may be subject to attacks. On the other hand it is helpful at this point to compare the security habits concerning email attachments between employed and unemployed students.

From Table 8 below, it seems that students that are currently employed have a significantly higher level of security awareness concerning e-mail attachment behavior that those who are not.

Assume that you receive an e-mail with a file attached to it. In which case(s) would you open the file attachment?	**#**	**All**	**Emp**	**Unemployed**
If it originates from a person that I know	56	35.0%	19.1%	42.3%
If it originates from an authority (i.e. University) that I know	22	13.8%	8.5%	16.2%
If the e-mail successfully passes the security checks of my computer	49	30.6%	38.3%	27.9%
Always	9	5.6%	10.6%	3.6%
Never	19	11.9%	23.4%	7.2%
Other	5	3.1%	4.1%	2.7%

Table 8: E-mail attachments behavior

Password usage is strongly associated with information security precautions. It is widely accepted that good passwords represent the first line of defense against internal or external attacks. The next question tried to identify the password awareness needs of students by examining the cases under which they would reveal their passwords (Figure 15).

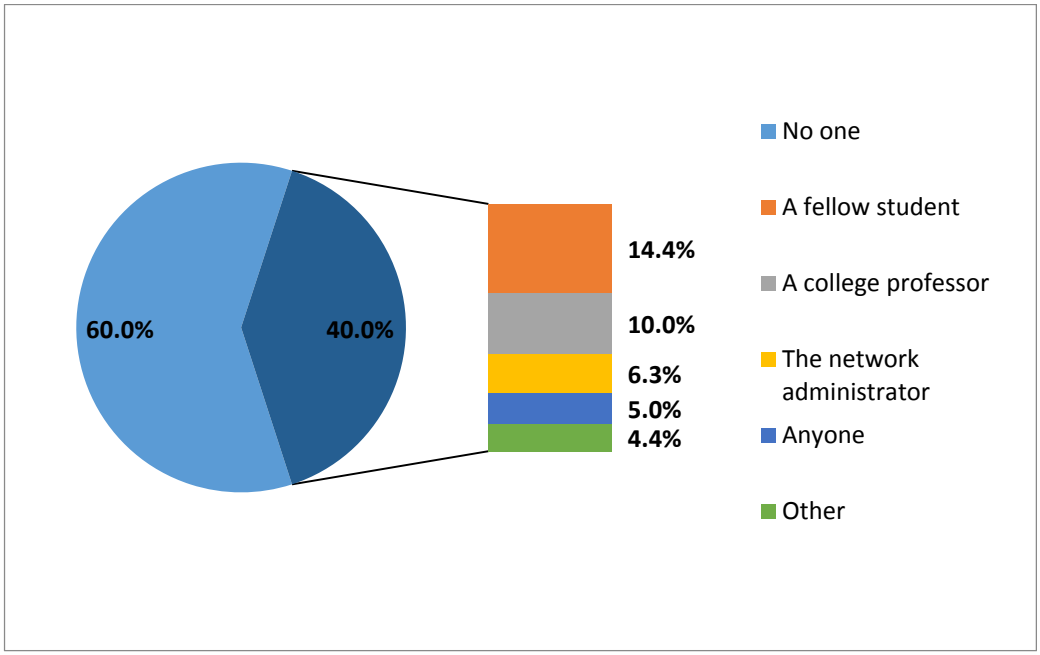


Figure 15: To which of the following people would you reveal your password if requested to do so?

Although 60% of respondents would never reveal their passwords to anyone, a significant number (40%) would reveal their password to various groups of people (e.g., college professors, fellow students, network administrators). If these figures are compared against employed and unemployed students, the figures change significantly showing a higher level of security awareness among those in employment. Only 27% of students in employment feel confident to reveal their password as compared to 41% of those who are not employed. Still this is a significant percentage making those respondents susceptible to social engineering attacks. This is particularly important as it is not just the security of their personal assets at risk, but their employer's as well.

The next question continued the examination of password usage as a method of security attack prevention (Figure 16). In this case, the users are presented with a list of choices and they are asked to choose which of these were acceptable and safe to choose as their password. 41% of the respondents would choose a combination of letters and digits in upper and lower case which represents a fairly safe choice. At the same time a similar number would choose something that was easily remembered. Although such a choice cannot be fully considered as a security flaw, it is questionable whether something easily remembered is considered a strong password. If these figures are compared against employed and unemployed students, it is rather unusual to report that 49% of non-employed students would choose a safe and strong password (combination of letters and digits in upper and lower case) compared with only 27% of those in employment.

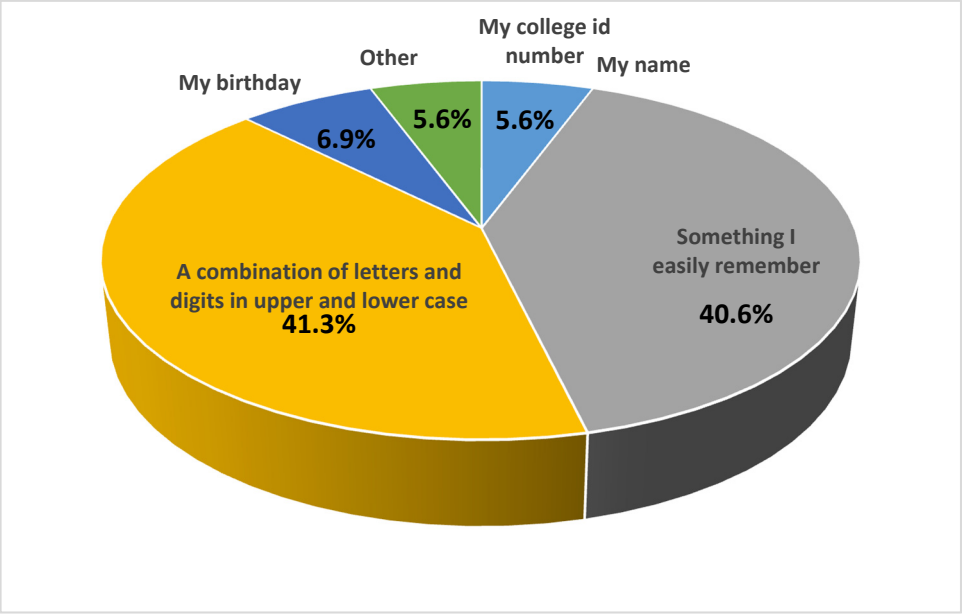


Figure 16: Which of the following password would you feel are acceptable and safe to choose as your own?

When asked about password usage, 38% used the same password for everything that needed a password, with 56% reporting that they did not re-use passwords.

4.5 Pre-university awareness level - Survey Results Discussion

The participants in this survey represented a group of young individuals registered for an introductory course in information systems during their first year of their degree. The population sample was varied from many study disciplines either from the school of liberal arts and sciences or the school of business, and the results exemplify the rule that security is also of relevance to a non-technical audience. Information security curricula should include both technical and non-technical issues. Information security is widely recognized as technical as well as non-technical (von Solms and von Solms, 2004a).

Although from the survey findings appears that participants have a good level and understanding of information security issues, the problem of achieving security awareness among the online population still remains; especially when discussion is about secure use of e-mail, password, and internet usage habits. The recent years broadband adoption (also reflected within the respondent group) along with its always on nature combined with the significantly increased speed of service means that users are significantly more exposed than their dial-up counterparts (Furnell et al., 2007).

At the same time, the large number of respondents that use a computer at school (second higher after home), indicate the role that academia has to play in information protection. A good and solid understanding of information security issues acquired at school will provide the foundation of an acceptable security awareness level at home and at the work environment.

The majority of respondents engage in a range of applications for which security ought to be a consideration (Table 5). Despite the fact that many respondents perceive that they are aware of potential threats and risks, and believe they pose the necessary security knowledge, their practice does not always evidence this. Often there is a considerable gap between what user know about information security terms, concepts, measures and practices and what they actually do in reality (Kruger and Kearney, 2006; Dodge et al., 2007). Although they argue that they possess the necessary knowledge to protect their information assets, they are willing to open an e-mail attachment if it originates from a trusted source (e.g., Friend or university authority), or feel comfortable to reveal their password if they are asked to do so. At the same time they are ready to engage themselves in non-secure practices like downloading music and programs using file sharing programs or file repositories. Concerning this type of downloads (music or programs), the question was very specific and was indicating the users' download preference using file sharing programs (the use of torrents was specifically mentioned) or file repositories which is definitely considered not only an insecure but also illegal practice.

One factor that may influence a user's security behavior is whether security was emphasized or somehow "presented" and communicated when they bought a system and started using it to get online. Surveys indicate that a significant majority of users do not receive any security-related information or advice when they purchase a computer or an Internet connection (Furnell et al., 2007). The survey attempted to assess where advice might be sought after the original purchase and during the use of the equipment. It seems that informal and more "personal" sources of advice, such as friends, colleagues and college professors are the most popular than other categories. This finding is also supported by the

Trustguide project (Lacohee et al., 2006) which indicates that individuals build trust with a service through the experimental use of it. Thereafter, in cases where protection of computer assets from potential dangers comes into question, it is clear that information communicated by a peer or a college professor was more valued than other more formal sources. At the same time, the awareness efforts of official and mass media sources to educate the online population seem to lack in engagement and impact. Finally, from the survey responses it appears that there is a need for information security training in order to achieve an acceptable level of awareness and user practice. As illustrated in Table 6, among others, a large number of respondents lack knowledge for important InfoSec terms like “phishing”, “social engineering”, and “trojans”. Although the lack of knowledge for basic security terminology like “shoulder surfing” and dumpster diving” is not considered a weakness, their perceived knowledge of information security principles seems a little bit mixed and imbalanced. They mostly feel that they possess the necessary knowledge in order to protect their information assets (66%) but they are ready to reveal their password to friends and relatives or open e-mail attachments. They claim to be able to understand if a website is secure but they cannot describe what constitutes a secure site although they are very confident with online shopping.

At the same time a considerable 49% are NOT confident with recognizing a security incident. Fortunately, the wide majority of respondents is concerned about the safety of their information assets (64%) and is very positive towards the importance of information security training (74%). This would make it easier to integrate information security concepts in the curriculum in a more structured and systematic way.

4.6 Presentation of Results – Established students awareness level

It is widely understood that academia plays an important role in information protection. Not only does it introduce students to information security concepts and how to protect vital data and information resources, but it also equips them with the necessary security skills in order to succeed in their future careers and their wider personal use of IT systems. The aim of this survey was to investigate the need for more general security awareness amongst the online population and in order to achieve this sample data was used from a University environment. The objective was to investigate the level of security awareness of students currently registered on an introductory course in information systems along with the examination of opinions and habits covering students' use of the Internet, their level of security knowledge, password habits, methods used for protecting computer and electronic data, use of e-mail, etc. The sample population was comprised of students with a broad range of ability, interest and technology skill.

One of the challenges of today's rapidly changing technological environment is for academia to prepare professionals that can protect critical infrastructure and investments in people, equipment and information assets (Yurcik and Doss, 2000). Academia is the starting point in producing professionals who are information security literate, so focus has to be placed upon what can be achieved there.

The critical question that arises is whether the level of awareness of students changes as they progress to their studies. Are there any differences between the level of awareness of entering students and those towards graduation? In other words does academia play a role in the effort to raise the awareness level of the

online population? In order to identify whether the level of awareness changes as students' progress in their education, a similar research study was conducted. Similarly as in the previous case, students were chosen but in this case we have students from two different categories. Students that have completed up to thirty credit hours, in other words students that have completed their first year of studies and students with ninety or more credit hours completed, in other words students towards graduation.

A similar questionnaire of approximately 33 questions in three sections (see Appendix II) was used (background information, opinions and habits in the use of the Internet, and related services and true/false questions where the level of agreement with a specific information security issue/statement is examined) and again the results are presented and interpreted using the following four sections:

- Background information.
- Use of IT and the Internet.
- Security Knowledge and Perceptions and
- Security Practices and Behaviors.

The main difference between the two survey instruments is that in this survey, the participants were asked to watch a short e-learning unit in a form of a web-based presentation (See Appendix III). This was an initial attempt to check whether an e-learning approach could work in an effort to introduce generally required information security concepts to the student population. The e-learning unit was a combination of the visual learning and auditory learning styles (explained in more detail at chapter V of this thesis) in an effort to check if student learning can be improved by presenting elements with multiple ways. The purpose of the unit was to provide to the students a better understanding of basic

concepts that govern information security issues. More specifically, the purpose of the small e-learning unit was to:

- Introduce basic everyday information security concepts.
- Describe the threats and risks associated with unsecure behavior and,
- Provide a range of safeguard methods.

The unit started by providing an easy to understand definition of what is information security along with some information security facts related to information security threats and data breaches. Then the unit continued by presenting the following important “keys” to security:

- Software Updates.
- Use of Antivirus and Anti-spyware software.
- Use of Passwords.
- Data Backup.
- Online Messaging.
- Principles of online safety.
- Peer-to-peer and social networking.
- Social engineering.

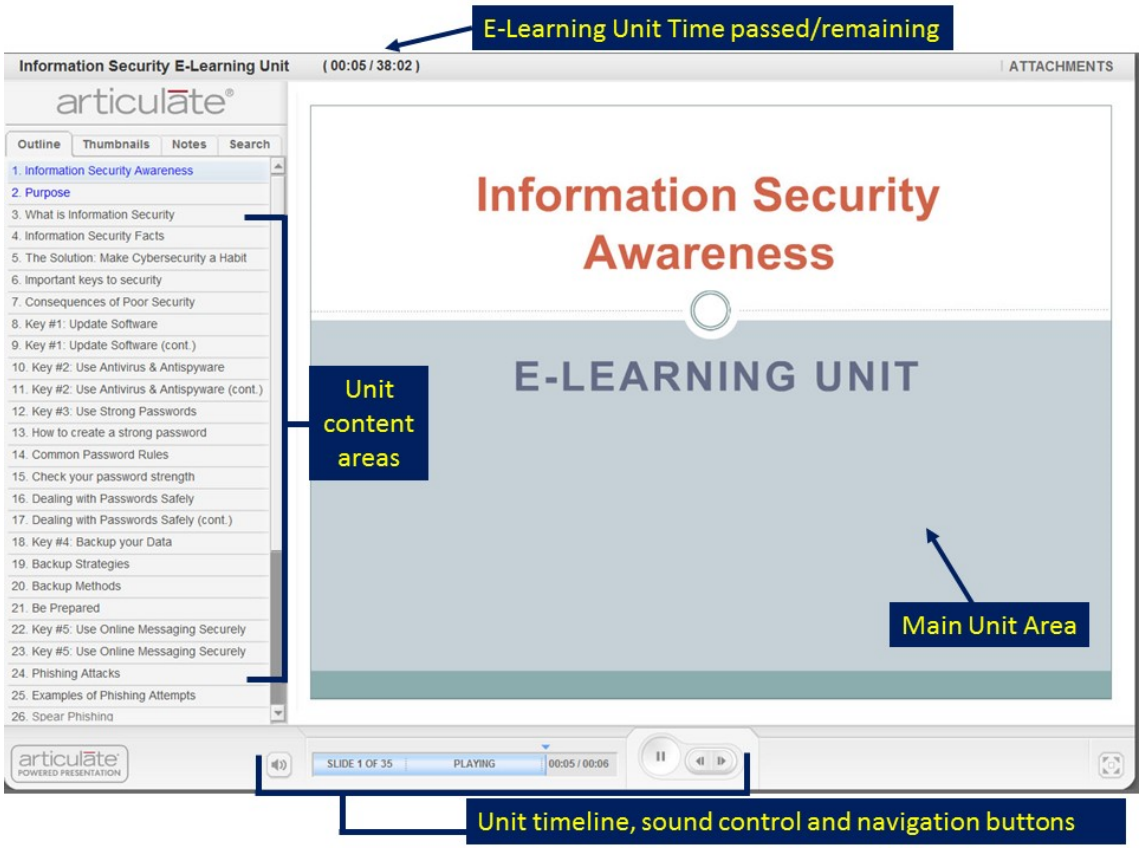


Figure 17: E-learning unit introductory screen

Figure 18: E-learning unit, Information Security Components

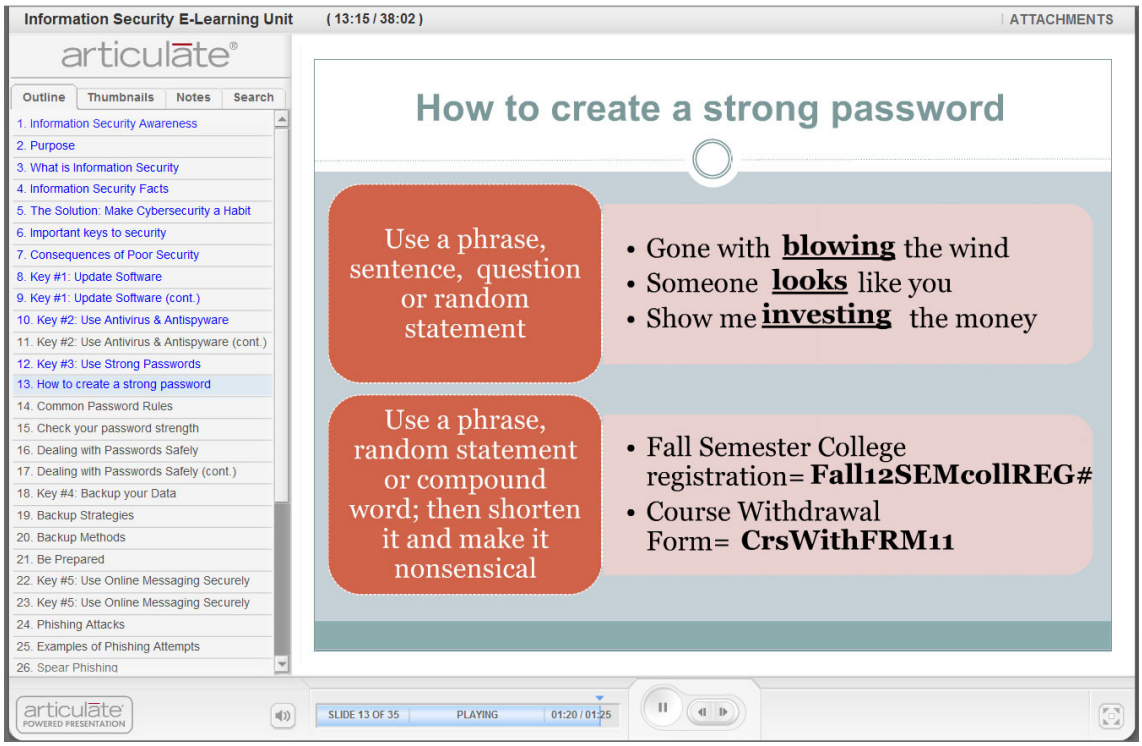


Figure 19: E-learning unit, creating a strong password

The above figure (Figure 19) represents a simplified approach on how to create a password that is strong and at the same time, it has a special meaning so it can be easily remembered. In the first case the suggestion is to choose your favorite movie, a song title or a famous quote, and alter it by putting a random word inside it or special characters. In the second case, the suggestion is to choose a phrase or random statement then shorten it and make it nonsensical to a stranger but still meaningful to the its owner. For example, in the case of a student, the phrase "Course Withdrawal Form" can be transformed to CrsWithFRM11 (adding numbers which may represent the year) which makes sense to them, can be easily remembered but still be used as a string password.

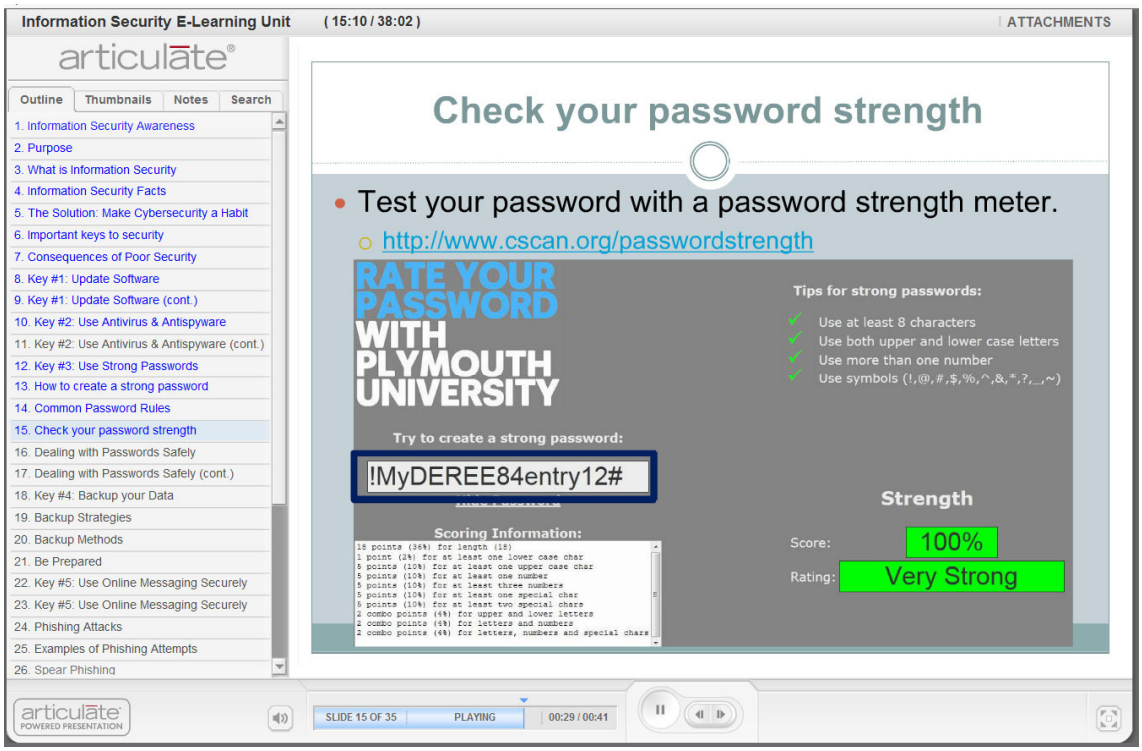


Figure 20: E-learning unit, checking the password strength

The purpose of the e-learning unit was not to educate users on online security issues, nor increase their level of awareness but –as mentioned before- provide them with a better understanding of basic concepts that govern information

security issues. The total duration of the e-learning unit was approximately 35 minutes and it was possible by the participants to jump or repeat specific parts.

At the end of the unit, the participants were provided with the link required in order to complete the information security survey. The survey results can be summarized as follows.

4.6.1 Established Students Survey, Background Information

A total number of 153 responses were collected out of the 400 approximate invitations sent and the participants were almost equally distributed between males (56%) and females (44%). In terms of student classification a similarly equal distribution between freshmen (40%) and seniors (60%) is observed. The results of both questions combined are shown in the table below:

	Freshmen	**Seniors**	**All**
Male (n)	35	50	85
%	22.9%	32.8%	55.7%
Female (n)	26	42	68
%	16.9%	27.5%	44.4%
All (n)	61	92	153
%	39.9%	60.1%	100.0%

Table 9: Gender and student classification combined

From the sample size in terms of student classification it can be concluded that the sample is representative and the results extracted sufficiently represent the level of security awareness between incoming and students towards graduation.

In terms of major representation to the survey, it seems that in the overall, students majoring in Business slightly dominate by 58% as compared with the students majoring in Arts (37%). The 5% of students appearing as undecided in terms of major is considered insignificant.

	Arts	Business	Undecided	All
Freshmen (n)	22	36	3	61
%	14.9%	24.5%	2.1%	41.5%
Seniors (n)	32	49	5	86
%	21.8%	33.3%	3.4%	58.5%
All (n)	54	85	8	147
%	36.7%	57.8%	5.5%	100.00%

Table 10: Student classification and major combined

When data in respect to student classification and major is combined (Table 10), it is clear that the seniors majoring in business slightly dominate the sample answers.

Almost half of the survey participants are currently employed (54%). When measured in terms of college year, it is clear that students towards graduation are the vast majority of the ones currently employed as indicated by Table 11. At a later stage of this analysis the group of employed students will be further measured in order to examine whether employment status has a significant contribution on the awareness level.

Status	Employment		
	No	**Yes**	**All**
Freshmen (n)	41	20	61
%	26.8%	13.1%	39.9%
Seniors (n)	29	63	92
%	18.9%	41.2%	60.1%
All (n)	70	83	153
%	45.7%	54.3%	100.00%

Table 11: Student classification based on employment status

The last question from the background information section indicates that most survey participants (35%) are under 20 years old. When this is combined with college year data, this age group is still the dominant one for freshmen (63%) but in the case of seniors, the >26 years old is the dominant selection (52%).

4.6.2 Established Students Survey, Use of IT and the Internet

The following sections presents the survey findings related with the use of IT and the Internet and the respective comparison between freshmen and seniors. Concerning computer usage, irrespective of student classification, the most dominant answers are at home and at school. When comparing the answers provided from freshmen and seniors, although the above observation still persists, there is almost a double number of seniors that use Internet at the office. This is completely in accordance with the results received from the background information, taking into consideration that there is significant number of seniors who are employed. At the same time, a noteworthy number of both freshmen (21%) and seniors (24%) have reported that they access internet on the move using a mobile device. This option is classified as the third most favorable method of accessing the Internet for both student groups.

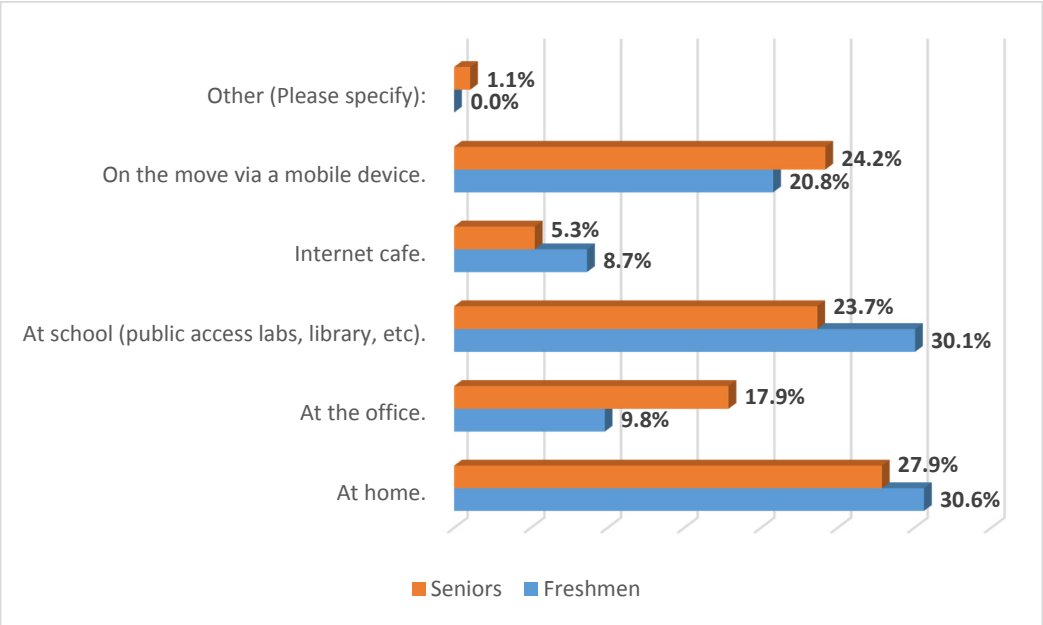


Figure 21: Respondents' modes of Internet access by student classification

The differences between the two groups are not very significant. Only in the case of accessing the Internet from the office it seems that there is a double number of seniors that access it from the office as compared to the freshmen group. This is totally justifiable taking into account that there is a larger number of senior students that are employed as compared to freshmen and because of Internet is a significant part of all businesses today. At the same time, it is in complete accordance with the number of freshmen that access Internet from the school (smaller number as compared with freshmen students). Another noteworthy observation is the number of students that use Internet on the move using a mobile device, which is significantly higher than the number of incoming students that have reported using it at the pre-university survey described previously in this chapter.

When comparing employment status and computer usage on the move through a mobile device, from the results it appears that there is no correlation between the two variables. Although students with employment seem to access the Internet on the move on a more frequent basis than others, the difference is not significant. The same conclusion is reached when comparing student status and Internet usage through a mobile device.

Most freshmen (81%) and senior (87%) respondents access the Internet using a DSL broadband connection. Similar percentages for both student groups are reported using either the school or the company Internet connection. At this point it is important to mention that there is a number of respondents that report access the Internet using a mobile device like a mobile phone. This number is significantly larger for seniors (77%) as compared with freshmen (52%).

Concerning Internet usage the most dominant answer for freshman users is between 1 and 3 hours per day (41%), with the option between 4 and 5 hours (33%) as the second most dominant. Concerning the seniors group, the same two options are the most common ones but with smaller percentages. Instead, there is a notable percentage of 23% of seniors that use Internet more than 8 hours.

From the table below, it appears that there is no direct relationship between employment status and average amount of time spent online on a daily basis. A slight correlation appears only in the case of average time spent online more than 8 hours.

Employment	< 1 hour	>8 hours	1-3 hours	4-5 hours	6-8 hours	All
No (n)	0	4	25	27	14	70
%	0.0%	2.6%	16.3%	17.7%	9.2%	45.8%
Yes (n)	8	22	26	22	5	83
%	5.2%	14.4%	17.0%	14.4%	3.3%	54.3%
All (n)	8	26	51	49	19	153
%	5.2%	17.0%	33.3%	32.0%	12.4%	100.00%

Table 12: Average time spent online classified by employment

Similarly as with the previous survey, the sample is well above the EU average and that the sample population are the most intensive internet users (European Commission, 2009).

The next question –similarly as the previous survey– measures the respondent's use of the Internet as they are asked to choose three answers from a list of common Internet applications. A comparison is performed between freshmen and senior students.

	Freshmen			Seniors		
Internet Usage	**#**	**Rank**	**ALL**	**#**	**Rank**	**ALL**
E-mail	44	1	69.8%	82	1	88.2%
Educational purposes	42	3	66.7%	57	3	61.3%
Chat rooms	4		6.3%	2		2.2%
Games	11		17.5%	14		15.1%
Web browsing (excluding social networking)	30	4	47.6%	68	2	73.1%
Shopping	3		4.8%	5		5.4%
Banking/Paying Bills	3		4.8%	4		4.3%
Instant messaging	7		11.1%	4		4.3%
Social Networking	43	2	68.3%	40	4	43.0%

Table 13: Internet usage according to student classification (first four preferences from each group appear in red).

From a general observation of the table results it is shown that both groups have the same internet usage preferences (first four chosen options) while their rankings slightly change. The use of e-mail is the most popular use of the Internet among the two student groups. This is in accordance with relevant research surveys which report high numbers of email usage between ages 18 and 29 (Zickuhr and Madden, 2012; Prescott, 2014). It seems that the use of email is more valued by students towards graduation taking into account that a large number of them are also employed and use it as a tool for their daily tasks. In the case of social networking, it seems that the use loses its "popularity" as the students' progress in their academic life and become more mature.

From the previous survey, there was a concern about the Internet usage for educational purposes since the figure reported was considered low. Using the sample from this survey, it seems that the usage figures for both student groups are significantly higher.

At this point a comparison of the answers to this question with the answers to relevant true/false questions presented later at the survey could be the basis for useful interpretations.

In the case of freshmen, although web browsing in terms of popular Internet usage method reports low figures (48%), a 77% report that they have used Internet to download music or programs using file sharing programs or online file repositories. A 66% of the same group report that they have bought things online. In the case of seniors, although figures reported for web browsing (73%) and buying good online (80%) are in close relationship they still report insecure behavior since an 80% report that they have used Internet to download music and programs from file sharing programs and online repositories. At the same time, these figures (program and music downloads) greatly contradict with the user's perception on downloading music, videos or programs without permission presented later on this report.

Finally, as it has been observed at the previous survey, it should be noted that that the very low percentage of respondents of both freshmen and seniors that buy things online (approximately 5% for both groups), still represents that this option is the least favorable internet usage among the options presented at this question and does not necessarily mean that students do not at all buy things online. This is clearly represented at a later question where significant amounts of freshmen (66%) and seniors (80%) report that they have been engaged in such activity.

4.6.3 Established Students Survey, Security Knowledge and Perceptions

The first question that actually deals with respondent's security knowledge and perception, is the one that examines their opinion about what may happen as a result of poor information security. Participants were asked to choose from a list

of options and more than one answers was permitted. The responses are presented in the table below:

College Year	Loss of access to computer and data	Loss of work not backed up	Loss of productivity	Personal liability and/or responsibility
Freshmen (n)	44	38	27	24
%	71.1%	62.3%	44.3%	39.3%
Seniors (n)	65	62	32	46
%	70.7%	67.4%	34.8%	50.0%

Table 14: Users' perception on the results of poor information security

Although participants could select all of them as valid responses, only a very small number has chosen to do so. In the case of freshmen, only 11 participants out of 61 have chosen all answers. In the case of seniors, a similar (although slightly better) situation is observed where 24 out of 92 participants have chosen all answers.

As it can be seen, freshmen and seniors have almost the same feeling that poor information security can results in loss of access to computer and data (71%). For the other options, answers are lower for both groups. It is notable that few freshmen (44%) and seniors (35%) feel that poor information security may result in loss of productivity. An even more notable observation is that almost one out of two respondents do not consider personal liability or responsibility to be one of the outcomes of poor information security. When these results are compared based on employment status in the case of seniors results are almost double ("Yes" responses). This is not observed in the case of freshmen but still figures are higher. The only exception to the rule is the case of personal liability where results do not change significantly between employed and unemployed students. In other words, employment does not have a significant contribution in user's perception on personal liability as a result of insecure behavior.

The next question is an effort to identify whether the respondents possessed the necessary knowledge in order to protect their information technology assets (Figure 23) (Figure 23). Similarly as in the previous survey there is a degree of subjectivity to this question since it does not ask for further clarifications but tries to measure their subjective judgment of whether their knowledge of information security issues was enough to protect their technology resources.

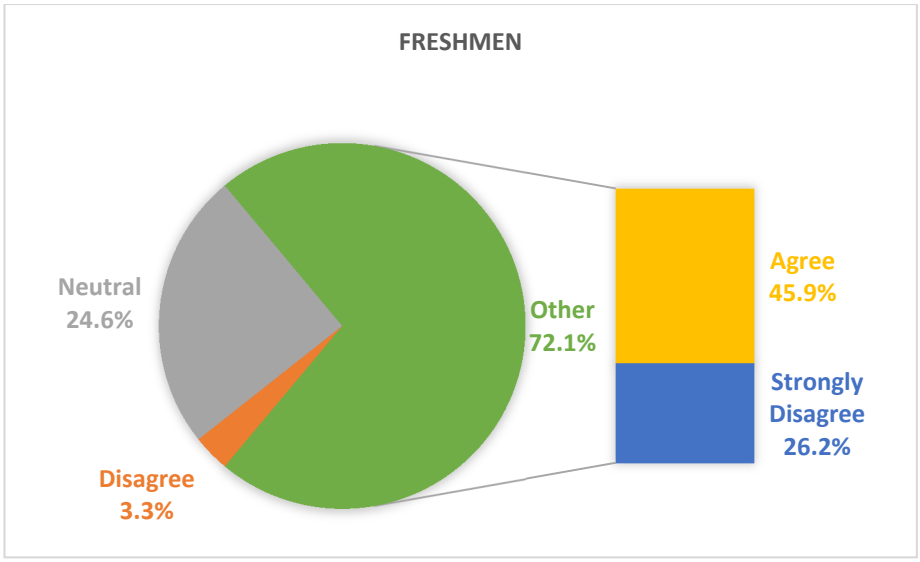


Figure 22: Responses to the statement 'I possess the necessary knowledge in order to protect my information technology assets' Freshmen group

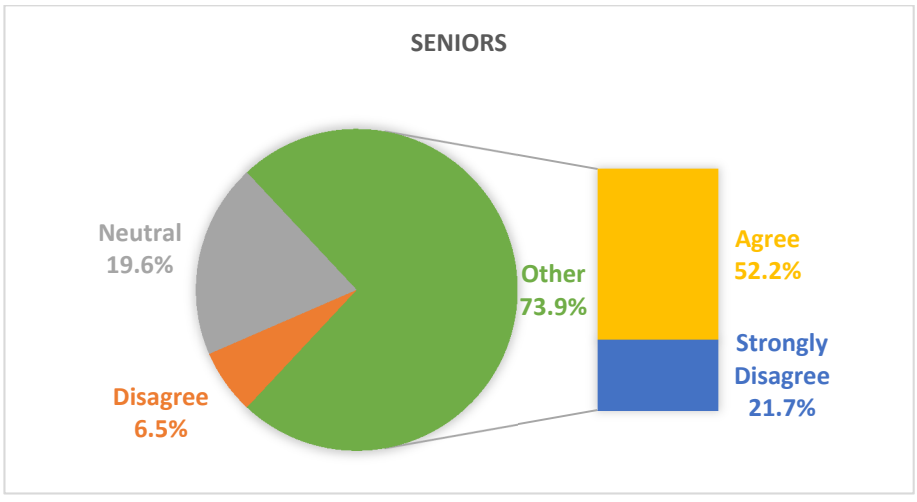


Figure 23: Responses to the statement 'I possess the necessary knowledge in order to protect my information technology assets' Seniors group

Approximately an equal number of respondents from both groups felt that they possessed the necessary knowledge to protect their information resources

(combined percentages of those who answered agree or strongly agree). It should be noted that a figure between 20% and 25% of both groups express a neutral opinion about this kind of knowledge.

The next question, is the first actual effort of the survey to touch base on the concept of phishing and examine respondents' opinions (basically from their existing experiences) on what constitutes a phishing attempt. The options provided do not intend to cover all possible phishing variations, but rather measure which of the most common phishing attempts can be identified by the two student groups. Selection of more than one options was allowed. From Table 15, it appears that urgent emails threatening loss of access to accounts if username and password are not provided are the most common ground for a phishing attempt by both student groups. The other options receive insignificant values.

College Year	**Invitations to see photos of family or friends**	**Pleas for disaster relief assistance**	**email threatening loss of access to accounts**
Freshmen (n)	26	15	46
%	42.6%	24.6%	75.4%
Seniors (n)	40	39	75
%	43.5%	42.4%	81.5%

Table 15: Potential premise for a phishing attempt

From a closer observation of the result above, it seems that all student groups have witnessed most common phishing attempts with no significant variations between the different student groups. Similarly as the previous question, a small number of respondents from both groups have reported witnessing all these as attempts for phishing attacks.

As with the previous survey, the research has attempted among others to consider information security issues that deal with password protection and use, e-mail usage habits and users' opinion about their level of information security knowledge although such an analysis is based on their subjective opinion. Similarly at this point the participants are presented with a list of information security terminology terms and are asked to indicate their level of familiarity. Again the list contained an imaginary term (whooping) to measure whether the respondents were providing considered responses. The following table presents the responses collected by both student groups plus the total percentages of those that have chosen "Very Familiar" and "Familiar" with highest values highlighted:

IS Terminology	5 Very Familiar		4 Familiar		3 Somewhat Familiar		2 Least Familiar		1 Not at all familiar		Sum of 4 and 5	
	F	S	F	S	F	S	F	S	F	S	F	S
Spyware	38.3%	52.2%	25.0%	25.0%	23.3%	14.1%	5.0%	5.4%	8.3%	3.3%	63.3%	77.2%
Phishing	28.8%	36.7%	27.1%	33.3%	13.6%	11.1%	13.6%	13.3%	16.9%	5.6%	55.9%	70.0%
Dumpster Diving	5.1%	8.7%	1.7%	8.7%	16.9%	12.0%	10.2%	21.7%	66.1%	48.9%	6.8%	17.4%
Shoulder Surfing	8.5%	15.2%	10.2%	9.8%	18.6%	13.0%	10.2%	27.2%	52.5%	34.8%	18.6%	25.0%
Whooping	5.2%	2.2%	8.6%	5.5%	19.0%	13.2%	10.3%	34.1%	56.9%	45.1%	13.8%	7.7%
Identity Theft	34.4%	47.8%	32.8%	27.8%	16.4%	4.4%	8.2%	12.2%	8.2%	7.8%	67.2%	75.6%
Spam	61.7%	71.3%	25.0%	24.1%	6.7%	0.0%	3.3%	2.3%	3.3%	2.3%	86.7%	95.4%
Trojan	45.8%	69.2%	20.3%	20.9%	20.3%	2.2%	0.0%	4.4%	13.6%	3.3%	66.1%	90.1%
Virus	66.7%	75.0%	22.8%	18.2%	10.5%	4.5%	0.0%	0.0%	0.0%	2.3%	89.5%	93.2%
Worm	43.9%	59.1%	19.3%	22.7%	21.1%	8.0%	5.3%	5.7%	10.5%	4.5%	63.2%	81.8%
Adware	32.8%	49.5%	24.1%	19.8%	19.0%	12.1%	8.6%	6.6%	15.5%	12.1%	56.9%	69.2%
Social Engineering	16.1%	42.2%	16.1%	7.8%	16.1%	10.0%	16.1%	23.3%	35.7%	16.7%	32.1%	50.0%
Spear Phishing	10.3%	18.4%	6.9%	6.9%	19.0%	8.0%	17.2%	26.4%	46.6%	40.2%	17.2%	25.3%

Table 16: Perceived level of familiarity with specific information security terminology by student group (F: Freshmen, S: Seniors)

It is clear from the responses both student groups were very familiar with traditional terms involving malware cases like “Virus”, “Trojan”, “Spam” and “Worm”. In the case of freshmen, a significant percentage of respondents do not recognize other serious information security terms like “Phishing”, “Social Engineering” and “Dumpster Diving”. Although their opinion is subjective, the percentages reported are considered very low. In the case of seniors, numbers are significantly higher at all terms but still significant lack of knowledge is reported for social engineering terms and approaches like “Spear Phishing”, “Dumpster Diving” and “Shoulder Surfing”. When responses are evaluated based on employment status, no significant variations appear.

When comparing these results with the ones obtained from the previous survey (Figure 24) we can see that the general pattern is that as students’ progress in their academic life, their perceived level of familiarity with specific information security terminology changes.

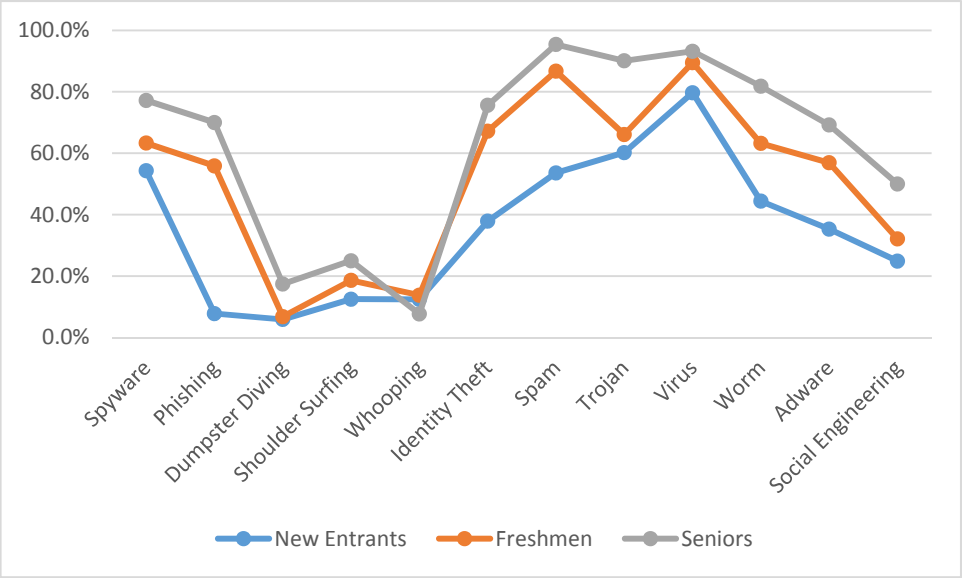


Figure 24: Comparison of the perceived level of familiarity with specific information security terminology between new entrants, freshmen and seniors (Familiar and Very Familiar answers)

In general all figures appear higher between the new entrants, freshmen and seniors. In the case of the traditional terms like “virus” and “spyware” that are widely used in everyday life, no significant variations are observed between the three student groups. At the majority of the other terms, a significant increase is observed at the perceived knowledge between new entrants and freshmen students (familiar and very familiar opinions).

This increase although it continues in the case of senior students, it is not that high as it was when comparing the first two groups. This can be explained by the fact that basic security concepts and terminology are introduced at an introductory computer science course (CS1070) taken by all students during their first year of studies but after that there is no additional effort to cover information security concepts anywhere in the curriculum. Indeed, in the case of terms where specific security knowledge is required (e.g. dumpster diving, shoulder surfing, social engineering), the variations between the three examined groups is insignificant.

Similarly as with the previous survey, the next question tries to identify how users obtain their information security knowledge and how they protect their computer assets from potential dangers (Figure 25).

More than one answers may be chosen from a list of the most popular sources available for information protection.

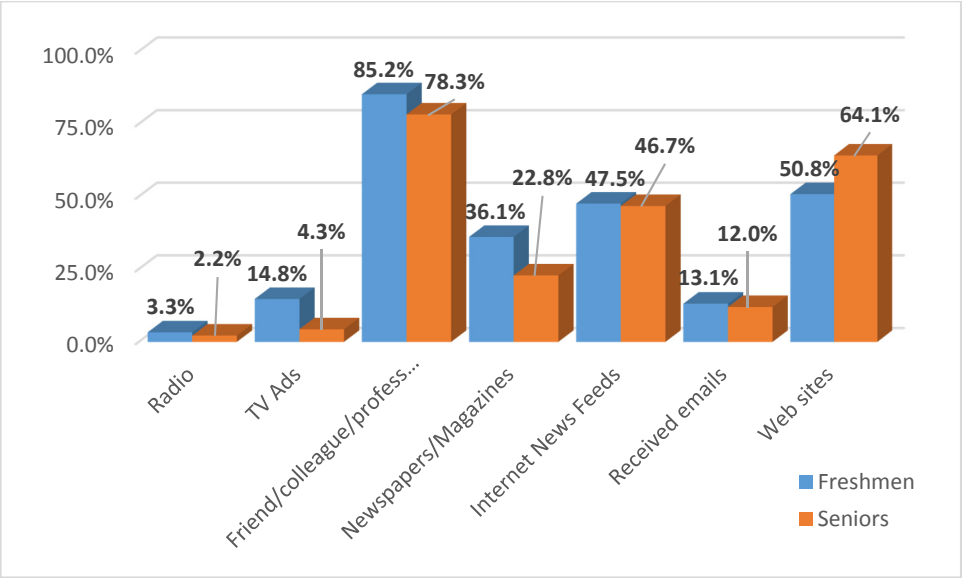


Figure 25: Sources of information for protection of computer assets by student group

It is evident from the survey responses that no significant differences are observed based on student status and participants are still more confident in using informal and more "personal" sources of advice, such as friends, colleagues and college professors. Other sources include web sites, newspapers/magazines and news feeds. Radio, TV ads and received emails have very low popularity among both student groups.

Taking into consideration the results of the previous survey, it seems that there are no notable differences between incoming students and established students. Both groups are more confident in using informal and more "personal" sources of advice. The only exception to this rule is the case of radio and e-mails as a source of information for protection where established students seem less willing to use.

The next question asked the respondents to indicate their level of agreement with specific statements that concern information security threats from hacking/hackers. The responses classified by student group appear below:

IS Statement concerning hacking	Strongly Disagree and Disagree		Neutral		Strongly Agree And Agree	
	F	S	F	S	F	S
If my data is encrypted, it is safe from hackers.	45.9%	36.9%	29.5%	37.0%	24.6%	26.1%
If my computer is behind a firewall, it is safe from hackers.	52.5%	48.9%	24.6%	27.2%	22.9%	23.9%
Despite its popularity, hacking is very rare.	68.8%	82.6%	19.7%	10.9%	11.5%	6.5%
I have very little to lose if a hacker invades my computer.	52.5%	58.7%	21.3%	21.7%	26.2%	19.5%
The greatest threat to electronic information comes from hackers.	42.7%	50.0%	26.2%	35.9%	31.2%	14.1%

Table 17: Opinions concerning hacking by student group

It seems that the opinions concerning hacking by both participant groups are fairly equal. When comparing same questions from the previous survey notable differences are only observed in the question whether hacking is very rare, where Agree and Strongly Agree opinions are much higher (33%), and in the question whether the greatest threat come from hackers where again Agree and Strongly Agree opinions are higher (54%). At all other cases no significant differences appear between the different groups. What needs to be taken into serious consideration are the opinions of respondents that appear neutral at the statements concerning hacking. These percentages vary between 20% and 37% among the two student groups which are considered very significant figures. Although we are still dealing with the subjective opinion of respondents, it has to be considered whether the answers refer to true neutrality or lack of knowledge. This hypothesis can be tested by measuring the “Agree” and “Strongly Agree” opinions of participants at the same questions. Although this can be considered as a non-scientifically valid interpretation it still can help into making valuable observations. From that comparison we can observe the following:

- Freshmen students have almost equal “Neutral” and “Agree and Strongly Agree Opinions”. Four out of five questions have no more than 5% difference.
- Seniors appear to have three out of five questions with no more that 5% difference and a very high degree of neutrality at the rest.

From the above observations, it can be concluded that neutral answers may really refer to lack of knowledge about the subject.

At the previous survey the incoming students’ opinions were examined in regard to downloading commercial music, videos and programs without permission and whether such behavior was wrong or not. The answers received were using a Likert scale ranging from strongly agree to strongly disagree. In this survey the same question was asked but in this case more definite answers where requested in the form of Yes/No answers. The same 28% of both student groups was reported as an acceptable behavior which represent almost two thirds of the respondents. In the case of freshmen no differences are observed for employed students but in the case of seniors, it seems that employment plays a vital role in their opinion since the percentage that report such behavior as acceptable drops to 14%. It is important to note that a significant percentage of the freshmen group (30%) chose not to answer at this question. It is interested to inspect the answers provided to this question with the answers provided at the question that examined whether peer-to-peer networks are considered a convenient and safe way to search and download. Although the objective of these two questions is different (first deals with inappropriate behavior and second with safety opinion on usage of specific Internet service), and the use of peer-to-peer programs is not the only

way for downloading commercial music, videos and programs, it is still worth considering whether these two questions provide related answers.

Strongly Disagree and Disagree		Neutral		Strongly Agree and Agree	
Freshmen	**Seniors**	**Freshmen**	**Seniors**	**Freshmen**	**Seniors**
43.0%	26.0%	39.0%	51.0%	16.0%	21.0%

Table 18: Opinions to the statement: "Peer-to-peer networks are considered a convenient and safe way to search and download files over the web"

From the table above it appears that "Agree" and "Strongly agree" answers to the question are lower in respect to the 28% of the respondents at the previous question (significantly lower in the case of freshmen) but a very notable percentage of both groups express neutrality to the statement, opinion that can be explained as lack of knowledge on the specific subject.

The opinion of the different student groups concerning the importance of backups is almost equally balanced. More than 4/5 of the freshmen (83%) and seniors (90%) keep important information in more than one place. Almost half of freshmen (43%) and seniors (46%) reported that they cannot understand if a website is secure to give information. From those that reported the opposite, and provided a justification of what constitutes a safe site (54 out of the 60 respondents) less than half were able to provide accurate or close to accuracy answers about what constitutes a secure site.

Finally, at the previous survey it was examined whether students use instant messaging programs. In the survey the question is modified in order to examine students' perception concerning instant messaging as a secure method for sharing university data. Taking into account the proliferation of instant messaging today either as standalone applications or as part of online software suites and social networks, such question could provide with a valuable insight on the

purposes of instant messaging use by students. It appears that only a 13% of senior students consider instant messaging as a safe method for sharing university data as opposed to the 27% of freshmen. No variations are observed if we compare student answers based on employment status.

4.6.4 Established Students Survey, Security Practices and Behavior

The last section of survey findings dealt with user's security practices and behaviors.

The next question tried to identify what type of protection was preferred by students in order to protect their computer and electronic data (Figure 26). The question presented a list of common information security procedures and more than one answer choices could be selected.

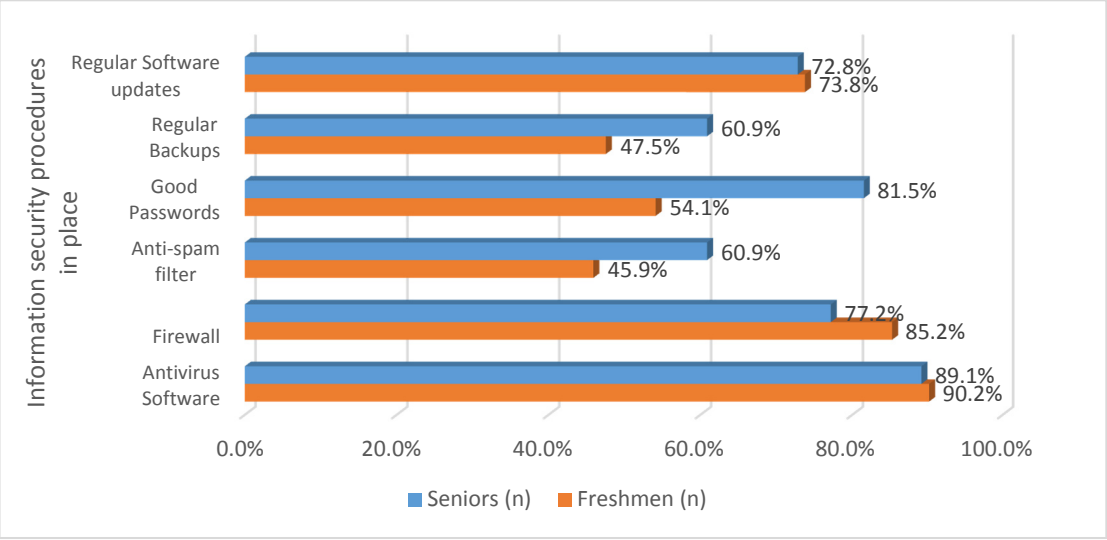


Figure 26: Do you have any of the following in place in order to protect your data and electronic data?

Similarly as with previous questions allowing more than one answer, also in this case all answers could be arguably selected as valid answers. Instead a small percentage from both groups have chosen to do so. More specifically, only 10

out of 61 of the freshmen students have chosen all options as methods used to protect their data. In the case of seniors a slightly better (22 out of 92 participants) but still low number is observed.

The use of antivirus software is considered the most popular option among freshmen and seniors with almost no variations at all. Same applies for the use of firewall and regular software updates, as the second and third most popular choices. In the case of freshmen, those who choose antivirus as a mean of protection, almost 83% of them decide to complement it with a firewall for extra protection. The same applies also in the case of seniors. Although in the case of freshmen, the choice of good password is not among the most common choices (same applies with the use of regular backups), seniors seem significantly more aware that the choice of good password greatly improves security measures. When comparing data according to employment status, it seems that employment does not have a significant effect in the choice security measures for both freshmen and seniors. The only serious deviation to this rule is the case of choosing good passwords since it seems that employed students tend to choose them as a method of protecting data in notably higher numbers than unemployed ones.

It is worth at this point to attempt a comparison between the figures of this survey and the figures observed on the new entrants group at the previous survey. It seems that for both survey groups the use of antivirus software receives equal popularity. In all other cases, it seems that established students report a higher number of protection measures in place as compared with new entrants. Moreover, it can be mentioned that as students' progress in their academic life, the number of available protection measures increase.

Talking about passwords, the survey examined whether participants use the same password for all services that need a password. The results varied significantly between freshmen and seniors since freshmen reported that they use the same password form all services that need a password by 37%. In the case of seniors this percentage is only 10%.

Since password usage is strongly associated with information security precautions, similarly as with the previous survey, additional questions were asked in regards to habits concerning choosing and revealing passwords. At first participants were asked whether they felt comfortable revealing their password if requested to do so. A definite “Yes” or “No” answer was required.

Answering “Yes” to this question does not mean that they would always engage themselves in such behavior but that rather they feel comfortable doing it under specific circumstances. Only eight of the participants responded “Yes”, and from those the most dominant option was the network administrator. A couple of students reported that they would feel comfortable to reveal their password to a fellow student. Responses were equally balanced in term of student status and employment.

The following question continued the examination of password usage as a method of security attack prevention. In this case, the users are presented with a list of choices and they are asked to choose which of these were acceptable and safe to choose as their password.

Student status	Freshmen	Seniors
My college ID number	8.2%	5.4%
My name	0.0%	0.0%
Something that I easily remember	24.6%	18.5%
A combination of letters in upper and lower case, digits and special characters that have a special meaning for me	80.3%	75.0%
My birthday	4.9%	0.0%
None of the above	3.3%	12.0%

Table 19: Which of the following password would you feel are acceptable and safe to choose as your password?

Between 75% and 80% of the respondents would choose a combination of letters and digits in upper and lower case which represents a fairly safe choice and is actually very close to the definition of what constitutes a strong password. At the same time, 19% of the seniors and 25% of freshmen would choose as a password something that they can easily remember. This can constitute an insecure habit if extra care is not taken so as to make sure that something easily remembered by the user is not at the same time weak and easy for others to guess.

The use of email has been identified in this and in the previous survey as the most popular Internet application. This survey continuous further this examination by identifying and examining security habits of participants concerning e-mail attachments. Similarly as previously concerning password usage, a general question is asked about whether students generally open email attachments and again a definite “Yes” or “No” answer was required. Again, answering “Yes” to this question does not mean that participants would always open email attachments but that rather they feel comfortable doing it under specific circumstances. For those that chose “Yes” an additional question was revealed asking them to identify under which circumstances they would open an email attachment by presenting a list of choices.

Concerning the definite Yes/No option, the opinion of respondents between Freshmen (45%) and seniors (52%) appears equally balanced on whether they generally open email attachments. Concerning the circumstances under which they would open an email attachment, the participants were able to select more than one option and also an "Other option was available for those that wanted to choose an option different from the ones presented. In case of freshmen students a 48% have chosen the "correct" answer (if the e-mail successfully passes the security checks of my computer), while a 44% of seniors have chosen this option. At the same time, a significant number of students have also selected the other two options.

In which case would you open the file attachment?	**Freshmen**	**Seniors**
If the mail originates from a person that I know.	77.8%	87.5%
If the mail originates from an authority (e.g. university, government, my bank) that I know.	63.0%	54.2%
If the mail successfully passes the security checks of my computer.	48.1%	43.8%
Always	0.0%	0.0%

Table 20: E-mail attachments behavior

This is another example of a question where all options could be selected. The only difference with similar multiple answer allowed questions in this survey is that only one answer is correct while the others although obvious and common choices can be considered as insecure behavior. In this case we examine whether students that have selected the "correct" option, have also chosen the "incorrect" ones. In the case of freshmen, a 30% of respondents have chosen the "correct" answer alone with no other selections. In the case of seniors this percentage drops to 24%.

Student Status	If the mail originates from a person that I know.	If the mail originates from an authority (eg. university, government, my bank) that I know.	If the mail successfully passes the security checks of my computer.	%
Freshmen	X	X	X	30%
Freshmen	NO	NO	X	**30%**
Freshmen	X	NO	X	23%
Freshmen	NO	X	X	15%
Seniors	X	X	X	24%
Seniors	NO	NO	X	**24**%
Seniors	X	NO	X	24%
Seniors	NO	X	X	29%

Table 21: E-mail attachments behavior, comparison of options selected

As it can be seen from the table above, although the "correct" option has been selected, significant percentages of respondents would also choose options that may be usually the subject to an attack. It is worth mentioning here that in the case of seniors their security habits concerning email attachments do not change significantly according to employment status. On the other hand in the case of freshmen it seems that a much higher percentage of those who are unemployed choose the correct answer (61%) as compared with those that chose it and are employed (22%).

Considering the proliferation of social networks in our everyday lives, the last question in this section dealt with respondents' habits when visiting a social networking habits. The options that could be chosen represent a brief summary on the most secure procedures that have to be taken into consideration when dealing with social networking sites and respondents could multiple answers.

Social networking security habits	Freshmen	Seniors
Disclose very few details about yourself and only with people you trust.	77.0%	75.0%
Don't accept invitations and offers from people you do not know and trust.	72.1%	78.3%
Avoid installing programs and plugins that are not verified.	70.5%	85.9%
Check privacy settings and read the policy that governs the degree of sharing personal information.	57.4%	72.8%

Table 22: Answers to the question 'Which of the following do you consider a good habit when visiting a social networking site like Facebook, MySpace and Twitter'

Although all options are of major importance when dealing with social networking sites, only a 42% of the freshmen and a 56% of seniors have chosen all options as important security precautions when visiting a social networking site. At the same time, as it can be seen from the table above, the option that receives the least popularity by both student groups is the one that deals with privacy settings and policies of social networking sites.

4.7 Established students survey, Results Summary and Discussion

The participants of this survey represent a balanced sample of young individuals from many study disciplines and the group was comprised of both first year college students and students towards graduation. Survey findings were analyzed mainly based on student academic status where a sample of freshmen (40%) and seniors (60%) is observed. At certain cases, results are also analyzed based on employment status mainly because half of the participants have reported such status.

At first, from the results received and the analysis performed, it is concluded that in the case of students, employment status does not play a significant role in shaping a secure online behavior. The results either in terms of “Use of IT and the Internet”, “Security knowledge and Perceptions” or “Security practices and behavior” do not show significant differences between those that have reported themselves as employed and those that have not. More specifically, no differences are reported in the cases of:

- Average amount of time spent online.
- User’s perception on personal liability as a result of insecure behavior.

- Perceived level of familiarity with specific information security terminology.
- Freshmen opinions about downloading commercial music, videos and programs without permission.
- Use of instant messaging as a secure method for sharing university data.
- Choice of security measures used.
- Willingness to reveal passwords.
- Email attachment behaviors for senior students.

Instead a few differences were reported in the cases of:

- Results on the outcomes of poor information security with the exception of personal liability.
- Seniors opinions about downloading commercial music, videos and programs without permission.
- Choice of good password as a security measure for seniors group.
- Email attachment behaviors for freshmen students.

In terms of the level of understanding of information security issues the problem of achieving security awareness among the online population still remains for both student groups. Although the subjective opinion of both groups is that they possess the necessary knowledge in order to protect information technology assets, there is still a significant number (1 out of 3) who do not report such confidence. At the same time in terms of secure use of e-mail, choice of good passwords and internet usage habits, the percentages reported by both groups do not directly relate with the subjective opinion reported above. At the previous survey the broadband adoption by most population along with the significant

increase in speed and quality of service, has been reported as an important factor that should be taken into consideration when deciding for the best method for establishing a successful security awareness raising method. An additional factor that should be considered is the worldwide availability and penetration of mobile internet services during the last years at all levels of the society. Reports indicate that mobile subscribers are growing four times faster than the global population (A. T. Kearney, 2013). Also the global mobile market has grown by 13.7% since 2008 with nearly seven billion total connections and a projection for 2 billion more till 2017. At the same time concerning mobile data all world regions show impressive growth rates which globally is projected to grow by 66% per annum through 2017. This growth is driven by the increased penetration of smartphones and by the increased data consumption mainly due to the fact that faster download speeds are available through the introduction of new mobile technologies (e.g. 4G). The numbers reported at this survey concerning either the use of a computer on the move through a mobile device or accessing the Internet using a mobile device confirm the trend reported above. This also represents an area where security awareness should be considered as a necessity.

At the previous survey, from the report usages of computers at school, the significant role the academia has to play in information protection has been identified, so that an acceptable foundation of security awareness level both at home and at work is provided. When comparing the results of this survey and more specifically data referring to student engagement in a range of applications for which security ought to be a consideration, security practices do not evidence a high level of awareness concerning potential threats and risks. In fact, although a large percentage of both participant groups (freshmen and seniors) report that

they possess the necessary knowledge to protect information technology assets, they behaviors evidences to the contrary. Although almost 75% of the respondents would choose something that constitutes a strong password, there is still a percentage between 20% and 25% that would choose something easily remembered. At the same time, they are willing to open an e-mail attachment if it originates from a trusted source. Almost one out of three students felt that it is acceptable to download commercial music and programs without permission and almost half of the respondents expressed their neutrality concerning the safety of using peer-to-peer networks. Finally, the use of regular backups as method of protecting data along with the use of antispam filter do not have the required popularity. At all these cases described previously, no significant differences were observed between freshmen and seniors which unfortunately draws the conclusion that academia has not played the expected role on shaping security aware personalities.

Taking into consideration the penetration of social networks in everyday lives, the threats associated with the use of such networks has significantly increased. Symantec reports that approximately 1 every 2.5 social networking sites are usually blocked by content filters which places social networking sites on the top of the list of the most popular web category types that are blocked by web policies (Symantec Corporation, 2014b). At the same time, the 2013 Norton report revealed significant threats that are closely associated with lack of security awareness among users in terms of social networking usage (Norton Corporation, 2013). More specifically:

- 39% of social media users do not log out after each session.
- One out of four media users share their login information with others.
- 31% of social media users connect with people they do not know and,
- 12% of social media users have been victims of identity theft.

The use of social networks has a lot of popularity between freshmen and senior groups. Social networks are the second most popular internet application for freshmen. In the case of seniors although such ranking falls into the fourth position, still the 43% of users using them cannot be underestimated. In fact both groups report insecure behavior in relation to social networks either in the case of using instant messaging as a secure method of sharing data (mainly freshmen) or choosing appropriate measures and following secure habits when connected to a social network.

In the case of collecting users' answers concerning their knowledge of important information security trends, the survey still reveals the need for information security training in order to achieve an acceptable level of awareness and user practice. Significant lack of knowledge is reported by both groups for terms that have to do with social engineering terms and approaches and phishing. Although most respondents report knowledge of terms like "Virus", "Spam" and "Trojan", they are ready to open an email attachment from people that they know or feel confident in using peer-to-peer networks. In the case of phishing, such lack of knowledge is also reported from a similar question where low percentages of respondents were able to recognize common phishing attempts. Further need for training is also justified by the fact that almost half of the respondents cannot understand if a site is secure but are confident with online shopping. It seems that also here academia has not played a vital role since answers do not vary significantly according to student status. Although at most cases senior student percentages are higher as compared with the freshmen ones, there are not that higher to justify a significant variance and this differentiation may be explained due to the higher number of senior respondents.

4.8 Further Research Steps

It has become evident that humans are the major cause of most information security incidents. For that they are also referred as “the weakest link in the chain” so awareness of information security procedures is essential to overcome those weaknesses. The first survey also investigated factors that may influence a user’s security behavior by examining from which sources users may seek advice for security matters concerning the use of their equipment or online behavior. The same question was also included in the second survey and both surveys indicated that users mainly seek advice from informal and “personal” sources such as friends, colleagues and college professors or Internet news feeds and web sites.

Taken into account that the wide majority of users do not receive any security-related information or advice when they purchase a computer or an Internet connection (Furnell et al., 2007), it is clear why the information communicated by a peer or a college professor is more valued than other sources. At the same time, the awareness efforts of official and mass media sources to educate the online population seem to lack in engagement and impact. The positive sign at this point is that the student population surveyed, understands the importance of information security training and is very friendly towards such efforts.

Humans *are* the weakest link in the information security chain but also an irreplaceable component in many secure systems (Cranor, 2008). It is evident that appropriate guidance is needed in order to strengthen the human factor of security and this goal can be achieved through security awareness raising. Based

on the assessment of the current state of security awareness among higher education recipients, there is still room for academia to fill the security awareness gap. Participants are able to learn and retain security knowledge if they are better exposed to security awareness education. Security awareness education has become one of the most focused areas in terms of threats prevention, and many organizations and businesses have established appropriate awareness programs that suit their needs. The problem is that while businesses who have established such programs provide awareness training to their employees, other companies lack security awareness programs so their employees remain susceptible to security threats. To achieve the goals of confidentiality, integrity and availability educating the future workforce *before* entering the workforce is the top priority.

In respect to this, the following chapters of this thesis, propose the development of an awareness raising initiative called the information security toolkit. As an awareness raising method, the toolkit will be addressed to the general user population and its objective will be to establish the security knowledge and skills that all IT users need to acquire in order to be competent and confident users of technology.

The findings of the two surveys presented before justify the development of the toolkit since students:

- Do not arrive at the university with sufficient security knowledge in order to be considered efficient technology users.
- Their engagement in normal university studies does not develop the required degree of further security knowledge.

On that basis, an additional approach is required which would be desirable to present in an accessible and structured manner such that users can develop and add to their knowledge in defined areas over time.

The toolkit will be the basis for the general technology user to understand the challenges associated with secure use of information technology and help him assess its current knowledge, identify lacks and weaknesses and acquire the required knowledge in order to be competent and confident users of technology.

4.9 Chapter Summary

The purpose of this chapter was to investigate the state of information security awareness in the academic sector in order to determine the potential of raising security awareness within the existing education systems.

For that reason the level of security awareness amongst the online population was investigated by using sample data from a university environment. The objective was to examine the state of information security awareness in the academic sector and investigate the awareness needs of students in order to (1) support them during their time of study, (2) prepare them for the workplace, and (3) protect them in their wider personal use of IT systems. In order to investigate the security awareness level of students, two separate surveys were conducted in order to investigate not only the awareness levels and needs of students in order to support them during their time of study and their preparation towards entering the workforce but also whether this awareness level changes as they progress in their studies. The first survey examines the awareness level of students when they enter the university and before they have any engagement to information security concepts as part of their studies. The second survey goes

one step further by examining the awareness levels of established university students using a sample from first year and last year students, in order to examine whether the awareness level changes as they progress in their academic life. In the case of the second survey, students before actually filling the survey questionnaire, are asked to watch a small e-learning unit in a form of a web-based presentation in order to have a better understanding of basic concepts that govern information security issues. This was an initial attempt to check whether an e-learning approach could work in an effort to introduce generally required information security concepts to the student population.

From the results of the two surveys, and the comparison between the two where possible, it seems that the awareness level of students concerning information security concepts is not at a sufficient level for students entering university education and does not significantly change as they progress their academic life towards entering the workforce. In respect to this, the development of the information security toolkit as an awareness raising initiative is proposed. The next chapter focuses upon its development as an awareness raising method that addresses the general user population.

Chapter V – The Information Security Toolkit

5.1 Introduction

The purpose of this chapter is to investigate the rationale behind the creation of the information security toolkit along with the theoretical framework on which it was actually developed. The chapter starts by presenting elements of information security learning in order to get an understanding of its meaning and importance and then proceeds with the requirements and rationale behind the development of the toolkit along with its content and distinct areas. Specifically, this chapter achieves the following outcomes: (1) understand the meaning of information security learning, (2) provide an understanding concerning the design of the toolkit from an information systems perspective, (3) identify the areas that an information security toolkit should contain and (4) describe the distinct toolkit areas along with issues and concerns behind its development.

5.2 Elements of Information Security Learning

Before proceeding to the actual process of the Information Security Toolkit development, it is worth getting an understanding of the meaning of information security learning. According to the National Institute of Science and Technology (NIST), information security, is a continuous learning process that has “awareness” as its starting point, followed by training and finally evolves into education. (National Institute of Standards and Technology (NIST), 1998). Security awareness is addressed to all employees in an organization and is primarily aimed at getting employees to focus on security matters using stationary or gadgets with security slogans (e.g. Posters, pens and mouse pads) so they recognize security incidents and respond accordingly. At the same time, “Security Basics and Literacy”, is required for those employees who are involved in any way with IT systems which, in today’s environment, includes all employees in an

organization taking into account that technology is an integral part in every organization. Training on the other hand, refers to how an employee can behave in a secure way and is achieved through continued teaching of security skills to groups involved with IT systems. Finally education addresses the need of information security personnel to perform complex multi-disciplinary activities along with the skills needed for IT professionals to enhance security knowledge and to keep pace with evolving threats and technology changes.

Information security surveys, government agencies and many researchers have provided feedback concerning information security awareness initiatives and why they are required. The common key point of their argument is that all users of an organization should be aware of information security policies and apply good security habits, when applying their everyday duties (National Institute of Standards and Technology (NIST), 2003; Schlienger and Teufel, 2003).

Research has determined that most information security incidents are the result of user error or negligence (McIlwraith, 2006; Ponemon Institute, 2012a) which represents a common data security breaches area often overlooked by many organizations. It refers to organizational employees who do not seem to understand the risks associated with the use of information technologies.

Information security awareness initiatives are considered a way of raising employee security consciousness along with making them aware of the consequences of their actions. Security breaches that are the result of negligent or malicious employees or other insiders are more than two-thirds of the incidents that occur today as opposed to the threats from viruses, hackers, technology failures, acts of nature, fraud attacks and spam (external threats) (Ponemon

Institute, 2012b) making the creation of awareness among employees about data protection activities a top recommendation.

Based on research studies information security awareness approaches can be classified into two main categories. The first category considers security awareness not as a form of informative or informal training but as a means of attracting end users' attention to IT Security issues. This has a final goal of responding accordingly to threats or motivating employees to develop the necessary security habits in order to protect the IT system (Katsikas, 2000; Hansche, 2001a). The goal of this approach is to create sensitivity concerning the threats and vulnerabilities of an information system and also remind employees of the need to protect the information they create, process, transmit and store. (Hansche, 2001a). In such cases, awareness activities are usually addresses to a broad audience and learners are considered as passive recipients of information. As such, the knowledge that is gained from such activity is usually not retained unless the activity is repeatedly exercised.

The second category refers to IS security awareness in the way that users have an understanding of IS security and optimally are committing themselves to it. This approach focuses on the concept of information security culture. Security culture is considered a subset of corporate culture which also describes what the organization and its employees must do. It usually starts with the top level management where it includes what senior executives should do to influence proper employee behavior and increase information security compliance, and continues downwards the hierarchy. Policies (e.g. Information Security Policy) are usually issued and authorized at this stage. Then the concept continues with educating personnel about information security in order to ensure that employees

act according to the management's wishes so company information is properly protected (Whitman and Mattord, 2004; Thomson et al., 2006). As a result of that, as users' IS awareness increases and improves, their behaviors and habits change thus causing them to secure organizational resources (Adams and Sasse, 1999; Martins and Eloff, 2002).

In respect to information security awareness, Puhakainen (2006) suggests a three step theory for improving users' security behavior:

1. IS security awareness training.
2. IS security awareness campaigns and
3. Punishment and reward.

The goal of IS security awareness training is to achieve behavioral improvements that are persistent across the organization. This can also include measurable indicators which verify that users' security behaviors have been improved such as decreased number of password compromises as a result of social engineering attempts.

However, because changes in behavior are not always easy to measure, other methods in order to gather data on the impact of awareness training are applicable. One method that can be used is to interview users or conduct focus group discussions between user groups that had attended IS awareness training in order to determine whether training has had any impact on their motivation, attitudes and behavior. Another method is to use surveys that have a goal of measuring the effectiveness of awareness training using a Likert-scale.

Similarly as with training, campaigns also aim to improve the attitude and behavior of users towards compliance with IS security policies and directives. However, there are differences between *awareness training* and *awareness campaigns*. On one hand, training has a goal to provide opportunities for goal-directed learning through the aid of instruction. It also includes the teaching of essential skills and knowledge in order to comply with IS security instructions and policies. On the other hand, campaigns are considered as a means to persuade users through interactive lectures or discussions to reach an understanding and agreement which eventually will lead to compliance with information security instructions (Puhakainen, 2006).

5.3 The Information Security Toolkit

The following section will continue by introducing the theory behind the development of the information security toolkit. It will start by presenting theories behind knowledge creation on which the toolkit will be based, determine the toolkit requirements and describe the elements of toolkit development from an information systems perspective.

5.3.1 Toolkit Requirements

The purpose of the proposed toolkit is to help people raise their level of awareness concerning information security. The toolkit will be the basis for general technology users to understand the challenges associated with secure use of information technology and help them assess their current knowledge, identify lacks and weaknesses and acquire the required knowledge in order to be competent and confident users of technology. The toolkit rationale is mainly derived from the following facts:

- Wide adoption of information technologies the last ten years has also changed the profile of end users who use this technology. Most end users operate all aspects of computer systems as well as critical data. This has brought great challenges in the area of information security forcing organizations to consider relevant approaches that integrate not only technology and processes but also people and the need to educate them on everyday issues concerning information security.
- There is a need for embedding information security in our society. The increasing number of individual home users represent a significant weak point in an effort to achieve an appropriate information security level and awareness raising methods should take into serious consideration the home user. Home users should be motivated to take the necessary security precautions in order to secure their own computer and the Internet in a home setting.
- Existing awareness raising efforts by representative websites although they provide a wealth of resources in various formats, they do not follow a structured learning framework. In most cases material is presented in an unstructured way without clear guidance on the steps or the sequence of topics someone must follow in order to have an overall idea on how to get prepared so awareness for online safety issues is assured. At the same time this unstructured approach does not guarantee neither coverage nor retention of topic knowledge.
- Awareness raising initiatives by institutions of higher education focusing on the development of a security aware workforce although promising, still lack the appropriate attention. In fact research conducted has indicated that there is a lack of sufficient information security knowledge for higher

education students when they enter higher education, which does not significantly improve through their engagement in normal university studies.

The aim of the toolkit will be to:

- Establish a structured approach so an awareness program adds value to the organization/individual and at the same time make a contribution to the field of information security.
- Provide the means so existing user knowledge is measured, giving an insight on where security knowledge is lacking through guidance on further knowledge creation.
- Provide an approach that people can use in a modular fashion, so that security knowledge and skills can be built up over time.
- Include efficient methods of presentation and interactivity so that participants are more engaged so an appropriate level of knowledge retention is achieved.
- Provide a web-based system that the user will be able to access it from anywhere by using minimal information technology resources.

The following sections will focus on the design of the toolkit from an information systems perspective taking into account the requirements described previously.

5.3.2 Knowledge Types

In modern organizations, individuals play a vital role in knowledge creation. Individuals create and share knowledge with each other and as a result, knowledge grows through a continuous and dynamic process.

Nonaka and Takeuchi (1995), propose a model (called the SECI model) for the organizational knowledge creation process in order to understand the dynamic nature of knowledge creation and to manage such a process effectively. The model is about continuous transfer, combination and conversion of different types of knowledge as users practice, interact and learn. According to that model, there are two types of knowledge which are both needed to explain organizational learning: (1) tacit knowledge and (2) explicit knowledge.

Tacit[5] knowledge, refers to a form of knowledge that is personal and is based on individual experiences, ideas, beliefs and understandings. It is highly subjective and is the basis for organizational knowledge creation. So, in terms of security behavior, tacit knowledge is considered as informal, undocumented or improvised actions performed by personnel as part of their everyday duties in respect to the use of information systems.

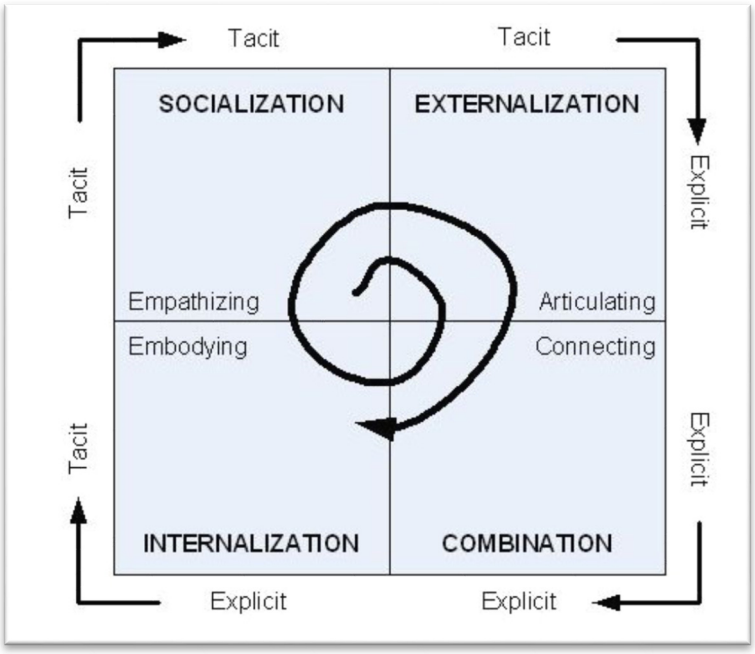


Figure 27: The SECI model by Nonaka and Takeuchi (Nonaka and Takeuchi, 1995)

[5] Tacit refers to something that is understood or implied without being stated (Oxford University Press . 2014).

On the other hand, explicit knowledge, is the knowledge that is formal and documented that leaves no room for confusion or doubt. Examples include organizational policies, manuals and directives. Western approaches to knowledge management mainly focus on explicit knowledge while Japanese approaches emphasize tacit knowledge. However, Nonaka and Takeuchi (1995), state that these types of knowledge are not separate but actually complement one another. The development of both tacit and explicit knowledge and also the interaction between the two is essential for an organization that wants to achieve change. Thus in an organization, the key to knowledge is the conversion of tacit knowledge to explicit knowledge.

The theory proposed by Nonaka and Takeuchi is based on four modes that comprise the continuous and dynamic interaction between tacit and explicit knowledge in order to achieve the creation of knowledge. The modes that identify existing knowledge and convert it into new knowledge are as follows:

- (1) Individuals among a group share tacit knowledge.
- (2) Tacit knowledge becomes formal (explicit) through the formulation and dissemination of appropriate policies.
- (3) Explicit knowledge is transferred to the individual. In this process individuals absorb explicit knowledge and convert it into tacit knowledge. This can be achieved through simulations and/or training activities.

The cycle then starts again from stage 1 in an infinite loop.

5.3.3 Toolkit development

The work carried out by Nonaka and Takeuchi can be used to explain the process of successful security awareness raising effort. The learning path in an organization and the four cyclical stages described above can be used to explain how awareness training can lead to appropriate security behavior and how the

development of an information security skills toolkit can help raise awareness that will lead to acceptable information security behavior.

This research proposes the development of an Information Security Toolkit in order to achieve appropriate information security behavior. In general, users who receive training are expected to demonstrate a more secure behavior than users who do not receive training (Puhakainen and Siponen, 2010). Since it has been proved that employees are often the greatest source of security breaches mostly as a result of ignorance or negligence, it is believed that the toolkit will help employees conveying explicit knowledge of security policies and appropriate behaviors thus converting it into tacit knowledge. The four modes theory explained above is put into context as follows:

(1). Employees undergo information security pre-testing in order for their security level to be measured and appropriate training (if needed) to be proposed. At this stage the tacit knowledge of the individual is measured.

(2). Users undergo security awareness training on areas that weaknesses have been identified into (1). This will be in the form of security awareness material where users will be introduced to correct and incorrect security behaviors. At this stage the security message is made explicit to the users.

(3). Since explicit knowledge needs to be made tacit to the users, after the material has been presented, users take a short test to measure to what extend the message has been internalized (4).

(5). The actual behavior of participants is measured to examine whether their security behavior has changed as a result of their exposure to the security toolkit.

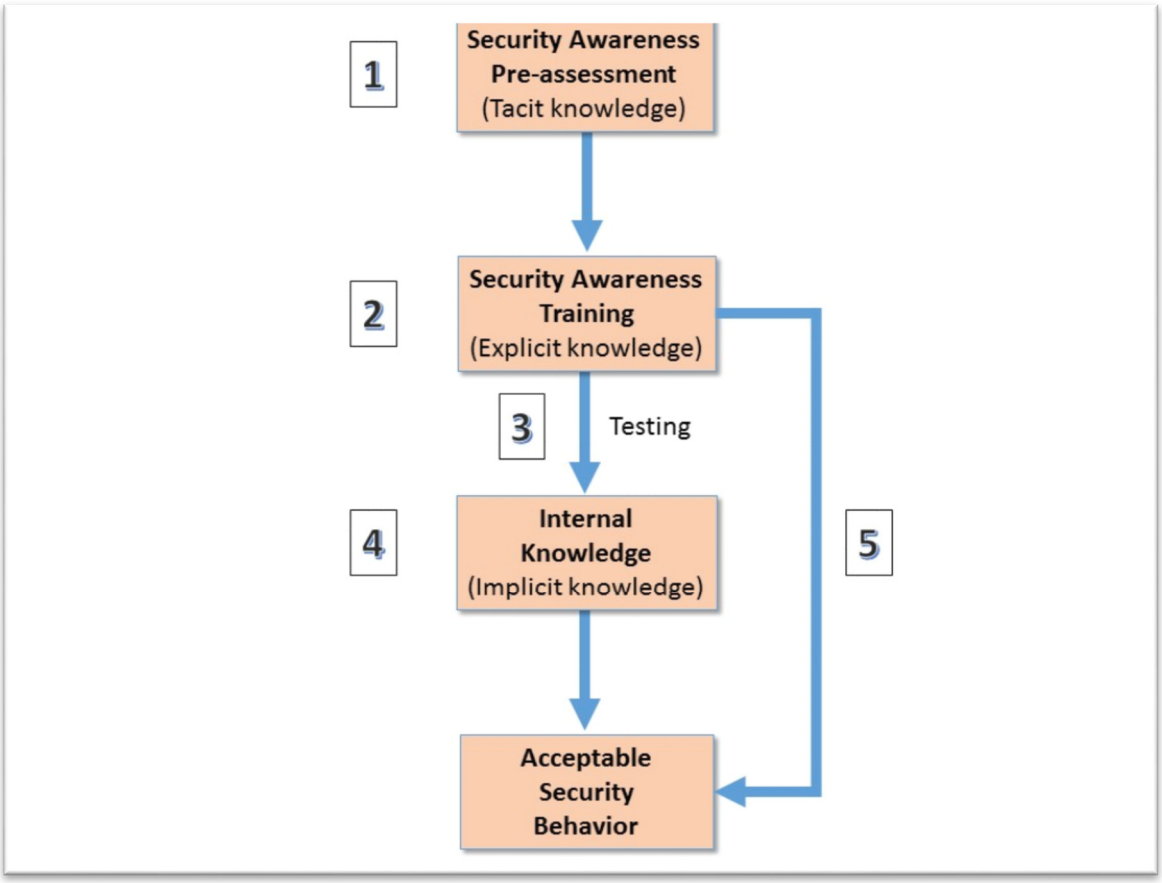


Figure 28: Application of Nonaka's and Takeushi's theoretical model in the security toolkit

The development of learning materials that are effective and consist of either instructor led or e-learning components require an understanding of basic learning principles and theories. There are a number of learning theories, and behaviorism, cognitivism and constructivism are considered the most common ones.

- Behavioristic learning involves one-way communication via reading or listening without the opportunity to reflect on the information received. Within the behaviorist view of learning, the "teacher" is the dominant person in the classroom (Behaviorism, 2014). In the context of IS security training the use of behavioristic methods involves the teacher presenting information security concepts (policies, threats, prevention measures, etc.) to learners through the use of different audiovisual means without paying

attention to learning processes or problem serving coursework (Karjalainen et al., 2013). According to behavioristic learning, in an effort to change IS security beliefs and reactions, the learner's progress is monitored and its desired behavior is strengthened through positive reinforcement, rewards or punishments.

- Cognitivism is learner centric and looks beyond behavior in order to explain the learning process. In the information security field, cognitive learning involves reasons for compliance with IS security procedures through the use of examples in regard to threats to information assets. According to cognitive learning theory factors such as repetition and personal relevance may improve the effectiveness of training (Puhakainen and Siponen, 2010).
- Finally according to constructive learning, construction of new ideas by users is based on how they interpret past experiences. In other words, existing user experience is the driving force of creating user own knowledge. In the context of IS security training, constructive learning is applied through discussions with employees concerning their experiences, attitudes and behaviors towards security policies. Through these discussions, employees form their own thoughts and knowledge concerning how to be secure and why it is important to be secure (Jenkins et al., 2012).

The information security toolkit, tries to combine the behavioristic and cognitivist learning theories described above in order to achieve the most effective learning outcome. More specifically according to the behavioristic model, the toolkit presents different information security concepts through the use of different audio visual means (e.g. text, graphics, and hyperlinks). Following the behavioristic

approach the learner's progress is monitored at the end of each unit of the toolkit. Following the cognitivism approach, the toolkit will emphasize why there is a need for compliance with information security procedures by using meaningful examples in regard to threats to information assets.

5.3.4 E-Learning Concepts and Delivery Approaches

E-learning or electronic learning typically refers to any type of learning that is facilitated and supported through the use of information and communications technology. The term therefore covers the use of computers and technology as a vehicle for exchanging knowledge within teaching and learning. This form of learning is conducted via the Internet, intranet, through a local network or by using digital storage media such as CD/DVD ROM.

E-learning can be classified as synchronous and asynchronous. Synchronous e-learning is taking place in real time through electronic means with a live instructor. The learning experience is similar to that of a regular classroom, except that there are no geographical barriers and learners can take courses anywhere in the world as long as a computer with decent Internet connection is available in order to use audio and video conferencing tools. Some of the tools that are associated with synchronous e-learning are the following:

- Virtual Interactive whiteboard: although it may be platform specific, the center of all synchronous e-learning tools is the virtual whiteboard where the instructor can display presentation slides. At the same time instructors and learners can collaborate through it in real time.

- Chat and instant messaging: through chat and instant messaging, students can easily check who is online and available for direct communication.
- Video: although the availability of the instructor through a video feed is not considered an absolute necessity for a successful synchronous e-learning course, still active engagement through video along with all the expressions and visual clues of a face-to-face conversation can be beneficial to the learner.
- Application and screen sharing: screen and application sharing is gaining a lot of popularity as a tool used by people who collaborate over the Internet. In fact the training needs of organizations operating in geographically dispersed offices can be facilitated by such a feature since instructors can share whatever is on their screen and provide a better learning experience to the learner.
- Breakout rooms: it is widely accepted that students learn best when they engage and interact with others in small groups where they are able to discuss class material. Breakout rooms, is a common feature among most e-Learning tools where online instructors – just like the physical classroom – can divide up students for small group work.
- Online polling: online learning involves the active engagement of the learner through anonymous quick answers to a series of questions that can be used as a basis for further class discussion. Polling features allows instructors to poll participants at any time using different types of polls.

The real value of synchronous learning has to do with the presence of a real instructor and the ability to communicate with other participants in the course but,

at the same time, it requires learners to virtually attend the course at a specific time.

On the other hand, asynchronous e-learning is self-paced. Many adult learners are busy and find synchronous e-learning impractical due to day and time constraints. Instructional designers, in order to target this problem and at the same time target a wider audience, began recording synchronous e-learning courses or prepare learning material in such a way so it is available to learners that are unable to attend live sessions. This is where asynchronous e-learning originates. Some of the most commonly used tools for asynchronous e-learning involve blogs, wikis, forum and webcasts. At the same time most modern learning management systems (LMS) like Blackboard, Moodle, Sakai and Desire2Learn usually integrate all these tools under a common platform.

In terms of asynchronous e-Learning, the most popular delivery methods are Computer-Based Training (CBT) and Web-Based Training (WBT). CBT is a form of delivery in which learners are engaged in the learning process by taking training courses on their computer. CDs or DVDs are the most common learning media for such asynchronous delivery. On the other hand, WBT courses operate on the Internet and can be used for both synchronous and asynchronous delivery.

Although learning that takes place totally online is a popular educational approach mainly for increasing knowledge, developing cognitive skills and cost effectiveness, it may not be very appropriate for concepts where real practice is required. Teaching skills that change learner's attitudes and behaviors can be effective through e-learning if complemented by appropriate simulations and games. This is where the blended learning approach can play an important role.

Blended learning – also referred to as “Hybrid Learning – combines traditional face-to-face instruction with online learning.

The information security toolkit will be based on the asynchronous model of learning, allowing the participants to complete the whole or parts of the toolkit at their own pace. The web capability of an HTML5 enabled learning management system can be used as a form of delivery. In order to enhance learner’s skills at areas where real practice is required, the toolkit will be complemented by appropriate simulations in order to ensure that a change in learner’s behaviors is positively achieved.

5.3.5 Elements of Toolkit Design

Designing successful e-learning courses is closely related with theories and studies on how people learn. It began with Pavlov’s studies on classical conditioning where learning occurs when a conditioned stimulus is paired with an unconditioned stimulus. A highly simplified version of Pavlov’s principles was included in the works of the American psychologist John Watson (1920). Then Skinner (1965), an American psychologist and behaviorist, built upon the previous studies and developed the behaviorist approach to learning. Skinner looked at the learning process in the opposite way, investigating how learning was affected by stimuli presented *after* an act was performed. He found that certain stimuli caused the subject to repeat an act more frequently. He called stimuli with this effect the "reinforcers". Reinforcers can be:

- Positive: when a behavior is followed by the presentation of a positive stimulus such us rewarding students for completing a task on time, which can lead to an increase in behavior.

- Negative: when the behavior is followed by the removal of an unpleasant stimulus, such as preparing for an exam in order not to get a failing grade, which can again lead to an increase in behavior.

At the same time, he found that certain stimuli caused the subject to decrease an act at least temporarily (he called stimuli with this effect the “punishment”) or forever (he called stimuli with this effect the “extinction”).

There are many models available that can help instructional designers in their effort of building a successful e-learning course. There is no approach that is universally accepted by all designers since most of them decide to choose whatever technique best suits the needs of the course’s audience and content.

The ADDIE model is considered the most traditional model for instructional design and all other models are derived from it. Its name is derived from its five phases (Branson and Rayner, 1975):

- Analysis: in this phase, the instructional designer identifies the learning problem, the goals and objectives and the audience’s needs based on existing knowledge.
- Design: in this phase the course objectives are written along with the structure and the sequences of the course. This includes detailed storyboards, prototypes, the look and feel, graphic and user interface design.
- Development: involves the actual creation of the course based on the specifics defined from the previous phase.
- Implementation: in this phase the course is delivered to its audience.

- Evaluation: in this phase the effectiveness of the course is assessed by measuring the participant's learning and retention.

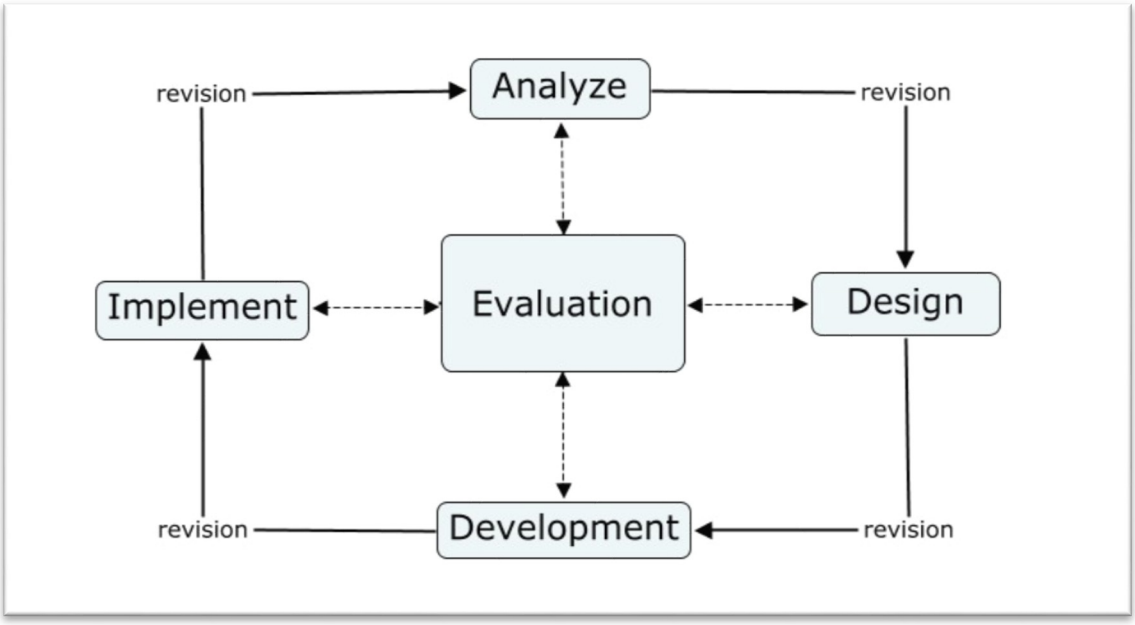


Figure 29: The ADDIE model for instructional design (Forest, 2014)

The Dick and Carey Systems Approach model (1996), follows a sequential approach similar to the ADDIE model. This is the favored model by many curriculum developers in higher education since it assumes the learner is active in the learning process and it incorporates the learner's needs, skills and learning context in the course design. According to this model instruction is broken down into smaller components and is divided into ten sections:

- Instructional goals: what is the goal of the instruction and what will the learners be able to perform upon completion of the training program.
- Instructional analysis: what skills will be involved in order to achieve the desired outcome?
- Identify entry behaviors: analysis of learners in terms of skills, attitudes, prior knowledge and motivation.

- Performance objectives: the needs and goals of instruction are translated into goals and specific objectives.
- Criterion referenced tests: develop instruments for assessment.
- Develop instructional strategy: what will be the instructional activities that have to be followed in order to achieve the required learning outcome (e.g. Presentation of information, practice, testing, etc.).
- Develop and select Instructional material: what type of instructional materials will be used (e.g. online media, printed media, etc.).
- Formative evaluation of instruction: identify areas that the instructional materials are in need of improvement.
- Revise instruction: revision of instruction after formative evaluation to identify problems and difficulties for the learners.
- Summative evaluation: evaluate the system as a whole, assess the effectiveness of instruction and whether the desired results were achieved.

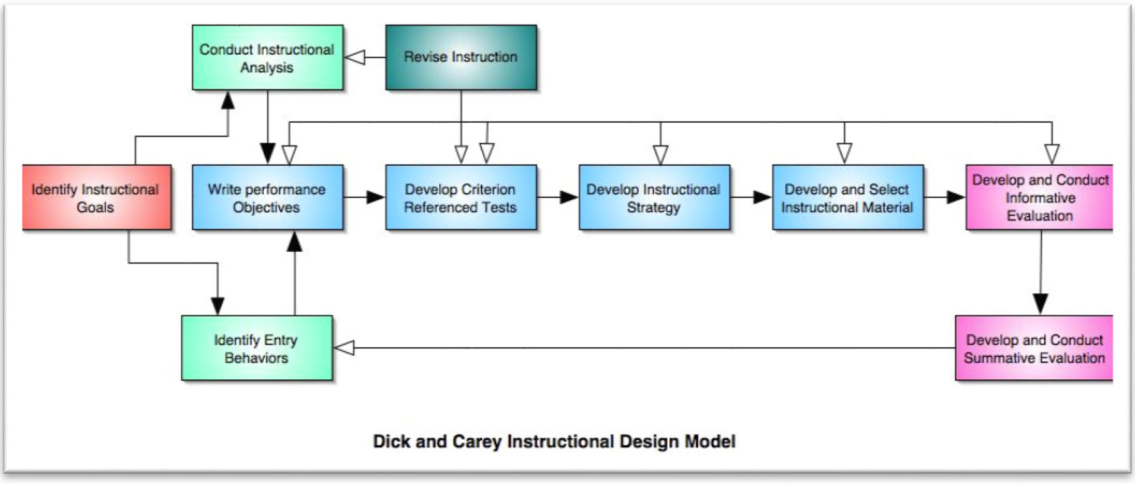


Figure 30: The Dick and Carey Systems Approach model (Dick and Carey, 1996)

According to this model, components are executed in parallel as opposed to the linear nature of the ADDIE model, and instruction is addressed as an entire

system focusing on the inter-relationship between context, content, learning and instruction. All components interact with each other and work together in order to bring the desired learning outcome.

The Rapid Instructional Design model developed by David Meier (2000), addresses the idea of accelerated learning and is considered ideal especially for learning projects with tight deadlines, limited budgets and constantly changing content. According to Meier traditional instructional design models are too time consuming and his theory is based on the fact that people learn more from applications with feedback rather than from presentations, so training courses should be focused activity based material rather than media-heavy material. Although it is commonly agreed that the Rapid Instructional Design model makes courses more interactive and engaging, it does not incorporate the analysis and evaluation phases which are considered crucial in the development of a successful e-learning course. The phases that are involved in this model are the following:

- Preparation: arouse learner interest and state learning goals in order to motivate learners.
- Presentation: encounter new knowledge and skills by incorporating interactive presentations and discovery activities.
- Practice: establish new skills and knowledge for the learner by incorporating games, hand-on activities and practice exercises for skill building. Provide corrective feedback to the learner at all phases.
- Performance: apply new knowledge and skills to real work situations.

The toolkit will be comprised of the following components:

1. The assessments repository which will include all databases that will story quiz questions to be used in:
    a. The pre-assessment stage of the toolkit where existing knowledge of the participant will be assessed.
    b. The post assessment stage of the toolkit where learning modules have been completed and participant's acquired knowledge should be assessed.
2. The learning unit(s) component which consists of:
    a. The front-end unit which is the actual presentation of the eLearning component of the toolkit accessible through the web.
    b. The back-end unit which contains the actual design and content of each learning module and can be used by toolkit administrators to add/remove or customize content packages based on information security learning materials.
3. The users component which consists of:
    a. End-user who actually use the toolkit in order to assess their existing knowledge through the assessment stages and raise their awareness level through the main eLearning components.
    b. Toolkit administrators who are responsible for managing module content and assessment repositories.
4. The user profile database which will contain the personal information of participants (e.g name, date they started their engagement with the toolkit, educational background, preliminary IT knowledge), along with toolkit modules completed and assessment results.

From an information systems perspective, the toolkit development is based on the ADDIE (Analysis, Design, Development, Implementation and Evaluation)

model, and comprises of the previously mentioned design steps. Although many critics of this model argue that it is too linear and inflexible, it still remains as the most popular model among instructional designers and most of the current instructional design models are variations of the ADDIE instructional design model. As previously described, in the ADDIE model, each step has an outcome that "feeds" into the subsequent step in a recursive and continuous process as long as there are updates on the learning materials. The five steps of the model, apply to the toolkit design as follows:

1. Analysis phase: this phase is responsible for the collection of information on the user in order to identify his existing knowledge and skills. The user is expected to provide personal information to the system plus information on existing security knowledge (e.g. recently attended a security course or awareness campaign). The objective of acquiring this information is the creation of a user profile database which will contain all the personal information of participants (e.g. name, date they started their engagement with the toolkit, educational background, preliminary IT knowledge), along with toolkit modules completed and assessment results. This information will be maintained by the toolkit administrators who in turn will be responsible to update the toolkit content as awareness needs change. Also user profile will be amended accordingly as the toolkit engagement continues to include modules completed, assessment results and maybe re-assessment and knowledge refreshment plans. The concept of the user profile has not been fully addressed in the current toolkit prototype as it does not directly relate to the aspects of the current research under investigation.

2. Design phase: this phase contains the learning path proposed to the user by the toolkit system as a result of the information obtained at the previous phase. The user needs to take a series of pre-assessment tests, in order to measure his familiarity with specific information security topics and determine whether additional training is needed. Although pre-assessment cannot be considered a completely accurate observation, it can save users' time by providing them guidance on which topics their knowledge is considered sufficient so no further training is needed. Although part of the design phase, this procedure has elements that still belong to the analysis phase since information on users' pre-existing knowledge is still to be determined. After the pre-assessment results have been obtained, the user will be presented with the learning packages that has to complete. The design phase continues with the toolkit modules learning objectives, user interface design, and content creation taking into consideration the participants' learning styles.

   A learning style is an individual's pattern of acquiring and processing information in a learning environment. Each person prefers a different learning style and technique. To better process new information a person must hear it, see it or try it. Most learner's preferences fall into one of these categories. By understanding their own learning style, individuals can use techniques better suited to themselves. This improves the speed and quality of your learning. Examples of learning styles include the following:

   - Visual Learning Style: these learners learn best by seeing. In order to satisfy visual learners, instructional designers should include images, videos, slides and demonstrations in their courses.

- Auditory Learning Style: auditory learners understand and retain information by hearing it.
- Verbal Learning Style: learners prefer using words both in speech and writing.
- Kinesthetic Learning Style: learners learn best by doing. To accommodate these learners, instructional designers should consider hand-on activities such as games and experiments in their courses.
- Mathematical Learning Style: learners prefer using logic, reasoning and systems.
- Interpersonal Learning Style: learners prefer to learn in groups with other people.
- Intrapersonal Learning Style: learners prefer to work alone and use self-study.

There is no scientific evidence that shows that people have a fixed learning style or at least a style that helps achieve a better level of learning and retention. However providing students with multiple ways to learn content, has been shown efficient in improving student learning. (Hattie, 2011). There are many tools available on the web that may help a learner determine the best learning style to be used for maximum retention.

At the same time, differences in age or culture may result in significant differences in the preferred learning style. While all people are able to learn through a variety of media different generations many have different preferences in learning. (Cekada, 2012).

An instructional designer is usually presented with the challenge of creating a successful learning experience that is geared towards all generations. Although it is almost impossible to create a learning experience that would close the gap between generations, there are certain ways and approaches that if followed would help build courses that satisfy most learners' needs.

Generational Learning Styles

Traditionalists	Baby Boomers	Generation X	Generation Y or Millennials
• Ages 66 and over • Prefer learning through lectures • Displike role-plays and games	• Ages 47-65 • Like to learn through lectures • Enjoy small group activities	• Ages 29-46 • Prefer eLearning to traditional learning • Enjoy experencial learning activities • Prefer self-studying	• Ages 18-28 • Prefer eLearning to traditional learning • Prefer hands-on learning • Prefer learning through social networking tools such as wikis, blogs, podcasts and mobile applications

Table 23: Generational Learning Styles (Arshavskiy, 2013)

Understanding the learning styles is one way to cover the needs of most generations of learners. According to studies, traditionalists prefer an auditory learning approach through lectures because most of them grew up listening to the radio as the only media available for communicating information. Baby boomers, on the other hand, prefer visuals and workshops because they grew up watching TV. They like an environment where they are challenged and can share experiences and prefer to utilize books, manuals and PowerPoint (Arshavskiy, 2013). Learners who fall

under the Generations X and Y have a lot of similarities in the way they learn and retain learning. They both prefer to learn through exploration, and for them a fun learning environment which is interactive and media centered is the most suitable for achieving retention. Because both grew up playing games, writing emails and using different types of social media tools, they prefer kinesthetic and visual learning styles (Cekada, 2012).

As an instructional designer designs and creates courses, they should consider incorporating a variety of activities that utilize all learning styles. Further to that they should focus on a blended approach by mixing learning strategies that appeal to both younger and older generations.

The information security toolkit as an awareness raising method is addressed to the general user population and its objective is to establish the security knowledge and skills that all IT users need to acquire in order to be competent and confident users of technology. For that reason, effort was made to create a learning experience that is geared towards all generations. Taking into consideration the difficulties that such an effort may impose, different learning approaches were used in the toolkit in an effort to satisfy the learning styles preferred by all generations. Voice narration was used throughout the eLearning unit parts in order to satisfy the learning approach of traditionalists plus use of graphics and hypermedia in order to support the approach of baby boomers. The ability of the learner to expose himself to the toolkit through a web interface satisfies the requirement of generation X and Y groups for an interactive and media centered environment. At the same time, the toolkit through its

HTML5 compatibility is accessible through mobile devices and can be integrated into modern LMS systems.

3. Development phase: this phase contains the creation and assembly of the contents created in the design phase. Taking into consideration the need for developing the toolkit in a fast and effective fashion, the design of the toolkit prototype was based around the Rapid Instructional Design model. Taking into account that the toolkit should allow for fast and easy updates in order to adapt with the constantly changing scene of information security, this method is considered as the best solution based on the availability of suitable development tools today, the ease of their use and their wealth of features for engaging and interactive design.
4. Implementation phase: this phase is where actually learners engage themselves with the toolkit including pre and post-assessments and learning paths as they have been identified by the toolkit administrators. Participants should be able to access the toolkit online at their own pace. However, each participant needs to complete certain training packages within a specific timeframe based on their level of importance. This classification will be determined by the training administrator. Post-assessment quizzes will take place after users have completed each training package in order to evaluate their knowledge obtained from the training. Pass or failure at the quiz will automatically trigger a required update at the users' profile for the training administrator. Specifically in the case of failure, participant will have to repeat the training package and the post-assessment until he passes. Finally, a re-assessment phase may be scheduled at a specific time interval (e.g. six months) depending on

organizational policy, in order for the participant to refresh his memory and update his security knowledge with new concepts if required.

5. Evaluation phase: following the recursive nature of the model, this phase checks and ensures that the toolkit materials are up-to-date and that the learning process is effective.

5.3.6 E-Learning Effectiveness

E-learning is now considered a well-established method of instruction and many organizations and training institutes have leveraged its benefits. With more than 77% of American corporations using e-learning, it is the second most important training method within organizations (IBIS, 2013). Such facts indicate the benefits of e-learning, however, it is important to understand the key factors that drive e-learning effectiveness.

- Content and structure: content is considered the most important component of a successful e-learning piece and must meet the requirements of the learner. Structure refers to how the course is structured for e-learning. Following the ADDIE and Dick and Carey principles, the following should be considered in order for the e-learning piece to be organized and well structured:
    - Content organization: It is preferable if the course flow is broken down into small logical modules which are easy for the audience to follow and learn.
    - Use of interactive content: interactive content should be strategically placed inside the e-learning piece. Although there is no generally accepted principle on the frequency of interactive content,

a good rule of thumb is to include an interactive exercise or activity for every learning objective in a module.

- Use of pictures and graphics to present/explain concepts: proper use of graphics is important in an e-learning project. As suggested by Clark and Mayer (2011), – called the “multimedia effect”– it is better to use graphics with text rather than just text alone since people learn and retain learning when it comes from words together with pictures than from words alone. In addition, empirical evidence from the same study indicates that placing a text element near the illustration it describes, facilitates the learning process (continuity principle). Finally, there is a debate between instructional designers whether high fidelity graphics should be used instead of low fidelity ones. According to Malamed (2014), before placing a realistic graphic into an online course, it is better to think how much realism will be most effective for learning. Research points to the fact that realistic graphics are not as effective as those with reduced realism. On the contrary, low fidelity graphics require fewer cognitive resources from the learner’s part in order to transform the graphic into a simple form of crucial information. Low fidelity graphics take less time to scan and assimilate as compared to more complicated ones and as a result less time to encode the information into long-term memory. Again, as mentioned previously, the debate may argue that a learning tool which looks it isn’t professional may be off-putting to users since they may think it has less value because it looks like an amateur production. At the same time, high fidelity graphics may give a professional looking impression to a learning

tool which actually contains nothing of value to the learner. The ideal situation here is to have a learning piece that achieves its objective through a balanced delivery of its content.

- Method and platform of delivery: it is important that e-learning is delivered using a stable platform. One of the most common platforms for e-learning delivery is through the Web. The Web is an instructional technology that allows the presentation of information to be independent of medium, subject, time and place. Learning through the web can be complemented by the use of a Learning Management system.
- Learning feedback: a successful e-learning piece should have appropriate mechanisms so the learner can give and receive feedback about the knowledge being acquired. The most common method is asking learners' questions and provide measurable feedback from their responses.
- Mobile learning: mobile devices today have penetrated most markets including corporate and educational and present an opportunity for effective learning that cannot be ignored. Among all mobile application downloads, educational related ones are greater than the overall average in both free and paid downloads (IBIS, 2013). The same study aims that m-education is an important sector for distributed learning. Another study has shown that undergraduate students own at least two Internet capable devices and prefer to use smartphones for educational purposes although most of the surveyed population argued that the use of a smartphone in class is either banned or discouraged (Dahlstrom et al., 2013).

5.3.7 The Security Toolkit Implementation

The key objective behind the development of the Information Security toolkit is to establish the security knowledge and skills required for the user's everyday

exposure to information technology and at the same time enable them to be confident and competent technology users. The security toolkit as a form of awareness raising method, was developed having in mind the 'distant' or at the 'learners' pace' method of delivery. For that reason there was an effort for the learner to interact and control the learning process as much as possible through continuous feedback regarding the knowledge transfer process. Also, the structuring and presentation of the toolkit approach around key aspects of baseline security knowledge will allow them to approach the task in a modular manner. In accordance to Alessi and Trollip's (2000) approach on methods and development of eLearning, the following four activities were used in constructing the toolkit components:

(1) Presentation of Information: although the material presented by the toolkit cannot be considered new for the everyday user, it was considered necessary some presentation of even basic information security concepts to take place.

(2) Learner guidance: through interactivity the toolkit supports the learning process through suggestions and hints.

(3) Practice: possibility for the learner to practice complex tasks.

(4) Assessing Learning: evaluate to what extend learning has been achieved.

In the actual development of the toolkit, since the goal of the awareness material was to focus attention on good security practices, its main content was to inform users about a number of security topics that everyone should be aware of. According to the "Chronology of Data Breaches" (Privacy Rights Clearinghouse, 2014), from 2010-2014, more than 7M records have been reported as incidents of payment card fraud and almost 2M records have been reported as loss due to insider threat from someone with legitimate access who intentionally breached information. These numbers indicate that how to make a computer secure and

keep its data safe is still a challenge by many users. The question that had to be answered when developing the toolkit was “on what IT security topics should the general population be aware of” and how these topics are going to be presented. Publicly available information security surveys, e-mail advisories, IT security related websites, periodicals and information security surveys (referred to in chapters II and III) were used as sources for determining the toolkit material. Extra effort was made to introduce security topics through a series of real-life and everyday user experiences and examples.

The security toolkit was comprised of the following parts:

- pre-assessment,
- Main e-learning unit,
- Post-assessment.

The survey findings presented in Chapters II and III of this thesis have determined that despite the fact that many respondents perceive that they are aware of potential threats and risks, and believe they possess the necessary security knowledge, their practice does not always evidence this. Often there is a considerable gap between what user know about information security terms, concepts, measures and practices and what they actually do in reality. For example although they argue that they possess the necessary knowledge to protect their information assets, they are willing to open an e-mail attachment if it originates from a trusted source (e.g., Friend or university authority), or feel comfortable to reveal their password if they are asked to do so. At the same time they are ready to engage themselves in non-secure practices like downloading music and programs using file sharing programs or file repositories.

The objective of the pre-assessment unit is to determine the participant's knowledge on specific information security topics and determine whether additional training is needed. Pre-assessment takes place in the form of multiple choice questions which the user has to answer. In this model of the pre-assessment unit, two information security areas are covered: (1) Introduction to information security concepts where the participant's knowledge on general information security issues is examined and (2) Human Aspects of Information Security where the objective of the assessment is to examine the participant's knowledge concerning security risks that can arise by poor user choices. The objectives of both pre-assessment units are displayed on the users' screen along with the total number of questions the user will be examined on. At the end of each area examined, a pass or a failing score is presented to the participant and they have the chance to review each answer given and determine the correct answer. A summary is presented at the end of the whole pre-assessment unit. Upon completion of each pre-assessment unit, the user profile database is updated with the result of each pre-assessment.

The objective of the main e-learning unit, that normally follows the pre-assessment unit, is to introduce to participants essential everyday information security skills and at the same time help those of the participants who want to be able to protect their computers, mobile devices and data from attacks. The unit is designed in such a way in order to provide an interactive learning experience to the participant and all that is required to follow it is a basic working knowledge of computers. In this model of the pre-assessment unit, two information security areas are covered:

- Introduction to information security concepts and

- Human Aspects of Information Security.

At the end of each e-learning unit, the user is returned to the main navigation screen which indicates what part of the e-learning unit has been completed. At that point the user can take a post-assessment quiz in the form of multiple choice questions so as to assess the level of knowledge that he has gained from the previously covered e-learning part. At the end of the post-assessment quiz, a pass or a failing score is presented to the participant and also they have the chance to review each answer given and determine the correct answer. While the participant progresses with each e-learning unit, the user profile database is regularly updated in order to include module completion progress along with the results of the post-assessment quiz thus allowing important comparisons of achieved knowledge as a result of toolkit engagement. The concept of the profile database will be completely incorporated into a full implementation of the toolkit and has not been addressed here as it does not directly relate to the aspects of research under investigation.

The toolkit was developed as a web-based flash application using Articulate Storyline and can be previewed from any flash enabled web browser. The reason for the choice of software utilized for the toolkit development lies mainly with its ease of learning as opposed to other software available on the market for rapid eLearning development. The tool comes with many ready to use rich interactivity templates, contains an easy to build and use quiz component plus other tools that greatly eases the development of the toolkit (e.g. timeline, triggers, layers, sound editor, etc.). Finally, the software tool enables publishing to HTML5, allows learners to use their iPad or other similar device for viewing courses and supports

content publishing to most learning management systems under the SCORM standard.

5.3.8 Toolkit Content Areas

In determining the content areas that the information security toolkit should contain, several sources were examined and analyzed in order to reach the most important topics that will help raise the level of awareness. The topics were initially determined from the analysis that followed the two security awareness surveys presented in Chapter 4 and then were checked for validity and common areas against the following sources:

- ISO/IEC 27002:2013: resources related to the standard on how to manage information security in an organization.
- ENISA: guidelines on how to raise information security awareness.
- NIST SP 800-50: the National Institute of Standards and Technology guidelines on how to build an information security awareness and training program.
- IT Governance Institute: a comprehensive set of resources that organizations need to adopt as a foundation for good security practices.
- EDUCAUSE and HEISC: resources publically available as part of the National Cyber Security Awareness Month organized by EDUCAUSE and the Internet2 Higher Education Information Security Council.

Taking into consideration that awareness is not training, the purpose of the e-learning unit as an awareness raising method is to focus attention on security in a way that will allow the general population to recognize security concerns and respond accordingly (National Institute of Standards and Technology (NIST),

2003). For that reason and in an effort to reach a broader audience, the topics were presented in a simple and brief manner yet covering most relevant material in a concise manner. According to Plessis and Von Solms (2002), there are two approaches for implementing information security awareness programs. The approach according to which awareness programs are based on the policies and procedures already in place in the organization, and the one that follows a generic approach and develops awareness programs that would not be dependent on an organization's policy. Because the focus in today's environment apart from educating employees is to also change their behavior and cultivate the appropriate information security culture, the e-learning toolkit should include aspects other than just organizational policies. Such aspects include basic information security concepts, why it is important to deal with security in today's environment, threats and vulnerabilities along with information about the types of attackers, human aspects of security, etc.

In determining what areas and specific topics the e-learning part of the toolkit should include, and in accordance to NIST Special Publication 800-50, an information security program should be focused on all the end users within an organization (National Institute of Standards and Technology (NIST), 2003). Also the security risks home users are facing have to be taken into account. In order to determine an appropriate security baseline that general users ought to be aiming towards, it is necessary to appreciate the nature of the technology they are using. In today's computing environments, end-users work with networked computers, storage devices and network infrastructures either at home or as part of an organization. They may even be working at positions that handle confidential or critical data or even be part of an IT department. At the same time NIST Special Publication 800-16, suggests that all individuals who use computer

technology or products similar to it, must know IT security basics and be able to apply them, regardless of their profession or job responsibilities (National Institute of Standards and Technology (NIST), 1998). In addition, NIST SP 800-50 suggests 27 information security awareness topics including password usage and management, protection from malicious code, e-mail and attachments, guidelines on using the web, data backup and restore, social engineering and others that should be included in any developed security awareness material addressed to all users in an organization (National Institute of Standards and Technology (NIST), 2003).

According to COBIT Security Baseline (ITGI, 2007), home users can be exposed to information security risks mainly due to:

- Using the Internet without being aware of the dangers associated with it.
- Installing software from untrusted sources that may contain security weaknesses.
- Using out-of-date operating systems, security software and application software.
- Being exposed to attacks from viruses, spyware, spam and phishing that may result to information and identity theft.

According to the same publication home users are divided into two categories, those with no technical knowledge and those who may be considered more advanced but not necessarily aware of all the security issues. Specific security precautions in the form of a summative list is provided to guide this wide range of individuals.

The topics and areas of attention in the list provided by ITGI for home users is in complete accordance with the ENISA report on how to raise information security awareness. More specifically topics like e-mail and electronic communication, passwords, security updates and patches are very important not only to businesses but also to individuals (ENISA, 2007; ENISA, 2010). Overall, most respondents of the report (Figure 31) agree that the following security areas are very important for staff to understand:

- Human aspects of security (Passwords, social engineering, social networking),
- System security (Malware, system defenses and recovery).
- Application security (use of internet, risks and defenses).
- Mobile device security (mobile device threats, attacks and defenses).
- Workplace and physical security (Out of the office security, clear desk policy, incident reporting).

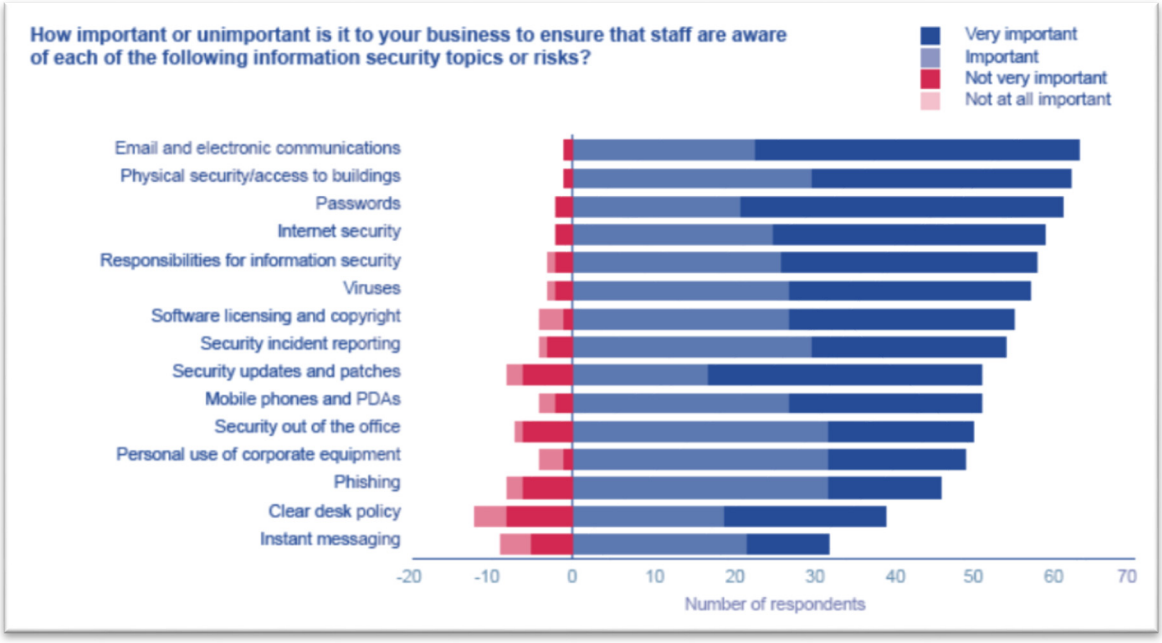


Figure 31: Importance of information security topics and risks (ENISA, 2007)

The EDUCAUSE information security awareness video & poster contest (2013) which was held as part of the National Cyber Security Awareness Month identified the most popular cyber security topics created *by* college students *for* college students. Through a series of posters, short videos and training videos, these topics are around themes like cloud security, antivirus, importance of backups, Internet security, passwords and workplace security.

The ISO27002:2013 standard recognizes that the adoption of an information security management system is a strategic decision for every organization(International Organization for Standardization (ISO), 2013). The standard describes how to manage information security in a company and among others a training and awareness plan is required in order to make employees aware about the benefits of information security and business continuity. Security awareness topics include general concepts about information security and its importance, the human factor, physical security, password use and guidelines, Internet use, e-mail use, etc.

The following table maps different information security themes and how they relate to different information security sources.

		Sources					
Key Theme	**Area**	**ENISA**	**NIST 800-50**	**Plessis & von Solms**	**ISO 27002:2013**	**EDUCAUSE & HEISC**	**IT Governance Institute**
General Information Security concepts / InfoSec Importance	Introduction to Information Security	√	√	√	√		√
Email and electronic communications	Human Aspects of Security	√	√		√	√	√
Physical security / physical access / Access Control	Workplace Security	√	√		√		√
Passwords usage and management	Human Aspects of Security	√	√		√	√	√
Internet security	Application Security	√	√		√		√
Viruses	System Security	√	√	√	√	√	
Software licensing / Allowed / Supported software	Workplace Security	√	√				√
Security Incident reporting	Workplace Security	√	√		√		√
Security updates and patches	System Security	√	√		√	√	√
Mobile devices / Handhelp device security / Laptop security / Encryption	Mobile Device Security	√	√			√	√
Out of office security	Mobile Device Security	√	√		√	√	√
Personal use of corporate equipment	Workplace Security	√	√				√
Phishing	Human Aspects of Security	√				√	√
Clear desk policy	Workplace Security	√			√		√
Instant messaging	Human Aspects of Security	√					
Shoulder Surfing	Human Aspects of Security		√				√
Policies	Workplace Security		√	√	√		√
Social Engineering	Human Aspects of		√	√		√	√
Web Usage	Application Security		√		√	√	√
Data Backups	System Security/Workplace Security		√				√
Individual accountability	Workplace Security		√	√	√	√	√

Table 24: Information Security key themes according to different sources

Based on the above considerations, the topics/units that are selected for inclusion in the e-Learning units are considered in more detail in the sections that follow.

Information Security Content Areas

Unit I: Introduction to Information Security

- Why it is important to deal with security.
- A brief and easy to understand definition of information security along with its components including examples.
- The need for information security.
- The consequences of poor security.
- Presentation of commonly used information security terms and definitions.
- The attackers along with their characteristics.
- Areas that need protection.

Unit II: Human Aspects of Security

- Human error: the largest information security risk.
- The use of passwords.
- Social engineering concepts and risks.
- Social networking concepts and risks

Unit III: System Security

- Attacks on systems using malware
- Types of malware
- System defenses

Unit IV: Application Security

- Internet and WWW basics
- Internet security risks (mobile code, cookies, P2P, email risks).
- Internet defenses (browser security, content filtering, identifying secure sites, email defenses)

Unit V: Mobile Device Security

- Mobile device threats and attacks
  - The nature of Wi Fi networks
  - Attacks on Wi Fi
  - Attacks on mobile devices
- Mobile device defenses and best practices
  - Home Wi Fi Security
  - Public network security
  - Mobile device security
  - Best practices

Unit VI: Workplace Security

- Restrictions to physical access
- Restrictions to data access
- Security policies
- Crisis preparedness and incident reporting
- Disaster recovery

Table 25: Information Security Toolkit content areas at a glance

Without taking into consideration the existing knowledge of users, all units are expected to play a specific vital role in an effort to raise information security awareness. Unit I – Introduction to Information Security is considered an excellent starting point for any type of user since it defines the concept of information security and relates it to the protection of valuable assets against unavailability, loss or damage. This unit sets the necessary background and framework for the topics that will follow in the toolkit. The rest of the units are considered of equal importance and based on the existing knowledge of the user may be completed

in any particular order although following the prescribed order is strongly recommended.

5.3.8.1 Unit I: Introduction to Information Security

The main objective of this unit is to stress the challenge of information security and explain its importance. Taking into account that information is a valuable asset for any organization or individual it needs to be protected in a proper way. The world has moved from an era where protection from computers and technology devices by invisible foes has dominated our everyday lives as opposed from physical attacks (Ciampa, 2014). With the rise in cybercrimes, (such as hacking, data thefts and virus attacks), no one can ignore the importance of information that is valuable to the company. Although all computer users have heard about attacks that can threaten their computers the majority of users remain unsure about how to actually keep their computer and data safe. At the same time, there is a huge demand for information security training preferably conducted at an early pre-employment stage. As a result, the objective of this unit is to define information security along with its purpose and challenges in respect to today's environment. Aspects like the nature and source of information security attacks along with the areas that need protection will be covered. Specific unit contents will include:

- Why it is important to deal with security.
- A brief and easy to understand definition of information security along with its components including examples.
- The need for information security.
- The consequences of poor security.

- Presentation of commonly used information security terms and definitions.
- The attackers along with their characteristics.
- Areas that need protection.

Upon completion of this unit, participants would be able to:

- Define security and its vital components and appreciate its importance.
- Understand the consequences of poor security.
- Assimilate the different terms related to information security and the information security attackers along with their characteristics.
- Recognize the areas that need protection.

5.3.8.2 Unit II: Human Aspects of Security

This unit examines aspects that have to do with the human aspects of security such as security risks that can arise by poor user choices. During the early years of information security, attacks were intended to erase a user's data or corrupt the disk of a computer so it cannot function properly. These attacks were malicious in nature and their objective was to deface or destroy. As the arsenal of security controls in organizations is becoming more effective at deterring attacks, focus has now been placed upon the weakest link, the human. Attacks are often attempting to trick users into revealing personal information, or download malware. For example, some attacks tempt users into revealing personal information such as credit card numbers or passwords; some others take advantage of user password habits (e.g. using the same password for multiple online services or use weak passwords) or try to take advantage of a trust relationship that may exist in social networking sites. The objective of this unit will be to examine security risks that can arise by poor user choices. The

qualities of a good password along with the attacks to weak passwords will be examined. Also attacks that take advantage of social engineering and the risks associated with using social networking sites will be covered. Specific unit contents include:

- Human error: the largest information security risk.

  Employee error or negligence is considered the root cause of many data breaches according to the Ponemon Institute (2012b). According to this study, the most common risky practices that employees routinely use are:

  - Sharing passwords with others.
  - Reusing the same password and username on different websites.
  - Using generic USB drives not encrypted or safeguarded by other means.
  - Leaving computers unattended when outside the workplace.
  - Losing a USB drive possibly containing confidential data and not immediately notifying their organization.
  - Working on a laptop when travelling and not using a privacy screen.
  - Carrying unnecessary sensitive information on a laptop when travelling.

- The use of passwords.

  Passwords are considered the first and last line of defense in securing individual's identity and data. Passwords are used every day in order to protect various information resources like personal computers, bank accounts or email accounts. It is important to understand and be able to identify if the password used at various online services is strong enough

to protect sensitive data and at the same time kept secure from unauthorized parties or individuals. The concept of weak passwords is examined. Many users tend to choose passwords that are easy to remember. For example many users prefer to use a common word as a password, choose short passwords that can be easily cracked through a brute force attack, use personal information in a password like information related to the user's name, social relations information such as friends' names, location information or hobbies, or use the same password on multiple online services. Common password rules that have to be followed when choosing a password are presented along with an easy to understand method on how to create a strong password. Finally participants have the chance to test the strength of their chosen password through an interactive online service and basic rules on how to deal with passwords safely are presented.

- Social Engineering concepts and risks

  The concept of social engineering as a low tech method used by hackers to obtain confidential information from legitimate users along with its various approaches: impersonation, phishing, hoaxes and their variations.

- Social networking concepts and risks.

  Although social networking sites are great places to meet and network for people that share similar habits and interests, they still pose serious security threats to users and their computers. At this point of the unit, the risk associated with visiting social networking sites are covered. Since Facebook is a social networking site commonly used by everyone, some

privacy setting considerations with respect to specific service features (e.g. Profile, photos, status updates, etc.) are introduced and a few easy to understand rules that should govern user behavior when visiting social networking sites are presented.

Upon completion of this unit, participants would be able to:

- Understand why human error still remain the largest threat to information security today.
- Understand the qualities of a good password along with the rules associated with creating and managing strong passwords.
- Understand the concept of social engineering, its variations and the steps that have to be taken into consideration for protecting assets and data against such attacks.
- Learn how to safely utilize social networking sites.

5.3.8.3 Unit III: System Security

Protecting a personal computer, whether it is a desktop, laptop or tablet can be a challenge even for the advanced computer user. The number and the different types of attacks that can be launched today against a personal computer have dramatically risen. At the same time, attackers are constantly changing the methods used to attack personal systems and acquire sensitive data. Every user must be able to protect their computer from a variety of attacks. At many instances, a single defense mechanism is not enough to fully protect a computer since it must be protected from a variety of attacks. There are several different defenses that must be in place for a computer to remain safe. In this learning unit the aspects of system security will be described. The different types of computer

attacks that occur today along with what defenses must be in place in order to keep system information secure will also be examined. Finally the steps that must be taken to recover from an attack will be considered. Specific unit contents include:

- Attacks on systems using malware.
- Types of malware.
- System defenses.
    - Performing system and application updates.
    - Using vulnerability management software.
    - Using antivirus software.
    - Using a firewall.
    - Using User Account Control.
    - Using backups.

Upon completion of this unit, participants would be able to:

- Understand the components related to the protection of a personal computer.
- Learn the different types of attacks to systems using malware.
- Familiarize themselves with the defenses against malware such as regular system and application updates, use of antivirus software, using a firewall and utilizing backups.

5.3.8.4 Unit IV: Application Security

Although the Internet has provided many benefits (especially in education), it has also become a primary pathway for attackers and their attempts to reach personal

information. A computer connected to the Internet is also exposed to a series of malicious attacks. The objective of this area will be to describe how Internet and related services work along with the risks associated with them. Also how attackers can distribute malicious code and the defenses against such attacks will be described. Specific unit contents include:

- Internet and WWW basics.
- Internet security risks.
    - Mobile code (javascript, java and activeX).
    - Cookies.
    - P2P programs.
    - Drive-By downloads.
    - Redirected web traffic.
    - Email risks
- Internet Defenses
    - Securing your browser.
    - Using content filtering and content advisors.
    - Identifying secure sites.
    - Email defenses.

Upon completion of this unit, participants would be able to:

- Understand the risks associated with the use of the Internet and the World Wide Web.
- Describe how attackers can compromise security using mobile code, cookies and drive-by downloads.
- Recognize the threats associated with the use of peer to peer programs.

- List the security risks associated with the use of e-mail along with methods of protection.
- Describe how specific web browser settings can be used in creating a stronger security environment.

5.3.8.5 Unit V: Mobile Device Security

In todays' environment, mobile devices (tablets, laptops and smartphones) and the wireless networks that support them, have significantly altered the way we live, work and interact. It is no longer necessary to use a desktop computer connected by a cable to a network in order to surf the web, access emails or connect to a company network thus increasing employee productivity. There is no sector of the economy that has not been dramatically affected by mobile devices and wireless technology. Just as users have widely adopted the use of mobile devices and wireless networks, so too have attackers. Networks that are available through a wireless connection have become a prime target for attackers. Users should treat mobile devices and associated wireless networks with the same importance as they treat their desktop computers. In this unit the threats and attacks on wireless data networks and mobile devices that use them will be described. Then, ways to defend and protect a home wireless network along with safety guidelines on how to use a public wireless network will be examined. Specific unit contents include:

- Mobile device threats and attacks.
    - The nature of Wi-Fi networks.
    - Attacks on Wi-Fi.
    - Attacks on mobile devices (laptops, tablets and smartphones).

- Mobile device defenses and best practices.
    - Home Wi-Fi security.
    - Public network security.
    - Mobile device security.
    - Best practices.

Upon completion of this unit, participants would be able to:

- Understand the nature of Wi-Fi networks.
- Describe the various attacks against a wireless network and list the various types of defenses that have to be taken into consideration.
- Explain how a home Wi-Fi network can be protected.
- Describe how to use a public wireless network securely.

5.3.8.6 Unit VI: Workplace Security

Information security attacks on businesses and organizations are more widespread than attacks on home networks. A successful attack that breaches a company network can expose hundreds of computers and information in these computers (e.g. confidential company data) is extremely valuable and highly sought after by attackers. The primary difference between home security and the security in the organization is who is responsible for creating and establishing levels of security. In a home network the user is responsible to set up security while in a business it is the organization that is responsible. Although in a business environment, computer and data security is pre-configured by a series of centrally controlled rules and procedures, it is important for employees to know what to expect at the office in terms of security instead of how to configure office devices for protection. Despite the fact that different organizations have different

established policies in respect to information security, there is a common baseline of security measures that almost all organizations follow. The purpose of this learning unit is to explore what an employee should expect in terms of security as a company employee. Physical security (physical access to facilities and computer systems) along with security provisions that restrict access to data and other common company security policies will be examined. Specific unit contents include:

- Restrictions to Physical Access.
- Restrict Data Access. (e.g. Tokens, cards).
- Security policies.
- Crisis preparedness and incident reporting.
- Disaster Recovery

Upon completion of this unit, participants would be able to:

- Define physical security and understand the tools and technologies that may be used to regulate physical access (e.g. tokens, cards, badges).
- Explain what a security policy is and the principles behind it.
- Understand general steps that have to be taken in order to prepare and respond to a crisis situation.

5.4 Chapter Summary

The purpose of this chapter was to investigate the rationale behind the creation of the information security toolkit along with the theoretical framework on which it was actually developed. The chapter starts by examining the elements of

information security learning in order to get an understanding of its meaning and process continuum that has “awareness” as its starting point, followed by training and finally evolves into education. The two main categories under which information security awareness is classified are presented. A model for knowledge building based on Nonaka’s and Takeushi SECI model is used in order to explain how awareness training can lead to appropriate security behavior. Elements of e-learning along with e-learning delivery approaches and instructional design methods are presented. The chapter concludes by presenting the structure and content areas of the information security toolkit, along with the rationale behind choosing each content area in an effort to create a baseline knowledge for information security that will support the security awareness raising methods addressed to the general population.

The next chapter discusses the process of implementing and evaluating the effectiveness of the toolkit. More specifically the process of putting a toolkit prototype in action is presented along with aspects of the development work behind it. Concerning the toolkit, its evaluation in terms of effectiveness and usability is assessed using three representative focus groups (a group of college first year students, a group of college students towards graduation and a group of people that hold administrative positions) and by exposing a group of experts to the toolkit in order to measure and analyze their opinions through a survey.

Chapter VI – Information Security Toolkit Implementation and Evaluation

6.1 Introduction

In the previous chapter the rationale was investigated behind the creation of an information security toolkit as an awareness raising method along with the theoretical framework behind its development. The chapter examined the process continuum of information security learning (awareness, training, education) and described a model of knowledge building based on the SECI model in order to explain how awareness training can lead to appropriate security behavior. The structure and content areas of the toolkit were presented in an effort to create a baseline knowledge for information security, which will support the security awareness raising methods for the general population.

In this chapter the process of implementing and evaluating the effectiveness of the toolkit is examined. More specifically the process of putting a toolkit prototype in action is presented along with aspects of the development work behind it. The process of a pilot testing phase conducted before the actual testing and evaluation phase will be described. Consideration is also given to the toolkit evaluation in terms of effectiveness and usability utilizing the following methods:

- Testing of the toolkit using three representative focus groups: a group of college first year students, students towards graduation and a group of people that hold administrative positions. The three groups were exposed to the different elements of the toolkit and their thoughts are discussed and presented.

Testing the toolkit effectiveness using two representative groups of individuals:

- a group of individuals from institutions of higher education who are involved in the learning process from various positions (e.g. Librarians,

technology specialists, academics, teaching and learning department staff, course designers, etc.). This testing was done by exposing this group of individuals to the toolkit and their opinions were measured and analyzed through a survey.

- a group that includes experts in the field, like people closely related to the IT function, IT managers/administrations and information security experts. This testing was done by exposing this group of experts to the toolkit and their opinions were measured and analyzed through a survey and by conducting short personal interviews.

6.2 Piloting a Security Toolkit Prototype

As explained in the previous chapter, the security toolkit was comprised of the following parts:

- pre-assessment
- main e-learning unit
- post-assessment

The purpose of the e-learning unit was to focus attention on security in a way that will allow the general population to recognize security concerns and respond accordingly. In other words it will help establish an acceptable level of awareness that will result in an appropriate behavior. Although in today's computing environments, not all users are working in positions that handle confidential or critical data, the penetration of technology in our everyday lives is significant. For that reason, the areas that were included in the e-learning unit were derived from the assumption that an information security program should be focused on all users within an organization (National Institute of Standards and Technology (NIST), 2003). At the same time, home users are usually exposed to information security risks mainly because of their lack of knowledge or negligence such as:

- Using the Internet without being aware of the risks and dangers associated with it or the consequences of a security leak or compromise.
- Choosing weak or common passwords for significant Internet services that may be easily compromised.
- Engage themselves in inappropriate online behavior through their use of social networking sites.
- Become victims of social engineering attacks.

Based on the above considerations, the following topics were chosen for the e-learning unit:

- Introduction to Information Security.
- Human Aspects of Security.
- System Security.
- Application Security.
- Mobile Device Security and
- Workplace Security.

In developing a security toolkit prototype, the following topics were chosen and the respective units were created:

- Introduction to Information Security.
- Human Aspects of Security.

The rationale behind this decision is as follows.

The starting point for any effort towards information security should be with the basics of information security. No matter if training is addressed to novice or experiences users, a unit that describes the basics of information security is the best start. Information security is not achieved by technical means alone, so this chapter would provide the foundation knowledge on how an everyday user should bother with security. Many users, not necessarily from personal experience

through training but mainly from the publicity and media coverage that security incidents have received, are aware of security terms and concepts but still remain unsure about how to actually keep their computer and data safe or what is important to protect. At the same time, they do not have a conceptual image of the topic area in terms of confidentiality, integrity and availability. At the same time it is important to learn and understand specific everyday examples that link and define these security components.

This unit will also provide the necessary foundation in order to understand today's challenges in securing information. Despite the fact that the amount of money spent annually on computer and information security continues to increase, the number of successful attacks increase also. Many people believe that poor information security behavior and practice may –in the worst case scenario– result in loss of access to their computer or data, loss of the work in case it was not backed up and ultimately loss of productivity but do not consider at all that the key in such cases is employee accountability. In other words they may be held responsible for any action or inaction that led to the security incident and at the same time the company may suffer a severe financial or reputational loss.

The presentation and basic understanding of terms and definitions that are related to the information security area is considered an important component in an effort to familiarize individuals with a core knowledge set needed to protect electronic information and systems. This basic literacy level is essential since it comprises the "alphabet" (a core set of key terms) essential for the protection of information and systems (National Institute of Standards and Technology (NIST), 1998). This will also assist users in their needed skills development to identify measures and approaches that could be adopted to overcome possible security

risks. When it is expected from someone to apply specific behavior related to an information security area, the type of problem or risk should be known in order to apply the necessary safety procedures (Kruger et al., 2010). Similarly, information about the different types of attackers, who they are and why they seek to compromise the confidentiality, integrity and availability of information assets is a valuable addition.

Finally, the 'Introduction to Information Security' module concludes by briefly describing the areas that need protection. This will serve as the link to the topics that will follow in the toolkit for which this module serves as foundation knowledge.

The rationale behind the inclusion of the human aspects of security in the toolkit prototype mainly lies in the fact that there is a dramatic change in the recent years to the profile of the generic computer user. Significant technological advances in the areas of computer and network security have added additional levels of protection for information systems and data. But these technological developments have resulted in shifting the focus of intruders from the well protected infrastructures to more vulnerable targets which are the people that operate these infrastructures. Although technology is an essential part in respect to the security of information assets but people are the ones who are responsible for the operation of such development tools (Lacey, 2009) .

The first step towards better information security behavior lies in the ability of the user to understand the importance of passwords. Even the best security system won't help if an intruder gets an employee's password. For that reason it is important that users understand the importance of strong passwords, provide

guidance on how strong passwords are constructed and safely kept and give the ability to the user to test the strength of their chosen passwords.

Social engineering is considered a serious threat to information security and should be considered equally important with other information security threats. The success of such attacks mainly lies in the fact that users have the tendency to help others without being aware of the value of information they possess (Luo et al., 2011). Social engineering involves a combination of techniques used to manipulate victims into exposing confidential information or engage in actions that compromise security. These attacks are not technical in nature and involve communication technologies with which the users are engaged on a daily basis. It is thus important that users are familiar with its different variations so they can be prepared accordingly.

Finally, awareness initiatives should take into serious consideration the increasing popularity of social networks amongst the online population. Although there are a lot of examples of security incidents involving such sites, the reaction of organizations to the social networking phenomenon is mixed. While there are organizations that have banned access completely, there are others that embrace social networking as a way to communicate information to staff, existing and potentials customers and at the same time as a tool to maintain contacts and build relationships (Everett, 2009). Also there are organizations that are more worried about reduced productivity as a result of employee engagement to such sites than potential security implications.

Social networking sites do pose a threat to information security and protection steps should be seriously considered and assimilated by everyone. Identity theft

through data aggregation (gathering around data from multiple social network sites in order to build a clear picture of an individual), and viral infection through the downloading of malware are only a few of the security threats that social networking site visitors may face.

The solution to such concerns in order to mitigate any potential risks is to raise awareness. Therefore all potential visitors must be provided with the appropriate knowledge in order to have a secure exposure with such sites as well as guidelines to appropriate usage.

6.3 Pilot Toolkit Development

The toolkit prototype was developed having in mind the requirement for ease of use by a novice user plus efficiency in navigation and material coverage. In designing the user interface of the toolkit specific human computer interaction practices were used in order to establish a prototype that achieves active engagement and interaction by the learner to meet objectives and achieve intended outcomes (Gathany, 2012). A successful e-learning product must apply interactive strategies in an effort to engage learners and stimulate recall of prior knowledge. Different levels of interactivity may be used in order to fit audience needs. The interface in order to be learner-friendly, should include a main menu and the necessary navigational elements that help learners know where they are within the course and how they can easily move through it (CDC, 2013). More specifically, the following standard practices apply when designing the interface and the navigation elements of an e-learning course:

- Navigation is clear and easy to use through a hyperlinked main menu.
- Next and previous buttons are easily located.

- Learners can exit the course and resume at the place where they stopped.
- Learners can always get feedback on their location within the course.
- Use of text and graphics is balanced and a template is used throughout the course in order to ensure consistency of fonts, colors, layouts and other design elements.

The content is indexed so that learners can find the information they seek easily. In this sense tabs that lead to additional information such as resources, references and glossary can be considered useful.

Taking into consideration the above best practices, the prototype screen consists of the following areas:

- Menu area (1): the menu area displays the different toolkit areas (e.g. units, pages in every unit). The title of each area works as a hyperlink and the user can jump directly to any part of the toolkit.
- Glossary (2): displays various terms presented in the toolkit along with a brief definition.
- Notes (3): the notes area is used to display a text version of the narrative presented in each of the unit screens.
- Main toolkit window (4): the main toolkit window displays the actual toolkit contents along with any user interactivity needed (e.g. hyperlinks, hotspots). The window allows the user to mute the sound if needed, contains a timeline allowing the user to pause, play or re-play the unit plus the necessary next and previous navigation buttons.
- Search (5): a search feature allows the user to search for any term within the toolkit and jump to this area directly.

- Resources (6): the resources popup window contains useful links and documents in respect to the area of security awareness.

Figure 32: Main toolkit screen

The toolkit starts with an introductory screen which then directs the user to a table of contents screen. Each unit has a content area and a quiz area. Although there is no restriction, it is advisable that the user completes the content area before moving to the quiz area. Upon completion of a toolkit area, the user is returned to the table of contents screen where a checkmark indicates completion of the specific area. At any time the learner can exit the course and resume work at the place he stopped.

The unit that deals with the introduction to information security focuses around the following areas:

- Why it is important to deal with security

Although the answer to this question should be pretty straightforward, in reality a lot of users usually fail to realize the fact that information security is an issue that affects everyone and should not be neglected. Although billions of dollars are spent annually on information security, the number of successful attacks continue to increase (Ponemon Institute, 2012a; Privacy Rights Clearinghouse, 2014). For that reason, simple and widely known facts from publicly reported information security breaches –yet neglected– are presented to clearly identify the need for information security awareness.

- Definition of information security.

  Before making it possible to defend against attacks, it is necessary to understand what information security is. The concept of information security is presented through an easy to understand definition of it (protection of information from unauthorized access, disclosure, disruption, modification or destruction) along with the goals of information security: (1) confidentiality, (2) integrity and (3) availability including simple everyday examples.

- The need for information security.

  Every user needs to know about information security issues that affect them as a person; as a student; or, as a member of the workforce. There are also issues that may affect users as members of a family. At the most practical level the need for information security lies with ensuring that your information remains confidential and only those who should have access to it can indeed access it, knowing that only authorized individuals are able

to change your information and making sure that your information is available when you need it. More specifically users should be able to:

- Defend against viruses and malware software.
- Recognize scam messages, social engineering attacks and spam.
- Be able to protect themselves from unsafe content while online.
- Use strong passwords in order to protect personal data.
- Take proactive actions and be prepared in case of a disaster.

- The consequences of poor security.

  The consequences of poor security should be known and understood by everyone. If a computer is compromised, this may lead to loss of access to the computer and data, loss of work that is not backed up and loss of productivity. At the same time if a security problem has put sensitive information at risk, or if a device containing sensitive data is lost or stolen the effects can be far reaching. A user may be held accountable for any negligent action or inaction that led to the incident. The organization may take a reputational hit or suffer financial loss (e.g. payment of regulatory fines, loss of funding, lawsuits, etc.).

- Presentation of commonly used information security terms and definitions. Information security terms and definitions, are heard or presented every day, but, can sometimes be confusing or misunderstood by the average user. In order to help understand commonly used terms, a list has been created in this part of the unit along with what they mean using simple English (National Initiative for Cybersecurity Careers and Studies., 2013; Zeltser and Skoudis, 2013). The definitions are presented with easy to navigate hotspots.

- The attackers.

  This part of the e-Learning unit module briefly describes the types of attackers who seek to compromise the confidentiality, integrity, or availability of our information assets. More specifically, the different types of attackers presented and explained here are:

  - Cybercriminals: organized gangs or individuals who are financially motivated and usually focus on wealthy individuals, businesses and governments.
  - Script Kiddies: individuals who attack computers with minimal knowledge often using automated attack software available from the web.
  - Cyberterrorists: refers to the use of information technology by terrorist groups that organize and execute attacks against networks, computers systems and other critical infrastructure.
  - Hacktivists: individuals motivated by ideology who attack networks and computer systems in order to promote a political agenda.
  - Government agencies: recently government agencies appear to have been behind attacks or monitoring activities on foreign governments and even their own citizens who they consider hostile or threatening.

- Areas that need protection.

  Finally the information security areas that need protection are briefly presented. This part serves as a connector to the units of the toolkit that will follow.

The unit that deals with the human aspects of security focuses around the following areas:

- Human Error: the largest information security risk

  Employee negligence or maliciousness is the root cause of many data breaches (Ponemon Institute, 2012b). Their 2012 study surveyed 709 IT and IT security practitioners and identified the most common risky practices that employees routinely use as:

  - Sharing passwords with others.
  - Reusing the same password and username on different systems and websites.
  - Using generic USB drives not encrypted or safeguarded by other means.
  - Leaving computers unattended when outside the workplace.
  - Losing a USB drive possibly containing confidential data and not immediately notifying their organization.
  - Working on a laptop when travelling and not using a privacy screen.
  - Carrying unnecessary sensitive information on a laptop when travelling.

- The use of passwords

  Passwords are considered the first and last line of defense in securing individual's identity and data. Passwords are used every day in order to protect various information resources like personal computers, bank accounts or email accounts. It is important to understand and be able to

identify if the password used for various online services is strong enough to protect sensitive data and at the same time kept secure from unauthorized parties or individuals. The concept of weak passwords is examined as many users tend to choose passwords that are easy to remember. For example some users prefer to use a common word as a password, choose short passwords that can be easily cracked through a brute force attack, use personal information in a password (e.g. related to the user's name, social relations information such as friends' names, location information or hobbies), or use the same password on multiple online services. Common password rules that have to be followed when choosing a password are presented along with an easy to understand method on how to create a strong password. Finally participants have the opportunity to test the strength of their chosen password through an interactive online service and basic rules on how to deal with passwords safely are presented.

- Social Engineering concepts and risks

  The concept of social engineering as a low-tech method used by hackers to obtain confidential information from legitimate users is examined along with its various approaches like:

  - Impersonation: playing out the role of a person on a victim (e.g. Repair person, IT support, trusted fellow employee, etc.) in order to get access to personal information.
  - Phishing: using email messages that seem official and genuine that include a catchy headline (e.g. "security alert") in order to steal confidential information like account numbers and/or passwords.

- Hoaxes: false warning usually included in email messages asking the legitimate user to take specific actions that –if taken- could allow an attacker to compromise the system.

Further to that, the most common variations of phishing attacks like pharming, spear phishing, whaling and vishing are introduced and explained. These attacks rely on psychological manipulation. At the same time, there are social engineering attacks that rely on physical acts. The objective of these attacks is to take advantage of user actions that can result in a user revealing security information in an indirect way. The concepts of dumpster diving and shoulder surfing are presented. Finally, a brief guide on how to spot the signs of a social engineering attack is presented.

- Social Networking concepts and risks

Social networking sites are great places to meet people that share similar habits and interests. But Facebook, Twitter and similar social networking sites can also pose serious security threats to users and their computers. At this point of the unit, the risks associated with visiting social networking sites are covered. Since Facebook is a commonly used social networking site, some privacy settings considerations in respect of specific service features (e.g. Profile, photos, status updates, etc.) are introduced. Finally, a few easy to understand rules that should govern user behavior when visiting social networking sites are presented.

6.4 Assessment of toolkit effectiveness

An information security awareness program is considered effective if it is capable of establishing the appropriate knowledge and influence the attitude and behavior of the participants towards positive changes in their security culture. According to the NIST institute there are three steps that should be taken into consideration when developing a security awareness program (Wilson Mark and Hash Joan, 2003):

- Design the program
- Develop the material
- Implement the program

An effective awareness program should start by identifying the requirements and key problem areas, analysis of the root causes and at the end develop the programs that indicate corrective actions (Lacey, 2009). Although expressing knowledge and awareness is relatively easy to achieve, changing the actual attitude can be a much harder task. Changing attitudes involves a learning experience but changing behaviors requires a clear understanding of the desired behavior.

In order to make sure that an awareness program has reached its objectives, appropriate measures need to be in place. Kruger and Kearney (2006) in his study gives an example on the development of a measurement model for information security awareness. In this model (applied in an international gold mining company), changes in security behavior were monitored based on three dimensions:

- What the employee knows (knowledge).
- What the employee thinks (attitude).
- What the employee does (behavior).

These dimensions were subdivided into further areas like keeping passwords and personal identification numbers secret, using the Internet and email in an appropriately safe manner and using mobile equipment carefully.

The need for businesses to focus on measuring actual behaviors towards information security in order to evaluate spend effectiveness has also been a recommendation of the PWC Information Security Breaches Survey (PWC, 2014). As businesses are investing larger proportions of their budget on information security, the general level of awareness is rising. But, without effective measurement and evaluation of an awareness program, there is no real evidence for its effectiveness.

Measuring the above dimensions is not an easy task since there are no commonly agreed measures for the effectiveness of information security awareness initiatives. There are however, a number of different qualitative and quantitative measures that can assist in providing an insight into the level of information security awareness.

Quantitative measures may include data such as:

- The number of people trained.
- The frequency these people were trained.
- The pass and fail rates of these people on respective assessment tests.

As many organizations use e-learning as the main training tool through a learning management system, such systems can be used to administer e-learning and provide a range of useful reports such as completion rates and assessment scores. Although this kind of quantitative data measured over a period of time can be a good starting point since it can provide trends in the levels of information

security awareness that can be used to draw meaningful conclusions, it does not necessarily provide a valid indication whether the awareness training is effective (Davis, 2008). In order to provide a complete insight of the effectiveness of awareness raising methods, quantitative data needs to be combined with qualitative data for determining whether the desired effects have been achieved in terms of user behavior. Since information security lies in the overlap of attitudes, knowledge and behaviors, there are a variety of tools and methods that can be used to collect such qualitative data. According to Davis (2008), the most effective methods are summarized in the table below (Davis, 2008):

Attitudes	**Knowledge**	**Behaviours**
Surveys	Assessment Tests	Behavioural Measures
Interviews		Surveys
Focus Groups		Interviews
		Focus Groups

Table 26: Most effective methods for measuring the effectiveness of awareness raising methods

The following methods will be used for measuring the toolkit effectiveness:

- Focus groups as a form of group interview. The focus group will not only collect data from several people at the same time but will also encourage interaction and exchange of ideas that will help in exploring people's knowledge and experiences.
- Surveys as a tool for collecting quantitative data from a larger group of individuals.
- Short semi-structured interviews in order to explore the views, experiences, beliefs and/or motivations of a small group of people on a specific matter or topic.

In addition to focus groups, surveys will be used as an additional tool to measure the toolkit effectiveness.

6.4.1 Focus Groups

The use of a focus group is a method of qualitative research where the participants of the group are asked about their perceptions, attitudes, opinions or beliefs about a product, concept, effort or idea. Generally speaking, a focus group can be defined as a small gathering of individuals who share a common interest or characteristic. The group is assembled and conducted by an individual who acts as a moderator and uses the group and its interactions in order to gain additional information on an issue or a topic (Williams and Katz, 2001).

Although the use of focus groups is sometimes approached with a degree of skepticism concerning its effectiveness as a method of data collection, it gains a lot of popularity among researchers in specific data collection situations (Morgan and Krueger, 1993; Barbour and Kitzinger, 1999; Krueger and Casey, 2008).

The purpose of conducting a focus group is to promote an atmosphere of mutual understanding and openness where participants feel comfortable to share their ideas, experiences and attitudes about a specific topic. During the focus group, participants influence and at the same time are influenced, while the researcher plays the role of the moderator, listener, observer and finally the focus group result analyst.

In recent years, the use of focus groups has gained a lot of popularity as a qualitative method among researchers because of their characteristics. Focus groups have the ability to examine “how knowledge, ideas, story-telling, self-presentation and linguistic exchanges operate within a given cultural context”

adding an extra level of validity to traditional quantitative approaches (Barbour and Kitzinger, 1999). On the other hand, although collecting quantitative data (for example through the use of surveys) and measuring it through a series of statistical hypotheses or mathematical interpretations is enough for explaining how many people have a certain opinion on a matter, at the same time they do not explore the way certain points of view and opinions are constructed and expressed. Qualitative methods such as focus groups, participant observation and interviews pay more attention to the opinion of the participants and how this opinion is expressed in their everyday experiences allowing the researcher to gain a better understanding of the reality. Such reality cannot be easily and meaningfully expressed by the use of numbers (Berg, 2001). At the same time, surveys and other forms of quantitative research if combined with focus groups, can fill in the gaps and provide an additional degree of verification and validity. For example, by exploring and discussing the questions included in a survey, using a focus group, may reveal that the way some survey questions were constructed was misleading thus leading to inaccurate results and conclusions (Barbour and Kitzinger, 1999).

The benefits of using a focus group can be summarized as follows:

- Participants in a focus group can provide a rich source of information on a particular topic which could be very difficult to acquire by other traditional survey means. At the same time, the focus group encourages synergies among its members by developing new ideas that come as a result of personal opinions from specific real life situations.
- Participants are empowered in the way that they are treated and valued as experts. They have the opportunity to work collaboratively with the

researcher and at the same time interact with other participants of the group in a free and open manner.

In the past ten years, according to Williams and Katz (Williams and Katz, 2001), researchers have identified the usability of focus groups in education in achieving various objectives such as:

- Developing learning tools that appeal to students' interests and needs.
- Evaluating the knowledge and attitudes of students about curriculum issues.
- Formulating new marketing strategies for educational programs and,
- Enhancing survey results in educational research.

Especially in an educational setting, focus groups can provide a great insight to researchers in the following efforts:

- Supporting a decision making process: although a focus groups should never be used as the sole method for reaching a decision (Krueger and Casey, 2008), its input can be extremely useful when evaluating decisions. Especially when decisions have to do with a planning process. In the case of the Security Toolkit, a focus group is considered beneficial in assessing the beliefs, attitudes and feelings of students and staff towards the evaluation of the toolkit effectiveness.
- Evaluation and assessment of an educational tool: when dealing with a particular learning objective or when evaluating the effectiveness of a learning instrument, focus groups can be a useful departure point. In the case of the e-learning component of the Security Toolkit, a focus group involving students may bring valuable conclusions on how students absorb and retain knowledge about basic security concepts in relation to their existing knowledge and experiences.

- Make comparisons between qualitative and quantitative research and fill the gaps between the two when needed: as mentioned earlier, relying solely on survey research may not provide a complete picture for evaluating an educational program. In the case of the Security Toolkit, the combination of focus groups and questionnaires may draw additional conclusions that would not surface by market research alone. In other words, results collected from a questionnaire survey may be further enriched through the use of a focus group. At the same time, the focus group can encourage a more active contribution especially from people who feel they have nothing further to say after replying to a quantitative research question.

From the above, it has been concluded that conducting a focus group could be beneficial in assessing the effectiveness of the Security Toolkit as a security awareness raising method. In conducting the focus group, the following general guidelines were followed:

Research purpose

The focus group will be used to assess the effectiveness and usability of the toolkit as a whole and in its distinct parts:

- The pre-assessment unit will be evaluated as a method of assessing the existing security awareness knowledge level of the participant,
- The actual e-learning part will be evaluated as an efficient method of examining introductory concepts in information security and stressing its challenges and importance, and also examining aspects that have to do

with the human aspects of security such as security risks that can arise by poor user choices.

- The post-assessment part will be used to evaluate whether exposure to the previous e-learning has played a significant role in raising the awareness level identified previously.

Focus group moderation

The selection of an appropriate and skillful moderator is fundamental for conducting a successful focus group. A successful moderator must be able to listen, facilitate the interaction between the members of the group and at the same time learn from the group. They must also feel confident within the group and at the same time create an atmosphere of open discussion and free exchange of ideas. Due to the distinctiveness of the subject, it was considered important to have sufficient knowledge on the subject. For that reason it was decided that the author of this thesis will also be the focus group moderator.

Preparation of a focus group guide

In preparing the actual part of the focus group a series of steps were prepared in advance. More specifically,

i. A quiet and convenient place for all the participants was chosen in order to conduct the focus group.
ii. The moderator introduced himself to the group and presented the topic, rationale and objectives of the group.
iii. The moderator distributed to the participants a short questionnaire to determine their information security experience in order to prepare them

for the subject and at the same time welcome and facilitate an atmosphere of mutual exchange of opinions.

iv. The participants then proceeded with the online pre-assessment test; their views were recorded; and, feedback was received.

v. The moderator then made a short introduction to the topic of information security and the need for a security awareness raising for the general population.

vi. The participants proceeded with the actual e-learning unit and post-assessment at the end of each module.

vii. The moderator concluded the focus group by conducting an open discussion concerning the experience of the participants in using the toolkit. For that reason a series of questions was prepared. Taking into consideration that the question and answer session was conducted immediately after the participants fully completed the Security Awareness Toolkit, it was important that the questions chosen would facilitate an open discussion in relation to the toolkit experience.

The focus group was scheduled to last no more than two hours and the actual toolkit participant experience was recorded using screen capture software and a video camera.

Selecting appropriate participants

Effort had to be made in order to create groups that are homogeneous with common interests and concerns so members feel comfortable in speaking with each other. This method ensures that an open dialogue is facilitated. Also it was decided that was a balance in terms of gender and age. For that reason, three distinct groups were formulated:

i. A group of college undergraduate students with not more than thirty course credit hours completed (first year students). The rationale for choosing this group was to investigate what effect the toolkit would have on students that were at the beginning of their college career and may have had very little or no information security experience. Although it is accepted that college students use information technology in their everyday life, this does not necessarily mean that they have an appropriate level of awareness concerning the risks about using this technology.

ii. A group of college undergraduate students with ninety course credit hours or more completed (last year students or students towards graduation). It is generally accepted that students towards graduation are more mature mainly as a result of their studies and their proximity to joining the workforce. But this maturity does not necessarily include security awareness as a component at least for those that do not have information technology as a core part of their studies. Choosing such a group to investigate what effect the toolkit will have on graduating students will provide a valuable insight concerning their everyday attitudes towards information security.

iii. A group of workers employed at various administrative positions. Although sophisticated technology and technical countermeasures are present at most companies to protect information and computer systems, humans remain the weakest link in the information security chain. An appropriate security awareness level for the general workforce is crucial for the success of any information security effort. The inclusion of such a group to the study was done in order to investigate if exposure to the toolkit would have an effect on their level of security behavior.

There are debates whether focus group members should know each other. Some researchers argue that the ideal focus group, is one that all participants are very comfortable with each other (e.g. similar age group, common group interests) but none of them know each other (Eliot & Associates, 2005; Marczak and Sewell, 2005). Others argue that a group of people who know each other are likely to find it easier to talk openly and honestly during the session (Bush, n.d.). Although it was not the intention to include group members that know each other, since all invited participants come from the same institution, such an outcome could not be controlled. Indeed in the case of the administrative group formation, extra care was taken so group members chosen do not include high executives or people whose presence or opinion could affect the free flow of the discussion.

The Focus Group in action – Students Group A and B

The study involved a group of 7 students (3 male and 4 female) with at most 30 credit course hours completed and a group of 8 students (3 male and 5 female) with more than 90 credit course hours completed. The participants were asked the following questions in order to determine their everyday habits in terms of information security by completing a small questionnaire. The questionnaire came from the surveys presented and analyzed in Chapter IV of this thesis and contained questions that were covered by the topics of the security toolkit:

Question	**Answer Choices**
Do you own a computer at home?	• Yes • No
Do you have a personal Internet connection?	• Yes • No
How much time do you spend online per day?	• < 1 hour, • 1-3 hours, • 4-5 hours,

	• 6-8 hours, • >8 hours
Please rank your main uses of Internet?	• E-Mail, • Educational purposes, • Chat rooms, • Games, • Web Browsing (excluding social networking), • Shopping, • Banking/Paying bills, • Instant messaging, • Social Networking
I possess the necessary knowledge in order to protect my information technology assets.	• Strongly Disagree, • Disagree, • Neutral, • Agree, • Strongly Agree
Do you have any of the following in place in order to protect your computer and electronic data?	• Antivirus Software, • Firewall, • Anti-spam filter, • Good Passwords, • Regular Backups, • Regular Software updates
To which of the following people would you reveal our password if requested to do so?	• A fellow student, • A college professor, • The network administrator, • Anyone, • No one • Other
Which of the following password would you feel are acceptable and safe to choose as your password?	• My college ID number. • My name. • Something that I easily remember. • A combination of letters in upper and lower case, digits and special characters that have a special meaning for me. • My birthday. • None of the above • Other
Which of the following may be a potential premise for a phishing attempt	• Invitations to see photos of family or friends. • Pleas for disaster relief assistance.

	• Urgent email threatening loss of access to accounts if username and password are not provided
Level of familiarity with the following terminology	• Spyware • Phishing • Dumpster Diving • Shoulder Surfing • Identity Theft • Spam • Trojan • Virus • Worm • Adware • Social Engineering • Spear Phishing
Information security training is considered very important for me.	• Strongly Disagree • Disagree • Neutral • Agree • Strongly Agree
Which of the following do you consider a good habit when visiting a social networking site like Facebook, and Twitter	• Disclose very few details about yourself and only with people you trust. • Don't accept invitations and offers from people you do not know and trust. • Avoid installing programs and plugins that are not verified. • Check privacy settings and read the policy that governs the degree of sharing personal information
I use the same password for everything that needs a password	• Yes • No
Using the option "remember password" in your web browser or email program is an acceptable method for easily remembering a password.	• Yes • No

Table 27: Information security everyday habits questionnaire

From the answers collected from the introductory questionnaire the following observations were made. Concerning group A (1st year students):

- Almost all students have a computer at home (86% of the participants) and all of them with an Internet connection.
- The majority of the participants spend between 1 and 3 hours online. The second most popular choice is 4-5 hours online. Although the sample is very small to make accurate comparisons, the results to this question are in accordance with a survey previously conducted.
- The use of e-mail and social networking sites remain the top choices among the main uses of Internet.
- Among the focus group participants, half of them are neutral concerning their knowledge to protect their information technology assets.
- Among the methods that are in place in order to protect computer and electronic data, antivirus software and the use of regular backups are the most popular methods. The use of good passwords came fourth in their choices.
- Most of the participants, do not feel comfortable in revealing their password (5 out of 7). From those who have no problem revealing their password, a fellow student is the most likely recipient.
- Concerning the password that they feel acceptable and safe most participants (4 out of 7) would choose a combination of letters (upper and lower case), digits and special characters that have a special meaning to them. At the same time there are participants that would choose something that is easily remembered (2 out of 7). On the other hand, 3 out of 7 participants prefer to use the same password for everything that needs a password. The same number of participants prefer to use the option “remember password” as an acceptable method for easily remembering a password.

- The majority of the participants (6 out of 7) would identify a phishing attempt as an email message threatening that access to accounts will be lost if username and password are not provided. One participant identified this kind of threat as an email message that asks for disaster relief assistance.
- The participants familiarity with information security terms can be summarized as follows:
    - Participants feel familiar or very familiar with the terms Spam, Trojan and Virus.
    - Participants feel least familiar or not at all familiar with the terms Dumpster diving, shoulder surfing and spear phishing.
- More than 70% of the participant agree or strongly agree that information security training is considered very important.

In terms of visiting social networking sites the following habits apply:

Social Network Site Habits (1st Year students)	**Number of respondents**
Disclose very few details about yourself and only with people you trust	5
Don't accept invitations and offers from people you do not know and trust	4
Avoid installing programs and plugins that are not verified.	3
Check privacy settings and read the policy that governs the degree of sharing personal information.	3

Table 28: Group A - Social networking sites habits (1st Year students)

Concerning group B (Senior year students):

- All students have a computer at home (100% of the participants) with an Internet connection.

- The majority of the participants spend between 1 and 3 hours online, but still there is a minority of respondents that spend between 4 and 5 or 6 and 8 hours online.
- The use of e-mail is the dominant choice among the main uses of Internet. As opposed to the 1st year group, the second most popular choices are Web browsing and usage for educational purposes. As compared with the previous group, social networking sites did not seem so popular.
- Among the focus group participants, 75% of them (6 out of 8) agree or strongly agree whether they possess the necessary knowledge to protect their information technology assets.
- Among the methods that are in place in order to protect computer and electronic data, antivirus software and the use of good passwords are the most popular methods, with the use of regular backups rated the lowest.
- Among the participants, only one felt comfortable in revealing their password and this is the case when asked by the network administrator.
- Concerning the password that they feel acceptable and safe most participants (6 out of 8) would choose a combination of letters (upper and lower case), digits and special characters that have a special meaning to them. At the same time there are participants that would choose something that is easily remembered (2 out of 8). Only one participant preferred to use the same password for everything that needs a password. Three participants preferred to use the option “remember password” as an acceptable method for easily remembering a password.
- As with the other group of students, the majority of the participants (6 out of 8) would identify a phishing attempt as an email message threatening

that access to accounts will be lost if username and password are not provided.

- Seven out of eight of the participants agree or strongly agree that information security training is considered very important.
- Concerning this group's familiarity with information security terms, there are a lot of similarities with the previous group. More specifically:
    - Participants feel familiar or very familiar with the terms Spam, Trojan and Virus.
    - Participants feel least familiar or not at all familiar with the terms Dumpster diving, shoulder surfing and spear phishing.
- In terms of visiting social networking sites the following habits apply as far as this group is concerned:

Social Network Site Habits (Senior Year students)	Number of respondents
Disclose very few details about yourself and only with people you trust	5
Don't accept invitations and offers from people you do not know and trust	6
Avoid installing programs and plugins that are not verified.	5
Check privacy settings and read the policy that governs the degree of sharing personal information.	7

Table 29: Group B - Social networking sites habits (Senior Year students)

The participants continued with the pre-assessment part of the security toolkit. No difficulty was observed in running and navigating around the unit. At the same time only two of the participants used the toolkit feature that allowed them to go back and review the answers provided and determine the correct options. The results of the participants' exposure to the pre-assessment unit are summarized as follows:

Student Group A – First Year Students			
Participants	**Introduction to Information Security**	**Human Aspects of Security**	**Review Feature**
Participant 1	Pass	Fail	Yes
Participant 2	Fail	Fail	No
Participant 3	Fail	Pass	No
Participant 4	Fail	Fail	No
Participant 5	Pass	Fail	Yes
Participant 6	Fail	Fail	No
Participant 7	Fail	Fail	No

Table 30: Group A - participants' exposure to the pre-assessment unit

Student Group B – Senior Year Students			
Participants	**Introduction to Information Security**	**Human Aspects of Security**	**Review Feature**
Participant 1	Pass	Fail	Yes
Participant 2	Fail	Fail	No
Participant 3	Fail	Pass	No
Participant 4	Fail	Fail	No
Participant 5	Pass	Fail	Yes
Participant 6	Fail	Fail	No
Participant 7	Fail	Fail	Yes
Participant 8	Fail	Fail	Yes

Table 31: Group B - participants' exposure to the pre-assessment unit

Representative screenshots of the exposure of participants to the pre-assessment unit are included below:

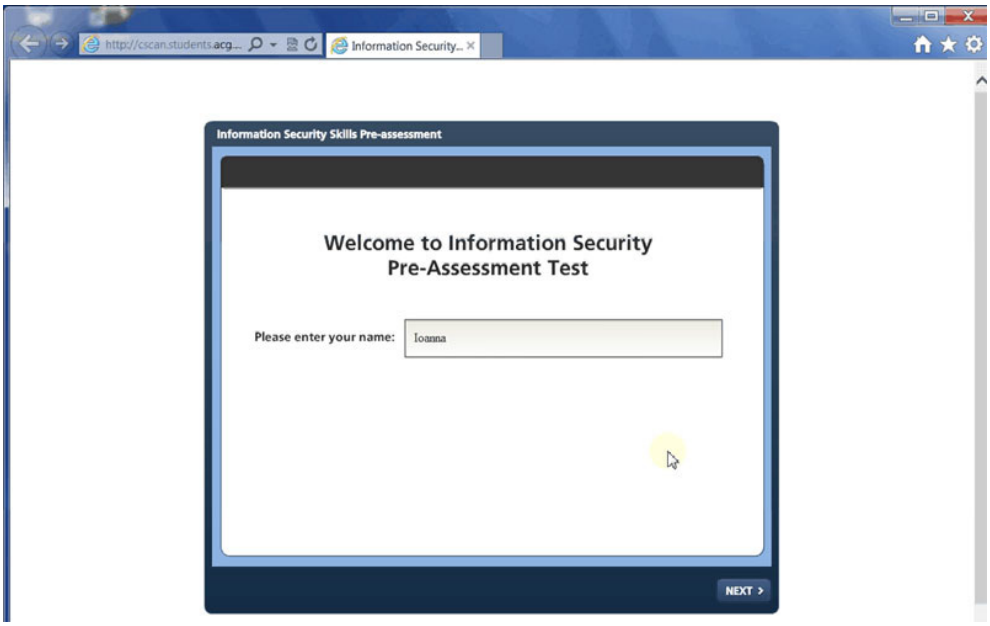


Figure 33: Pre-assessment unit introductory screen

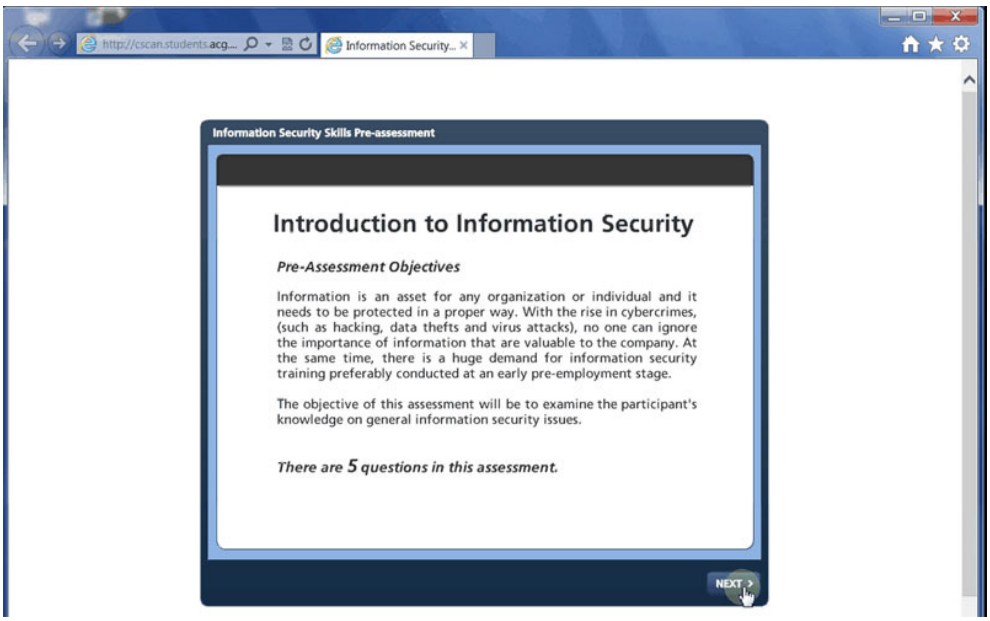


Figure 34: Pre-assessment unit objectives

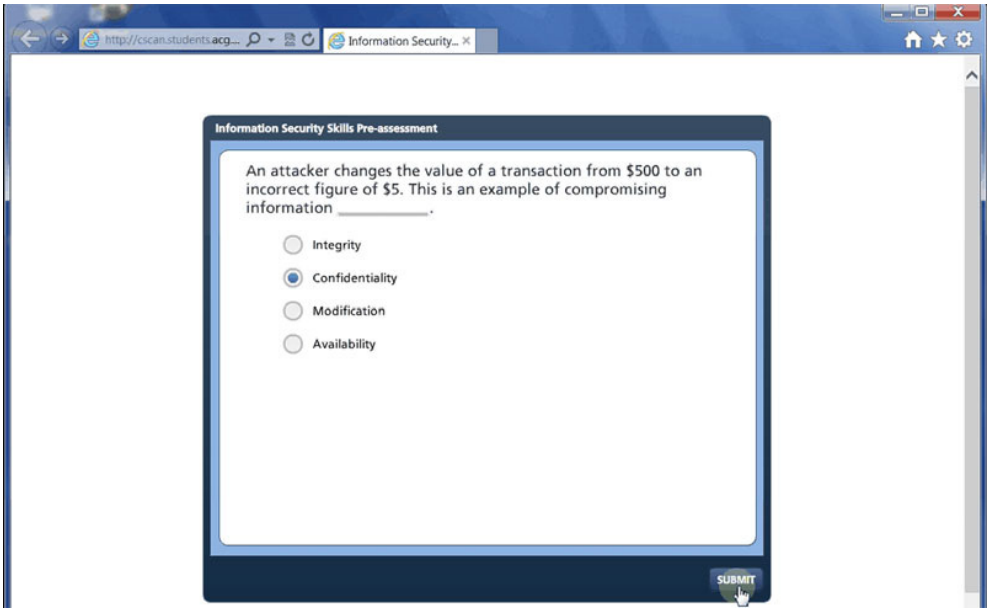


Figure 35: An actual question screen

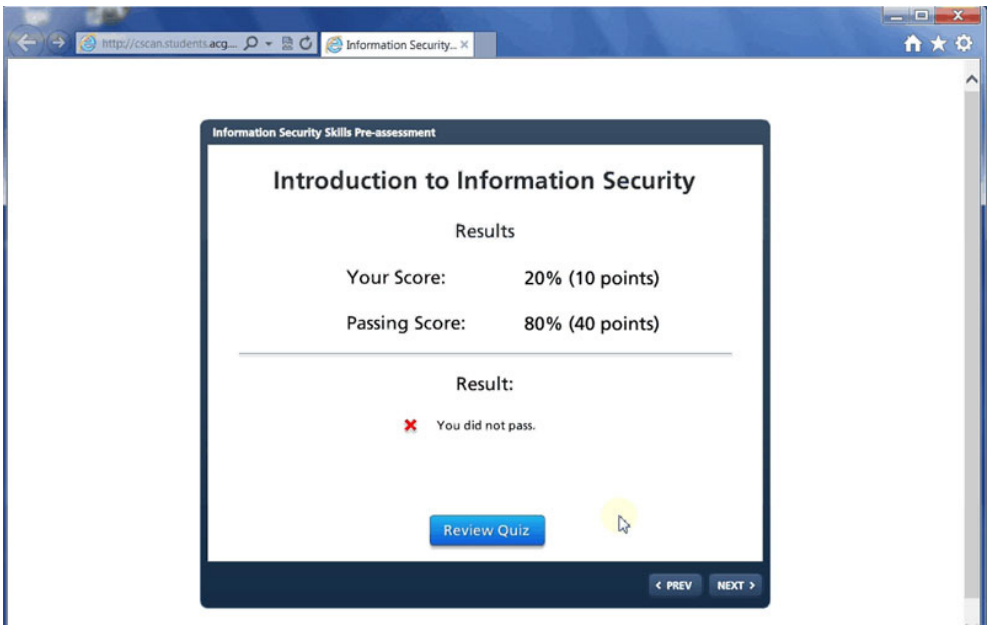


Figure 36: End of unit results screen

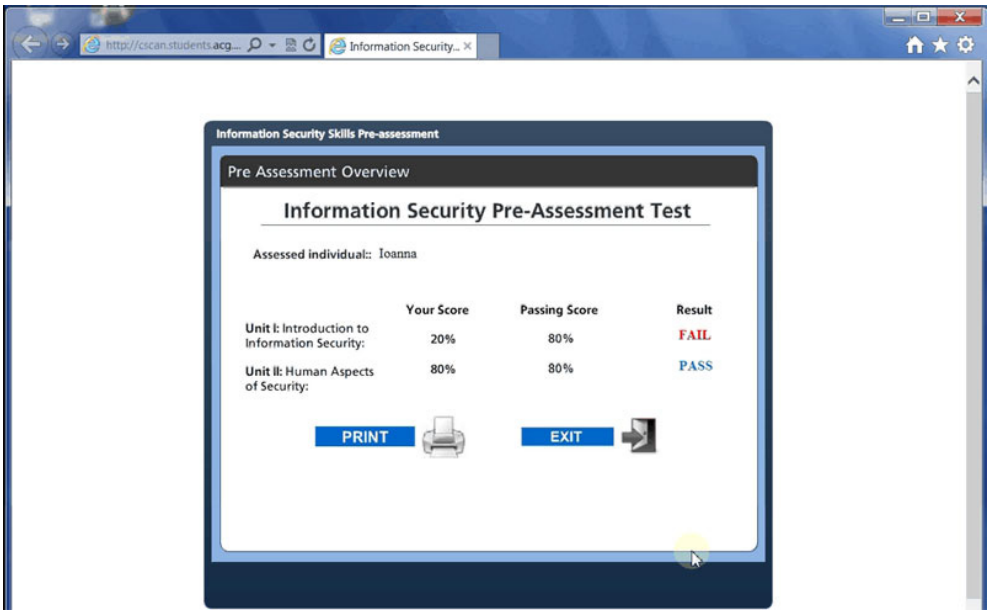


Figure 37: End of pre-assessment unit results screen

The moderator then continued by making a short introduction about the topic of information security and the need for security awareness raising for the general population. More specifically, without referring into technical terms, the topic of information security was defined in terms of confidentiality, integrity and availability using simple everyday example about each case along with its

importance in today's economy since all business operations are enabled by technology. Finally, the importance of the human factor in IS security was stressed since numerous security surveys identify that end users are the weakest link in the information security chain since they remain susceptible to phishing, are faced with password problems, do not use the Internet in a safe manner and are frequently subject to social engineering. Such cases, indicate the need for a more effective user training in order to raise the level of security awareness.

The participants were informed that they are going to watch a short e-learning unit that presents specific information security topics in an interactive way. The unit consists of two main areas and there is an assessment at the end of each area.

The whole e-learning unit experience went smoothly. Participants used the timeline buttons in order to play and pause the timeline as needed and the navigation buttons to move around the unit pages. On pages that contained interactive elements, participants used the hotspots in order to reveal additional content areas.

The results of the participants' exposure to the post-assessment unit are summarized as follows:

Group A – First Year Students			
	Introduction to Information Security	**Human Aspects of Security**	**Time to complete the e-learning unit**
Participant 1	Pass	Pass	26'
Participant 2	Pass	Fail	35'
Participant 3	Pass	Pass	37'
Participant 4	Pass	Pass	33'
Participant 5	Pass	Fail	27'
Participant 6	Pass	Pass	30'
Participant 7	Pass	Pass	29'

Table 32: Group A - participants' exposure to the post-assessment unit

Group B – Senior Year Students			
	Introduction to Information Security	**Human Aspects of Security**	**Time to complete the e-learning unit**
Participant 1	Pass	Pass	33’
Participant 2	Pass	Fail	35’
Participant 3	Pass	Pass	34’
Participant 4	Pass	Fail	40’
Participant 5	Pass	Pass	29’
Participant 6	Pass	Pass	35’
Participant 7	Pass	Pass	29’
Participant 8	Pass	Pass	25’

Table 33: Group B - participants’ exposure to the post-assessment unit

Representative screenshots of the exposure of participants to the e-learning unit are included below:

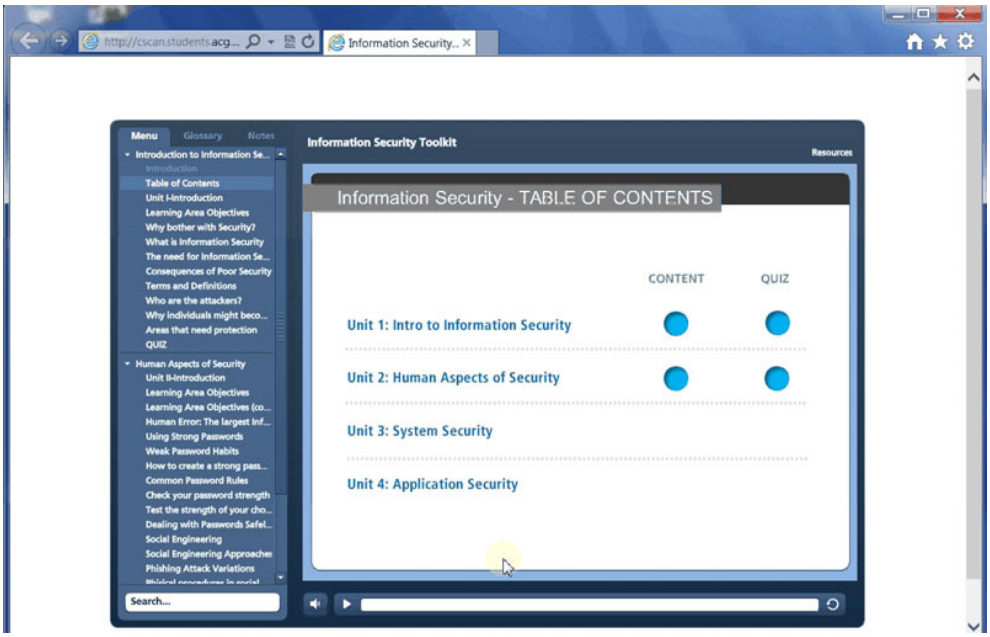


Figure 38: E-learning unit main screen.

Figure 39: Information Security definition and goals

Figure 40: Information Security terms and definitions

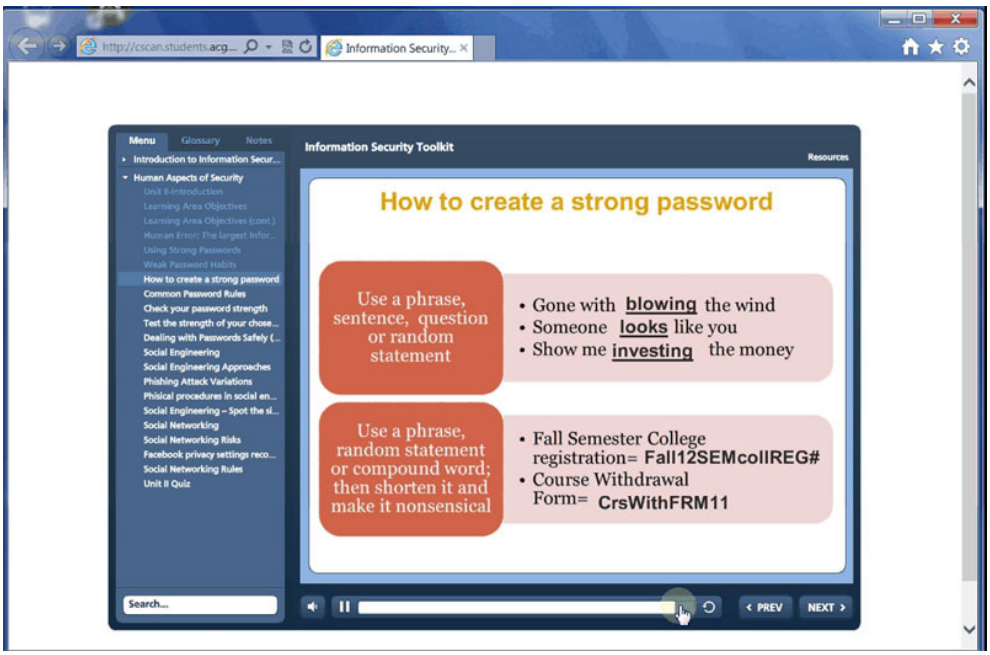


Figure 41: Tips on how to create a strong password

The Focus Group in action – Administrative Staff Group

The last focus group involved a group of 9 administrative staff employees (2 male and 7 female) that work at various administrative positions within the American College of Greece. As with the student groups, the same questionnaire was distributed to the group.

From the answers collected from the questionnaire the following observations were made:

- Seven out of nine participants own a computer with an Internet connection.
- The majority of the participants equally spend between 4 and 5 hours or between 6 and 8 hours online. This was justified since the majority of the participants daily work involves the use of a computer. There were also two participants who reported they spent more than 8 hours online.
- Compared with the student groups, the use of e-mail is by far the most common use of the Internet. Social Networking was not as commonly used

with respondents indicating a preference for Banking/Paying bills and Shopping.

- Half of the participants were neutral in the question of whether they possess the necessary knowledge to protect their computer and data with 2 out of the 9 respondents selecting either disagree of strongly disagree. Only one participant felt confident with their security knowledge.
- Among the methods that are in place in order to protect computer and electronic data, antivirus software was the first in the list followed by the use of a firewall and good passwords with regular backups the lowest rated.
- None of the participants felt comfortable in revealing their password. Concerning the choice of a safe password, 7 out of 8 participants would prefer a combination of letters in upper and lower case, digits and special characters that have a special meaning for them. At the same time 7 out of 9 participants did not use the same password for all services that need a password and nobody used the option to “remember password”.
- The majority of the participants (7 out of 9) would identify a phishing attempt as an email message threatening that access to accounts will be lost if username and password are not provided. The other two options are equally popular.
- The participants familiarity with information security terms can be summarized as follows:
    - The group seems familiar or very familiar with the terms “Spam”, “Trojan” and “Virus”.
    - The group seems least familiar or not at all familiar with most of the other terms including “Dumpster Diving” (100%), “Social

Engineering" (100%) and "Spear Phishing" (85%). At the same time a percentage close to 50% applies to the other terms.

- Almost 90% of the participant agree or strongly agree that information security training is considered very important.

In terms of visiting social networking sites the following habits apply:

Social Network Site Habits (Administrative staff)	Number of respondents
Disclose very few details about yourself and only with people you trust	8
Don't accept invitations and offers from people you do not know and trust	5
Avoid installing programs and plugins that are not verified.	6
Check privacy settings and read the policy that governs the degree of sharing personal information.	5

Table 34: Administrative staff - Social networking sites habits

The administrative staff participants continued with the pre-assessment part of the security toolkit. As with the student groups, no difficulty was observed in running and navigating around the unit. The results of the participants' exposure to the pre-assessment unit are summarized as follows:

Administrative Staff Group			
Participants	**Introduction to Information Security**	**Human Aspects of Security**	**Review Feature**
Participant 1	Pass	Fail	Yes
Participant 2	Fail	Fail	Yes
Participant 3	Fail	Pass	Yes
Participant 4	Fail	Fail	No
Participant 5	Pass	Fail	Yes
Participant 6	Fail	Fail	Yes
Participant 7	Fail	Fail	No
Participant 8	Pass	Fail	No
Participant 9	Pass	Pass	No

Table 35: Administrative staff - participants' exposure to the pre-assessment unit

As with the student groups, the moderator, after the pre-assessment completion continued with a similar introduction to the topic of information security and the importance for an appropriate security awareness level for the general population. More attention was drawn to the everyday security risks that employees may face as part of their information technology exposure in their everyday professional and personal life.

More specifically, the importance of the human factor in IS security was stressed based on facts and figures from widely publicized security surveys that identify end users as one of the most common causes of security breaches today.

The participants were also informed that they were going to watch a short e-learning video that presented specific information security topics in an interactive way.

The results of the participants' exposure to the post-assessment unit are summarized as follows:

Administrative Staff Group			
	Introduction to Information Security	**Human Aspects of Security**	**Time to complete the e-learning unit**
Participant 1	Pass	Fail	32'
Participant 2	Pass	Pass	40'
Participant 3	Pass	Pass	38'
Participant 4	Pass	Pass	33'
Participant 5	Pass	Pass	29'
Participant 6	Pass	Pass	30'
Participant 7	Pass	Fail	29'
Participant 8	Pass	Pass	38'
Participant 9	Pass	Pass	37'

Table 36: Administrative staff - participants' exposure to the post-assessment unit

6.4.1.1 Focus Group Discussion – Students Group

Student groups showed a great interest in the security toolkit and the way it was delivered especially in the case that it could be used as a substitute to a traditional instructor led course offered in a normal classroom setting. Although it is generally accepted that e-learning works best as a supplement to traditional forms of learning, the majority of the students expressed the opinion that such a subject would be best presented and covered using only e-learning means of delivery. Taking into account that most participants have a computer at home with Internet access, they were willing to accept this innovative way in order to learn at their own pace, use repetition if necessary and keeping themselves updated on the latest trends on information security.

Concerning the toolkit usability, the participants generally agreed that the toolkit was easy to use, useful and had a positive influence on them in adopting and using it further as an awareness raising system. One addition that one of the participants suggested was the creation of a “unit preparation” module (he actually mentioned that could be named “how to use this system”) that would demonstrate navigation aspects around the unit and special notations that are used (e.g. Hyperlink notations that are used for definitions inside text).

In terms of the toolkit effectiveness and depth of coverage, the students expressed their opinion that the toolkit can help them improve and complete their security knowledge that is needed for their everyday exposure with information technology. The presentation and coverage of information security terms was adequate along with the examples used and the rationale on why information security is important. The different types of attackers were well presented without any unnecessary technical coverage and at the same time some of the attacker

types that were new to them were presented clearly. Finally, the areas that need protection were presented briefly and clearly.

Concerning the human aspects of security module of the toolkit, the student participants understood why the focus of information security has shifted from efforts to erase data or corrupt a disk, to human elements, which are considered the weakest link in the information security chain. The qualities of a good password were sufficiently presented and the proposed methods and techniques of choosing one were easy to understand. The students really enjoyed testing the strength of their chosen password but at the same time expressed their concern that as the number of services that require password authentication constantly increases, it would be difficult in the future to avoid either using common passwords among services or choosing the remember password option. Concerning social networking sites and mainly the use of Facebook, although the participants agreed that the material concerning the risks associated with such sites was sufficiently presented, they expressed their doubts whether such sites really carry risks for which any user should be aware of. Although, they were all aware of security cases that have received a lot of attention by the media, they felt that such cases were very rare or over exaggerated. One participant expressed his personal opinion that Facebook and other social media sites, are a perfect example of freely expressing ideas in an anonymous way, that clearly contradicts with the way governments and official media want to filter and control the flow of information and for that reason they try to ban them by inventing risks that either do not exist or are very rare.

As a final word, it should be noted here that a small percentage of students from both groups failed the post-assessment part for the “Human Aspects of Security

unit. This is justifiable for the following reasons which also apply in the case of the administrative group presented in this chapter:

- Exposure to the whole toolkit was part of the focus group and time was limitations applied.
- Participants were exposed to the toolkit part only once, and did not had the time to go through it for a second time or at their own pace.
- This small failure rate was marginal. Because of the testing and evaluation purpose of the toolkit, the number of questions at the post-assessment unit were limited to five making it rather easy to fail. At the same time someone may consider the passing score (80%) as high. Both these aspects may be considered as contributors to this small failure percentage.

Despite this observation, the results from the users' exposure to the toolkit are considered successful.

6.4.1.2 Focus Group Discussion – Administrative Staff Group

From the discussion that followed the security toolkit exposure to the administrative staff group, it was clear that the participants value the importance of IT security for them as individuals and as part of a company, and realize the increased need for developing the necessary skills and competencies that will ensure the security of data and systems they operate. Although presented in the toolkit, most of the participants were well aware from publicized surveys and incidents that received a lot of media attention, that human actions are the principal reason for operational disturbances. Therefore they expressed their feeling that the toolkit can significantly contribute in an effort to raise the awareness level of employees and regulate their security behavior through a continuous learning process.

As mentioned before, most of the group participants own a computer at home but they are rather neutral in their opinion whether they possess the necessary knowledge to protect their computer and data. Their everyday data exposure deals with the management and processing of sensitive data and most of the participants may occasionally do company work at home which can add an extra level of risk concerning their exposure to security threats. For that reason they were very positive to the idea of the toolkit as a method of enhancing their security competencies. Although it was understood that the toolkit was rather a prototype model for supporting security awareness raising methods, they suggested that in its final and complete form, it could track not only which user logged in and went through it but also (through the mini quizzes at the end of each module) who has actually read and absorbed the material.

The participants felt that the toolkit was easy to use and presented in an efficient way and engaging way. The depth of coverage of the material was sufficient and the post-assessment quizzes could easily be answered after toolkit completion.

More specifically, the participants, although already familiar with the idea and importance of information security, through the toolkit exposure they could better link it with the concepts of confidentiality, integrity and availability and the examples associated with them. Similarly with the students group, the different types of attackers were well presented along with other types that they were unfamiliar with (e.g. Hactivists).

In terms of passwords and their use, the participants felt that the coverage of the topic importance and methods of creating a strong password was sufficient but also expressed their concern that as more and more online services require the

use of a strong password and at the same time force its periodic renewal, it would be difficult to easily remember all of them, thus driving them to insecure practices such as using the same password among services or writing down passwords.

In terms of social engineering, the toolkit helped identify its aspects and variations and at the same time classify threats that they were already been exposed (e.g. Spear phishing) without knowing the essence behind them. Moreover, since their everyday job has to do with dealing with sensitive data (e.g. Student information), the risks that may originate from dumpster diving and shoulder surfing were more clear for them.

Finally, concerning social networking, the group argued that they were very rare users of social networking sites and believed that the risks associated with such usage is very low, but at the same time, since most of them have young children, they felt that the presentation of such threats and safeguards from the toolkit was useful in their effort to mentor their children concerning safe online behavior.

6.4.2 Assessing toolkit effectiveness through surveying and expert group

As mentioned previously, the toolkit effectiveness was also tested using a group of individuals from institutions of higher education. The participants were involved in the learning process from various positions such as librarians, technology specialists, teaching and learning staff and instructional designers. This testing was done by exposing this group of experts to the toolkit and their opinions were measured and analyzed through a survey.

Surveys are considered an excellent tool for extracting and analyzing information from large number of respondents. The toolkit was presented to the participants

of the 2014 AMICAL Annual Conference organized by the AMICAL Consortium. AMICAL (American International Consortium of Academic Libraries) is an international consortium of liberal arts institutions of higher education based on the American educational model. Its mission is to advance learning, teaching and research through the collaborative development of library, information services and curricular resources among member institutions. The consortium has more than 26 institutions of higher education as members from 21 countries across Eastern, Central and Western Europe, West and North Africa, the Middle East, Central and Southern Asia, and Russia. The purpose of the presentation was to introduce the participants to the Information Security Toolkit as an interactive tool that teaches fundamental everyday security concepts in an effort to raise the participant's awareness level.

After the presentation, the participants were asked to evaluate the toolkit at their own pace (See Appendix IV). More specifically, an email invitation was sent to conference participants briefly stating the rationale behind the toolkit development and asking them to participate in evaluating its effectiveness. The participants had to go through:

- The pre-assessment part whose purpose was to determine the participant's knowledge on specific information security topics (through multiple-choice questions) and determine whether additional training is needed.
- The main e-learning unit that introduced essential everyday information security skills and provided guidance on how users can protect their computers, mobile devices and data from attacks, followed by a post-assessment unit that measured the knowledge assimilated.

Finally, after the completion of the above parts, participants were asked to evaluate the effectiveness and usability of the toolkit as a whole by completing a short survey. The survey was comprised of approximately 53 questions (see Appendix IV) divided into the following parts:

- A part that was assessing the effectiveness of the toolkit in relation to the material included in Unit 1 – Introduction to Information Security, of the toolkit. Consisted of multiple choice questions assessing both the e-learning and post assessment unit plus a final open ended question, allowing the participant to write down any particular comments and suggestions.
- A part that was assessing the effectiveness of the toolkit in relation to the material included in Unit 2 – Human Aspects of Security, of the toolkit following a similar question pattern as the previous part.
- A part that had the objective to briefly consider toolkit usability by including questions related to the presentation and vocabulary used in the system, flow control of information, system appearance in terms of colors, fonts, graphics and layout, and ease of system use.
- A final part that included questions in respect to overall toolkit satisfaction.

The survey invitation was sent to approximately 340 participants of which 116 responded (34.1% response rate). In terms of job function the participants can be classified as follows:

Job description	n	%
Library staff	15	12.93%
Technology specialist	13	11.21%
Instructional designer	12	10.34%
Distant learning specialist	12	10.34%
Teaching and learning staff	11	9.48%
Faculty	23	19.83%
Administrative staff	28	24.14%
Other	2	1.72%
Total	**116**	**100%**

Table 37: Survey participants by job function

Concerning the effectiveness of the "Introduction to Information Security" unit, the results can be summarized as follows:

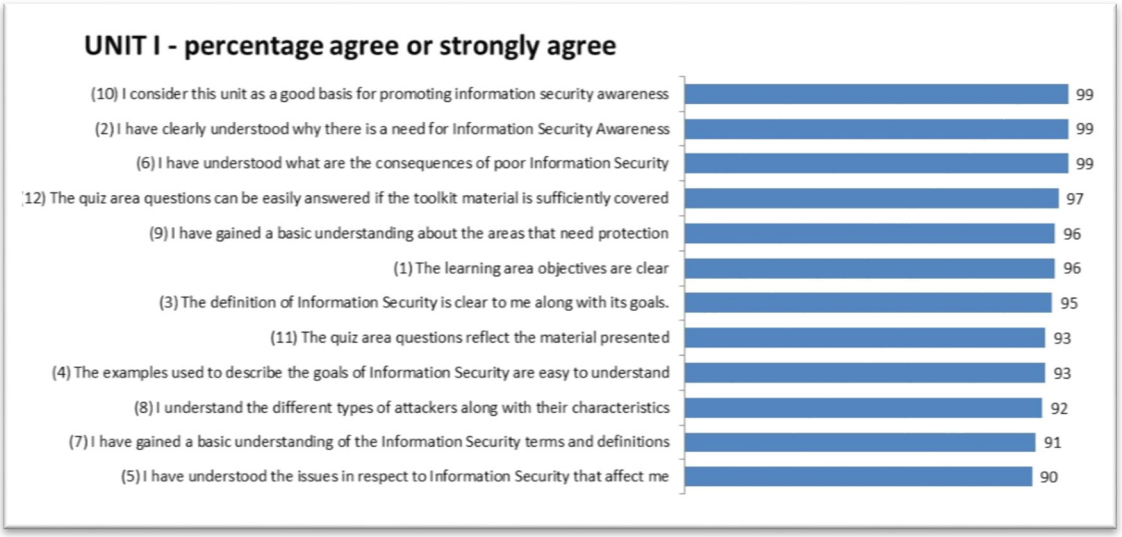


Figure 42: Introduction to Information Security unit. Percentage agree or strongly agree

The majority of the respondents considered the unit as a good basis for promoting information security awareness. From their exposure to the unit they felt that they understood the areas that needed protection and the different types of attackers along with their characteristics. Issues like the rationale and need for information security awareness along with the consequences of poor security were clear and understood. The definition of information security and the unit learning objectives

were clear. Participants felt that the post assessment questions covered the material presented and could be easily answered if the toolkit material was sufficiently covered.

When tabulating the results by job function, no significant differences are observed. The only variation that can be witnessed is that library staff have less "Strongly agree" answers when compared with the rest of the groups.

	Unit I percentage agree or strongly agree by job function						
Questions	Technology Specialist	Teaching and Learning staff	Library staff	Instructional designers	Faculty	Administrative staff	Distant Learning Specialist
The learning area objectives are clear	100%	100%	67%	100%	96%	100%	100%
I have clearly understood why there is a need for Information Security Awareness	100%	100%	100%	100%	96%	96%	100%
The definition of Information Security is clear to me along with its goals.	100%	100%	67%	100%	92%	100%	100%
The examples used to describe the goals of Information Security are easy to understand	100%	100%	67%	100%	92%	93%	100%
I have understood the issues in respect to Information Security that affect me	92%	100%	67%	67%	92%	93%	100%
I have understood what are the consequences of poor Information Security	100%	100%	100%	100%	88%	100%	100%
I have gained a basic understanding of the Information Security terms and definitions	100%	100%	67%	100%	88%	86%	100%
I understand the different types of attackers along with their characteristics	100%	100%	100%	100%	92%	71%	100%
I have gained a basic understanding about the areas that need protection	100%	100%	100%	100%	92%	86%	100%
I consider this unit as a good basis for promoting information security awareness	100%	100%	100%	100%	92%	100%	100%
The quiz area questions reflect the material	100%	100%	67%	100%	96%	89%	100%
The quiz area questions can be easily answered if the toolkit material is sufficiently covered	100%	100%	100%	100%	96%	86%	100%

Table 38: Introduction to Information Security unit. Percentage agree or strongly agree by job function

The survey questions in regard to "Human Aspects of Security" included a question about whether the unit has sufficiently covered the rules behind the use of biometric passwords. This material was not included in the unit and the question was used on purpose in order to detect whether participants had realized that such content was missing from the unit. Concerning the effectiveness of the "Human Aspects of Security" unit, the results can be summarized as follows:

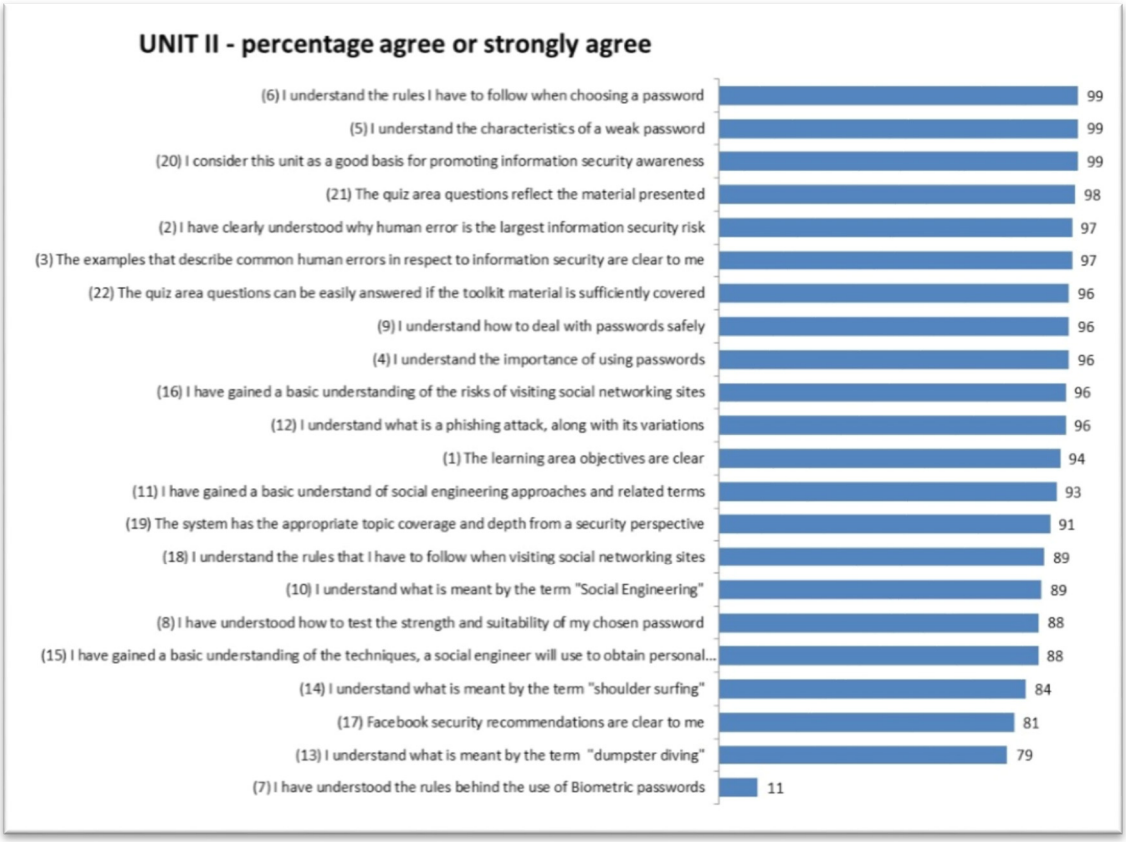


Figure 43: Human Aspects of Security unit. Percentage agree or strongly agree

The survey questions related to the unit effectiveness were concentrated around the following areas:

- Human error as the largest risk in Information Security.
- The concept of using passwords along with their importance and rules that should govern their creation.
- The presentation of social engineering concepts along with their risks in respect to information security.
- Social networking concepts, rules and methods of protection.

In general, participants felt that after the completion of Unit II of the toolkit, they had a good understanding of what constitutes a weak password and the rules that have to be followed when choosing a password. They understood the

importance of using passwords along with how to deal with them safely. Also the majority had expressed the opinion that they had an understanding on how to test the strength and suitability of their chosen passwords. Most of the respondents have clearly understood why human error is the largest information security risk and the examples that describe common human errors in respect to information security were clear. They felt that the post assessment questions covered the material presented and can be easily answered if the unit material is sufficiently covered. In respect of social engineering, although percentages are high, it seemed that the participants had expressed a small degree of concern over their understanding of the concept along with the terms associated with it. A similar concern had been observed in respect of the rules that have to be followed when visiting social networking sites. Concerning the question that examines whether the unit had sufficiently covered the rules behind the use of biometric passwords, the majority of participants had expressed their opinion that such material was not covered. Some of them even mentioned that in the open ended questions. On the other hand, it is worth to be mentioned that 31% of the participants that characterize their job function as “Technology Specialist” agree or strongly agree that they have understood the rules behind biometric passwords. It can be concluded that this group has come to this conclusion based on personal knowledge and experience as a result of their job function.

When tabulating the results by job function, no significant differences are observed.

	Unit II percentage agree or strongly agree by job function						
Questions	**Technology Specialist**	**Teaching and Learning staff**	**Library staff**	**Instructional designers**	**Faculty**	**Administrative staff**	**Distant Learning Specialist**
The learning area objectives are clear	100%	100%	67%	92%	100%	96%	100%
I have clearly understood why human error is the largest information security risk	100%	91%	100%	100%	100%	93%	100%
The examples that describe common human errors in respect to information security are clear to me	100%	100%	100%	100%	100%	82%	100%
I understand the importance of using passwords	100%	100%	100%	100%	100%	93%	67%
I understand the characteristics of a weak password	100%	100%	100%	100%	96%	93%	100%
I understand the rules I have to follow when choosing a password	100%	100%	100%	100%	96%	93%	100%
I have understood the rules behind the use of Biometric passwords	31%	0%	0%	17%	13%	11%	0%
I have understood how to test the strength and suitability of my chosen password	100%	100%	67%	100%	87%	79%	100%
I understand how to deal with passwords safely	100%	100%	100%	100%	96%	89%	100%
I understand what is meant by the term "Social Engineering"	100%	100%	100%	100%	96%	71%	67%
I have gained a basic understand of social engineering approaches and related terms	92%	100%	100%	100%	96%	68%	100%
I understand what is a phishing attack, along with its variations	92%	100%	100%	100%	96%	93%	67%
I understand what is meant by the term "dumpster diving"	92%	100%	67%	67%	96%	46%	100%
I understand what is meant by the term "shoulder surfing"	77%	100%	67%	67%	96%	71%	67%
I have gained a basic understanding of the techniques, a social engineer will use to obtain personal information	100%	64%	100%	100%	91%	64%	100%
I have gained a basic understanding of the risks of visiting social networking sites	100%	100%	100%	100%	96%	93%	67%
Facebook security recommendations are clear to me	100%	64%	67%	67%	87%	75%	67%
I understand the rules that I have to follow when visiting social networking sites	100%	64%	100%	100%	91%	89%	67%
The system has the appropriate topic coverage and depth from a security perspective	100%	100%	67%	100%	83%	86%	100%
I consider this unit as a good basis for promoting information security awareness	100%	100%	100%	100%	96%	93%	67%
The quiz area questions reflect the material presented	100%	100%	100%	100%	96%	86%	100%
The quiz area questions can be easily answered if the toolkit material is sufficiently covered	100%	100%	100%	100%	96%	82%	100%

Table 39: Human Aspects of Security unit. Percentage agree or strongly agree by job function

In respect to the usability of the toolkit, the following results have been observed:

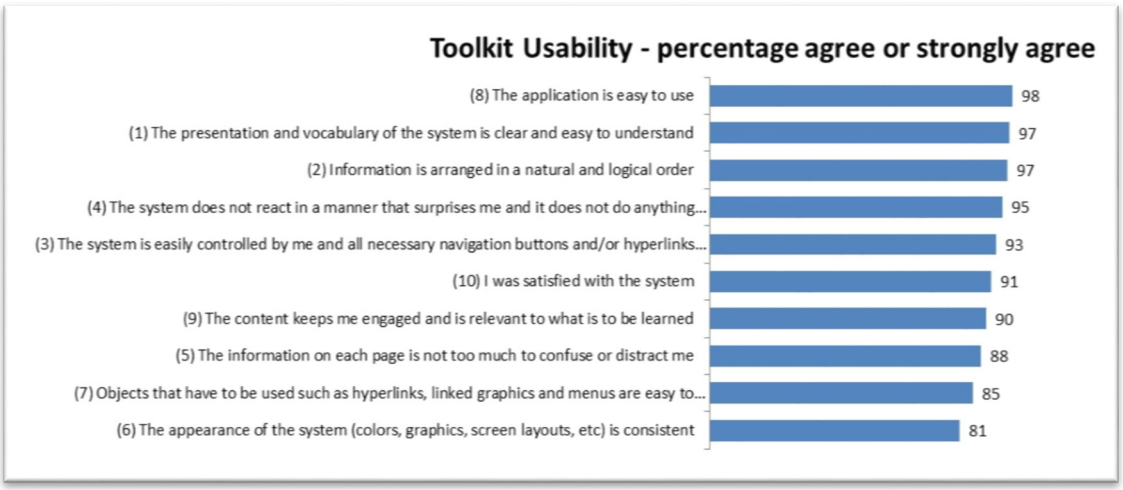


Figure 44: Toolkit Usability. Percentage agree or strongly agree

Although the objective of this survey was not to thoroughly examine the usability of the toolkit but rather assess its effectiveness, the vast majority of the respondents considered the application as easy to use with information arranged in a natural and logical order and presented in a clear and easy to understand way. In general, participants were satisfied with the system which kept them engaged with content that is relevant to what is to be learned. The only usability concern that is observed – although the percentage recorded is not significant – has to do with the appearance of the system in terms of colors, graphics and screen layouts and the ease of recognition in respect of hyperlinks, linked graphics and menus. Taking into account the graphical richness of modern websites and Internet applications such an observation should be taken into consideration when a full scale deployment of the toolkit is considered in order to achieve a perfect balance between toolkit appearance and functionality. Such observation is common among participants whose job function has been reported as “Distant learning specialist” as it is shown by the table below:

	Toolkit Usability - percentage agree or strongly agree by job function						
Questions	Technology Specialist	Teaching and Learning staff	Library staff	Instructional designers	Faculty	Administrative staff	Distant Learning Specialist
The presentation and vocabulary of the system is clear and easy to understand	100%	100%	100%	100%	100%	89%	100%
Information is arranged in a natural and logical order	100%	100%	100%	100%	96%	89%	100%
The system is easily controlled by me and all necessary navigation buttons and/or hyperlinks are present and easily used	100%	100%	67%	100%	96%	93%	100%
The system does not react in a manner that surprises me and it does not do anything unexpected	100%	100%	67%	100%	96%	100%	100%
The information on each page is not too much to confuse or distract me	100%	100%	33%	100%	96%	89%	100%
The appearance of the system (colors, graphics, screen layouts, etc) is consistent	100%	100%	67%	100%	100%	82%	0%
Objects that have to be used such as hyperlinks, linked graphics and menus are easy to recognize	100%	100%	67%	100%	96%	86%	33%
The application is easy to use	100%	100%	100%	100%	100%	93%	100%
The content keeps me engaged and is relevant to what is to be learned	100%	100%	67%	100%	91%	89%	100%
I was satisfied with the system	100%	100%	67%	100%	96%	93%	100%

Table 40: Toolkit Usability. Percentage agree or strongly agree by job function

A similar observation is reported by Library staff in respect to whether the amount of information on each page of the toolkit can cause confusion or distraction.

In terms of overall toolkit satisfaction the results can be summarized as follows:

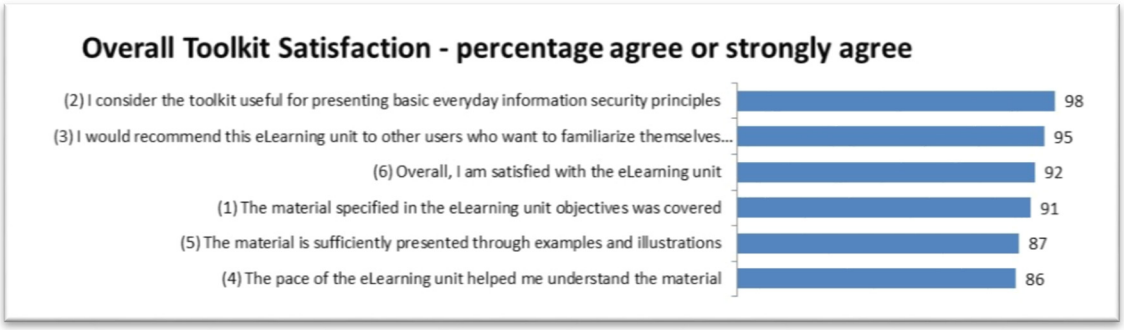


Figure 45: Overall Toolkit Satisfaction. Percentage agree or strongly agree

The majority of the participants consider the toolkit as useful for presenting basic everyday information security principles and would recommend it to others that want to familiarize themselves with such security principles. Overall, 92% of the participants are satisfied (agree or strongly agree) with the eLearning unit.

When comparing the results by job function, a small degree of skepticism is expressed by library staff in regard to the pace of the eLearning unit and whether such pace has helped in understanding the material.

	Overal Toolkit Satisfaction - percentage agree or strongly agree by job function						
Questions	Technology Specialist	Teaching and Learning staff	Library staff	Instructional designers	Faculty	Administrative staff	Distant Learning Specialist
The material specified in the eLearning unit objectives was covered	100%	100%	67%	100%	91%	86%	100%
I consider the toolkit useful for presenting basic everyday information security principles	100%	100%	100%	100%	100%	93%	100%
I would recommend this eLearning unit to other users who want to familiarize themselves with basic everyday security principles	100%	100%	100%	100%	100%	86%	100%
The pace of the eLearning unit helped me understand the material	100%	100%	33%	100%	96%	82%	100%
The material is sufficiently presented through examples and illustrations	100%	100%	67%	100%	87%	75%	100%
Overall, I am satisfied with the eLearning unit	100%	100%	67%	100%	100%	86%	67%

Table 41: Overall Toolkit Satisfaction. Percentage agree or strongly agree by job function

A similar but much smaller concern is expressed by the same group in regard to the appropriate coverage of the material through examples and illustrations.

6.4.3 Assessing toolkit effectiveness through and IT expert group

The toolkit effectiveness was finally tested using a group of individuals that are considered experts in the IT field. The participants are closely involved in the IT function from various positions such as IT system administrators, IT managers, IT consultants and security experts. This testing was done by exposing this group of IT experts to the toolkit and their opinions were measured and analyzed through a survey. Additionally, a deeper analysis of their thoughts on the toolkit as a whole and the information security awareness topic was documented by conducting short semi-structured interviews.

The invitation to participate was sent to 14 participants and all of them agreed to participate to the whole process. In terms of IT related job function, the participants can be classified as follows:

Job Function	Participants
IT Consultants	3
IT System Administrators	2
IT Managers/Directors	4
IT Helpdesk specialists	3
IT Security experts	2

Table 42: IT Experts group, participants by job function.

The experts that participated are considered qualified individuals with years of experience in their field of expertise and therefore their opinion is considered valid and credible. More specifically:

- All three IT Consultants are working for big multinational consulting companies (two in Europe and one in the US) specializing in IT Advisory and Business Risk services. They are all holders of relevant information security certifications (e.g. CISA, CISM, CISSP) and their job responsibilities, among others, include advisory services in assisting companies achieve maximum value from the use of IT by applying best security practices in order to protect their information assets.
- The IT System Administrators that participated are members of the system administration team of two large Internet service providers and a significant part of their everyday jobs deals with detecting and coping with security threats either from external sources such as intruders or internal ones such as careless staff.
- From the group of IT Managers and/or Directors two of them are directing the IT function of two large European universities. Their opinion is considered of high value since experts in computer security agree that computer security tends to be weaker at universities and one of the most commonly identified problems is that educational institutions are not doing

enough to encourage students as well as other campus users to protect their campus accounts (Foster, 2004).

- The helpdesk specialists are leading a team of helpdesk staff dealing with everyday user problems and help requests. All three work in Greek companies that specialize in outsourcing helpdesk services to organizations that either do not have qualified IT staff or do not want to invest in an internal helpdesk office. Their opinion is considered credible since everyday they receive numerous help requests for IT problems where many of them are security related.
- Finally, both security experts that participated has significant work experience in the internal audit and control divisions of two major Greek banks and their daily job routine among others has to do with dealing with the risks to security of information or data, incident analysis and investigation, information security testing, etc.

Similarly like the previous group of experts, an email invitation was sent to the group participants briefly stating the rationale behind the toolkit development and asking them to evaluate it at their own pace (See Appendix V). The participants had to go through the following evaluation sequence:

- The pre-assessment unit which objective was to assess the participant's existing knowledge.
- The main e-learning unit that introduces essential everyday information security skills and provides guidance on how users can protect their information assets, followed by a post-assessment unit for measuring the knowledge assimilated.

- Then, group participants were asked to evaluate the effectiveness and usability of the toolkit by completing a short survey comprised of approximately 45 questions organized in a similar way as the previous group of participants.
- Finally, short interviews were organized with each one of the group participants where their exposure to the toolkit along with their views and opinions were discussed more deeply.

As far as the group's responses to the survey are concerned, in terms of effectiveness of the first unit – "Introduction to Information Security" – the results can be summarized as follows:

Survey Question	**Participant's answers**				
	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
The learning area objectives are clear.	10	4	0	0	0
The unit clearly describes why there is a need for Information Security Awareness.	11	2	1	0	0
The definition of Information Security is clear along with its goals.	7	7	0	0	0
The examples used to describe the goals of Information Security are easy to understand.	6	8	0	0	0
The issues in respect to Information Security that affect users are clearly understood.	7	7	0	0	0
The consequences of poor Information Security are clearly understood.	9	4	1	0	0
The participant will gain a basic understanding of the Information Security terms and definitions.	5	9	0	0	0
The different types of attackers along with their characteristics are clearly understood.	4	9	1	0	0
The areas that need protection are clearly understood.	5	8	1	0	0
I consider this unit as a good basis for promoting information security awareness.	10	4	0	0	0
The quiz area questions reflect the material presented.	11	3	0	0	0
The quiz area questions can be easily answered if the toolkit material is sufficiently covered.	9	5	0	0	0

Table 43: IT Experts group, Introduction to Information Security unit. Participant responses.

The majority of the respondents either agree or strongly agree that this unit is a good basis for promoting information security awareness. They believe that there is a clear definition of information security and the examples used to promote its goals are sufficient. There is an adequate coverage of the most commonly used information security terms and the material coverage is in coherence with the quiz

area questions. Very small variations that are recorded in a few questions are considered insignificant.

Concerning the effectiveness of the “Human Aspects of Security” unit, the results can be summarized as follows:

Survey Question	Participant's answers				
	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
The examples that describe common human errors in respect to information security are clear.	8	6	0	0	0
The importance of using passwords is clearly understood.	12	2	0	0	0
The characteristics of a weak password are clearly understood.	9	3	2	0	0
The rules a user has to follow when choosing a password are clear.	5	9	0	0	0
The participant will understand how to test the strength and suitability of his chosen password.	10	4	0	0	0
The participant will understand how to deal with passwords safely.	6	8	0	0	0
The participant will understand what is meant when using the term “Social Engineering".	6	7	1	0	0
The participant will gain a basic understanding of social engineering approaches and related terms.	5	9	0	0	0
The participant will understand, what is a phishing attack, along with its variations.	8	6	0	0	0
The participant will understand what is meant by the term ‘dumpster diving’.	8	6	0	0	0
The participant will understand what is meant by the term ‘shoulder surfing’.	9	5	0	0	0
The participant will gain a basic understanding of the techniques, a social engineer will use to obtain personal information.	10	4	0	0	0
The participant will gain a basic understanding of the risks of visiting social networking sites.	4	9	1	0	0
Facebook security recommendations are clear.	0	3	9	2	0
The rules a user has to follow when visiting social networking sites are clear.	1	11	2	0	0
The system has the appropriate topic coverage and depth from a security perspective.	3	11	0	0	0
I consider this unit as a good basis for promoting information security awareness.	6	8	0	0	0
The quiz area questions reflect the material presented.	10	4	0	0	0
The quiz area questions can be easily answered if the toolkit material is sufficiently covered.	8	6	0	0	0

Table 44: IT Experts group, Human Aspects of Security. Participant responses.

Similarly as the previous unit, the participants believed that the unit is a good basis for promoting information security awareness and the quiz questions presented at the end can be easily answered from the material covered.

Important information security terms are clearly understood and the issue of social engineering as a method of obtaining personal information is adequately

covered. The use of password as a method of enhancing security along with the rules that have to be followed in order to choose a string password can be easily understood and followed by the unit participants.

The only variations by this testing group are recorded in the case of social networking sites. Although the opinions concerning the unit's coverage are not significant, the majority of the respondents feels that security recommendations concerning social networking sites and especially Facebook may need some more attention and further revision. In the overall, the unit is considered a good basis for promoting information security awareness by the majority of the respondents.

Concerning the usability of the whole unit, the results can be summarized as follows:

Survey Question	**Participant's answers**				
	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
The system uses a language that is natural, easily understood and similar to one that may be used in a day-to-day or study environment.	7	6	1	0	0
I am not confused by the use of terms and the way symbols, icons or images are presented.	5	9	0	0	0
Information is arranged in a natural and logical order.	9	5	0	0	0
The system is easily controlled by me and all necessary navigation buttons and/or hyperlinks are present and easily used.	7	7	0	0	0
The system does not react in a manner that surprises me and it does not do anything unexpected.	7	7	0	0	0
The information on each page is not too much to confuse or distract me.	6	7	1	0	0
Colors, graphics, icons and images are used in a consistent way throughout the system.	2	9	3	0	0
There is consistency in screen layouts, use of font types and sizes.	2	9	3	0	0
Objects that have to be used such as hyperlinks, linked graphics and menus are easy to recognize.	6	7	1	0	0
The application is easy for novice users to use.	8	6	0	0	0
The content keeps me engaged and is relevant to what is to be learned.	6	5	3	0	0
I was satisfied with the system.	6	8	0	0	0

Table 45: IT Experts group, toolkit usability opinions.

The majority of the group respondents during the personal interviews, discussed later in this chapter, expressed their opinion that deciding on aspects on toolkit usability is not their field of expertise but were rather expressing their personal opinion from their engagement with the toolkit prototype.

The main points concerning the toolkit usability as it is observed by this group can be summarized as follows:

- The whole unit uses a language that is easy to understand and can be used in a typical day-to-day environment addressed for novice users.
- The flow of the system is natural, easily understood by a novice user without any confusion or unexpected system behavior.
- Information presented at each different topic area is consistent without involving too much information that would confuse or distract the user.
- In the overall the majority of the respondents of this group believe that the system is usable, has a content that is relevant to what is to be learned and keeps the learner engaged.

The only areas of concern expressed by this group – although the number of responses are not significant – has to do with the with the appearance of the system in terms of colors, graphics and screen layouts and the ease of recognition in respect of hyperlinks, linked graphics and menus. This opinion is in significance with what has been reported by the experts group previously, where a concern in regard to the graphical richness of modern websites and Internet applications has been expressed. Such observation is suggested to be taken into consideration during a full scale deployment of the toolkit in an effort to achieve a perfect balance between appearance and functionality.

6.4.3.1 Using Interviews

Similarly like focus groups, interviews as a method of data collection, can be used in qualitative research in order to explore the views, experiences, beliefs and motivations of individual participants. They provide a deeper understanding of a specific research topic and are most appropriate when detailed insights are required from individual participants especially when quantitative data (mainly collected from questionnaires) is not considered enough (Seidman, 2012; Brinkmann and Kvale, 2014).

There are three types of research interviews:

- Structured interviews. These take the form of a verbally administered questionnaire with a list of predetermined questions. These questions are asked to the participant with little or no variation and with no intention to continue with follow-up questions to given responses that may require further elaboration. For that reason, structured interviews are relatively quick and easy to administer and may be useful if clarification for specific questions is required or if the respondents have literacy problems. Generally, they are of little use if further depth is required.
- Unstructured interviews. These usually do not follow any predetermined theory and are performed with little or no organization at all. It usually starts with an opening question such as “Can you describe me your experience with doing this?” and the interview progresses primarily upon this first response. Unstructured interviews are usually time consuming and can be difficult to manage. Also the lack of pre-determined questions provides little guidance on what to talk about and requires excellent interviewer skills especially on subject areas where virtually nothing is known.

- Semi-structured interviews. Semi-structured interview fall somewhere in between the above described categories. They usually start with several key questions that help define the areas to be explored and further allow both parties to deviate accordingly if an idea or opinion needs to be pursued in more detail. Comparing this method with structured interviews, it provides more flexibility because it allows more discovery and elaboration of information. At the same time ideas not previously been expressed can easily emerge from the participants in a similar way as the unstructured interviews.

An important first step in conducting a successful interview is to prepare an interview guide (Gill et al., 2008). During this process the following important points were taken into consideration:

- It is important for the interviewer to introduce himself and explain the aim of the interview so the interviewee is fully aware of the research purpose.
- Assure the interviewees about the confidentiality and anonymity of the interview.
- Prepare the questions having in mind that:
    - Questions should be relevant to the research question.
    - Questions should follow a logical sequence.
    - Questions are organized in such a way so it is easy to move between different topics as the interviewee may naturally move on another subject.
    - Questions are clear and easy to understand taking into consideration the person interviewed.

- Questions do not provoke a specific answer but instead allow people to feel free and give their own, honest answers.

The type of interview chosen was the semi-structured one because it combines the qualities of both structured and unstructured interviews. More specifically, at the beginning of the interview, the participants were asked a few key questions in regard to their profession, job description and duties and years of experience. Then the interview continued in a more open and unstructured way on the topic of information security awareness having the toolkit as a starting point and point of reference.

6.4.3.2 The IT Experts group interviews

As mentioned before, the evaluation of the toolkit from the IT experts group continues with a semi-structured interview. At the beginning of the interview, the participants were asked a few key questions in regard to their profession, job description and duties and years of experience. The last key question had to do with whether the participants feel that information security is an important component of the digital life of the everyday user and the role that awareness of information security risks has to play in establishing an appropriate level of culture. This question served as the point where the interview continued in a more open and unstructured way on the topic of information security awareness having the toolkit as a starting point and point of reference. All interviews lasted not more than 90 minutes. The results presented below are summarized by job function of each participant.

The group of participants that can be classified as IT consultants believe that the raising the level of security awareness is very important for the everyday user taking into consideration that cybercrime has risen significantly, especially in Europe where incidents have increased by over 40% since the year 2013. In order to understand the level of this increase it important to mention that it is more than double of the global GDP and global smartphone users combined. This serious percentage has its roots also to insider's incidents. Although not the only source of security incidents, they carry more serious implications in terms of cost. Taking into consideration that security budgets either remain stable or report a decline over the last three years, organizations should seek to implement the necessary processes and technologies to "prevent, protect, detect, and respond to elevated threats". Among prevention and protection measures, employee security awareness and training programmes are the areas that need to be strengthened.

Initiatives, like the development of the prototype toolkit, are always welcomed taking into consideration that implementation of such key safeguards has declined over 2013. Such efforts can greatly help in raising the overall awareness level especially if addressed to the general population and provide an extra advantage for companies in safeguarding their resources. The overall toolkit design and presentation is considered sufficient taking into account that the toolkit is easily accessible either by using a laptop or a mobile device and its presentation of topics is easy for the everyday user to follow. This group of participants could not say a lot concerning the overall presentation of the toolkit in terms of colors, graphics and images but felt that maybe this is something that has room for improvement in order for the topics presented achieve an optimum result.

Further to the topics and the material presented, this group of respondents believed that the way everyday security problems are presented is simple and to the point without exposing the user to too much or complicated information. Especially in the case of passwords and how it should be chosen, the toolkit provides an easy and friendly method on how passwords that are strong and easily remembered should be constructed.

The area that this group felt it needs some further attention and improvement is the one that deals with the rules a user has to follow when visiting social networking sites and especially Facebook. One participant believed that an online demo similar to the one that helps users in choosing a strong password would be helpful although difficult to create taking into consideration the frequent changes of the social networking sites environment.

Finally, this group believed that the toolkit could be further enhanced by taking into consideration the following:

- Include links to short documents, mainly in pdf format, where more detailed descriptions are provided for specific security issues already included in the toolkit pages although this contains the risk of not actually being visited or seriously considered by the user.
- Possibility to provide one additional option at the main screen of the toolkit (currently the existing options for each unit are “content” and “quiz”) called “demos” which will be solely dedicated in provided screen-by-screen demonstrations on important security topics (e.g. step-by-step guide on how to change our password). It was felt that such an addition would add

an extra level of friendliness to the toolkit by directing users on easy to understand everyday security steps.

- It might be helpful to subdivide each unit into smaller units and also give the participant to opportunity to "jump" directly and complete this subunit at his own pace. For example, "Human Aspects of Security" could include its main title at the table of contents, giving the opportunity to the participant to cover the whole unit at once but also provide its distinct areas (e.g. Using passwords, understanding social engineering, dealing with social networking risks, etc.) as separate links for the participant to complete.

The opinions of the people classified as IT Managers are very close with the ones classified as IT System Administrators. Both group participants believe that the greatest threat to information security comes mostly from uneducated employees and their negligent actions which are considered the top cause for organizational data breaches. All group participants during the interviews were able to report that they have experienced numerous incidents in their companies where the negligence of their employees has resulted in unintentional data loss.

In order to cope with such issues the basic approach that their companies follow has to do with the establishment of an information security policy and efforts for it to be consistent throughout the company. Although they are aware that this is not the case for a lot of organizations today due to significant budget cuts to information security spending, still it is considered the most suitable approach. The main principles that were expressed as part of this information security policy include:

- Information security measures dedicated to the preservation of confidentiality, integrity and availability.
- A clear definition of organizational responsibility in order to ensure proper implementation of information security measures.
- Provision of awareness and education programs on information security for all executives and employees in order to ensure the proper implementation of security measures.

Considering the last principle, most participants reported that such a program is either in place or being at the final stages of its development. Its main characteristics involve actions and learning initiatives similar to the ones described in the toolkit. Also, the topics presented at the toolkit prototype are part of the awareness initiatives already in place, plus some additional ones like the use of posters at respective office locations, awareness stickers at all company PCs and other measures.

As far as the toolkit prototype itself, the participants of this group believed that it contains all the necessary coverage in order to help achieve an appropriate level of employee awareness. Especially the first unit – Introduction to Information Security – was considered an essential step in order to set the stage, describe the existing environment and most importantly make the employees understand not only the existing threats but also the personal responsibility that are derived from these threats. At this point, some participants believed that it would be helpful to include some additional pages totally addressed to employee responsibility.

Concerning the “Human Aspects of Security” part, the participants believed that it has adequate coverage and focus upon the weakest link of the information

security chain – the human element and material is presented in a simple but understandable way. Some additions suggested here included elements that may be specific to the protection policies established by each company like the use and implementation of two factor authentication and the policies that exist at each company in respect to the use of social networking sites. Especially concerning the use of social networking sites, because some participants believed that such sites not only are not banned but instead are used as part of the company's marketing and promotion initiatives extra care should be taken so employees are "not that social in their use of social networking" and update the policies regarding such use regularly.

Finally, this group believed that the toolkit could be further utilized by taking into consideration the following suggestions:

- Be part of an overall employee orientation plan or as an important element of a new employee welcome "kit". Some companies as part of their recruitment process engage prospective employees in a series of tests (e.g. skills, character or psychological tests) and inclusion of tests involving the security awareness of a future employee could be included.
- Be considered as part of an overall employee continuous education and development program where employees have to go through periodically, refresh their knowledge and skills and the completion and success level is used as an additional evaluation method for promotion and succession.
- Establish additional mechanisms where the effectiveness of the toolkit as an awareness raising method is continuously evaluated by measuring the resulting information security culture as a result of toolkit engagement.

IT helpdesk specialists are usually considered the first point of contact for all everyday security incidents and related questions. It is the most common place where a user turns to resolve a problem related to IT matters and acts as a hub of activity with its primary goal of solving user issues as quickly and effectively. This interview participants have reported that most helpdesk requests have to do with security incidents or questions and are the result of either uneducated or negligent employees. Almost 8 out of 10 requests have to do with either loss of access questions followed by password reset requests.

From the interview it appeared that although helpdesk request specialists believe that the toolkit is useful and could further serve as a method of security awareness raising method, they have doubts on how in the overall this could have a real value unless it is part of an overall organizational security policy. One of the participants freely expressed that:

> *"Every day I receive the same security request –usually associated with password resets or how to access questions– from the same people that usually involve the same courses of action. They simply do not care, nor do they understand the consequences of their actions of negligence. They know that we are here to solve their "problem" again and again. Top level management seems not to care either as far as helpdesk requests are solved quickly". I do not see how the toolkit could help unless it is enforced by a strict organizational policy that is backed up by top management".*

For helpdesk specialists that have an automated helpdesk system where requests are at first electronically logged and –based on the actual ticket request- feedback and possible courses of action are suggested so the user can solve the problem on its own, still a significant number of such requests finally reaches the helpdesk technician for face-to-face resolution.

Despite the concerns described previously, in the overall the toolkit is considered a useful step in an effort to raise the awareness level in terms of security issues.

Still it has to be backed up by a respective organizational policy supported by top level management. Based on the requests that they receive every day, helpdesks specialists believe that users are totally unaware about the consequences of their actions. First of all, very few have a clear idea about what is information security, what it involves and more importantly what is the role they have to play in the overall organizational security strategy. Many believe that “IT is here to protect me”. For those reasons, the first unit of the toolkit is considered of crucial importance since it will set the scene for information security appropriate behavior and most importantly define the level of employee commitment to it. At this point some participants further suggested that it may include additional “pages” that clearly describe the required responsibilities for each employee along with the personal consequences of any actions that lead to security incidents.

The second unit deals in a more focused way with actions related to employees everyday security behavior and it is presented in a friendly and easy to understand way. Still the opinion was expressed that the interface could be further enhanced by employing modern graphics and presentation techniques. The assistance of graphics and interface designers at this point could be proven beneficial. Finally, the part concerning the use of social networking sites and the rules a user has to follow when visiting and engaging with them securely is a place that may need further consideration. The suggestion at this point was to include additional examples and step-by-step guides concerning protection. In addition the policy of the company in respect to the use of these sites should be included.

The group of information security experts believed that security awareness raising efforts similar to the toolkit are here to stay and should be supported and properly financed. Taking into consideration that security budgets during the last

five years have remained stable –and this is the best case scenario- companies do not have the means of investing in critical awareness raising methods that deviate from the norm. Most companies usually refer to ready-made materials that are addressed to information security awareness with little or not at all provision of customization in order to address specific policies and make it more friendly or personal to the user. At the same time, existing well-established security awareness websites providing free resources, despite the wealth of information provided, information is presented in an unstructured way. A user who is security aware may easily visit such sites and either learn more on a specific subject or use the materials to create his own awareness campaign. But unfortunately this is not the case with novice users who actually are not aware of security issues and can achieve a complete learning outcome by using a structured and guided learning package.

The information security experts interviewed believe that the toolkit is a good basis for security awareness raising initiatives and has the appropriate length and coverage for the most basic security matter that users deal in their everyday life. The coverage of most security related terms and definitions that novice users are bombarded through the media is adequate and the examples used to describe the outcome of information security are easy to understand. At the same time they believed that the description of common human errors in respect to information are clear although, similarly as the IT consultants expressed, there may be some room for further improvement by including more guided and step-by-step examples in areas like social engineering and engagement with social networking sites. Also the effort to introduce the concept of examining user knowledge through the use of a quiz was well received although some concerned was expressed on how this would be measured on a continuous basis.

One final approach that was identified by this expert group worth mentioned is the following. Security experts and it managers when they want to implement security awareness initiatives (similar to the toolkit) are facing a lot of challenges. Such a process usually involves a lot of people. Content creators for the developing the actual material, interface designers that would design the user interface following specific user friendliness patterns and finally application developers and database programmers that will built the actual piece that would tie everything together in a single piece. Maybe the most time consuming part is the one that involves the latter. Deciding on which platform will be used in order to build the final piece involves a lot of preparation and is highly dependent of existing expertise (if any) or budgets available in case the platform has to be built through outsourcing. This is the crucial part which makes many companies either postpone such an awareness raising project or use instead ready-made sporadic material without having a structured piece. The toolkit presented is a good example but what happens if someone needs more personalization or customization? The idea expressed here is the development of a toolkit “engine” which would include the existing toolkit components (e.g. pre-testing, main unit(s), post-assessment) without any content but with all the development mechanisms capable to add content. The idea could include building the necessary database backbone for testing, the interface for adding removing questions plus the necessary content creation tools similar to the ones available in modern learning management systems. Of course it is understood that such an approach will involve a lot of time and expertise by many different IT professionals for its initial development but once such a prototype is established it could be easily further enhanced through the open source community.

6.5 Summary

This chapter examined the process of implementing and evaluating the effectiveness of the toolkit. The process of putting a toolkit prototype in action has been presented along with aspects of the development work behind it. In terms of toolkit evaluation of its effectiveness and usability, the following methods have been used and its results have been described:

- Testing of the toolkit using three representative focus groups: a group of college first year students, a group of college students towards graduation and a group of people that hold administrative positions. The three groups were exposed to the different elements of the toolkit and their thoughts are discussed and presented.
- Testing the toolkit effectiveness using a group of individuals from institutions of higher education who are involved in learning process from various positions (e.g. Librarians, technology specialists, teaching and learning department staff, instructional designers, etc.). This testing was done by exposing this group of experts to the toolkit and their opinions were measured and analyzed through a survey.

From both methods it has been concluded that the security toolkit is considered a valuable resource in an effort to establish a sufficient level of security awareness amongst the online population.

From the results of the focus groups conducted to students groups, it appeared that the toolkit helped them improve and complete their security knowledge that is needed in their everyday exposure with information technology. In terms of human aspects of security, the toolkit presented and covered in a sufficient

manner all the necessary concepts and precautions that have to be taken into consideration in respect to aspects associated with the human element in information security. More specifically, it covered aspects, such as common human errors, efficient use of passwords, social engineering concepts and risks associated with the exposure to social networking. Similarly, the exposure of the administrative staff group to the toolkit showed that administrative staff value the importance of IT security both as individuals and as members of a company, and realize the increased need for developing the necessary skills and competencies that will ensure the security of data and systems they operate. Finally, they expressed their feeling that the toolkit can significantly contribute in an effort to raise the awareness level of employees and regulate their security behavior through a continuous learning process.

From the toolkit exposure to a group of experts and the measurement of their opinions through a survey, it appeared that the majority of the participants consider the toolkit as useful for presenting basic everyday information security principles. Such a conclusion can be drawn by either measuring the survey results of the participants as whole or measuring the results by job function. In terms of the general concepts of information security presented in Unit I of the toolkit, the majority clearly understood the consequences of poor information security and why there is a need for information security awareness. In this respect they consider this unit as a good basis for promoting information security awareness. In terms of the concepts presented in the human aspects of security unit, the majority of participants have understood the role of the human error in information security and why it is considered the largest risk. The concepts associated with the use of passwords along with the rules that have to be followed in order to choose strong password and keep it safe have been presented in an

efficient way. Although percentages are considered high, a small degree of concern has been expressed by the participants in respect to social engineering concepts and associated terms. A similar concern has been observed in respect with the rules that have to be followed when visiting social networking sites. Finally, most participants feel that the post-assessment questions of both units can be easily answered if sufficient exposure of the toolkit has taken place.

Chapter VII – Conclusion and Future Work

7.1 Research Achievements

Information security has become an established discipline as more and more businesses realize its value. One of the major challenges of managing an information system is to provide appropriate measures to protect these systems. Many surveys have indicated the importance of protecting valuable information and an important aspect that must be addressed in this regard is information security awareness. Information security awareness is about enabling all participants in the information security function to clearly understand the role they play and are aware of the rules and regulations they are expected to adhere to.

From the conducted literature review, the profound need and importance for addressing information security awareness along with its interdisciplinary nature has been identified. Although security awareness is an essential proactive measure in an effort to protect personal and organizational information systems through effective security practices, still there is a lot to be done in order to achieve an appropriate awareness level for the general population. Both surveys conducted in Chapter 4 indicated that the awareness of the online population is not at a sufficient level. Using two distinct groups of students as a sample, it was determined that although they understand the importance of information security and the dangers associated with the lack of it, they still engage in insecure behaviors due to the absence of appropriate information security awareness raising initiatives.

Towards this goal the thesis proposed the development of the “Information Security Toolkit”. As an awareness raising method, the toolkit was addressed to the general user population with objective to establish the security knowledge

and skills that all IT users need to acquire in order to be competent and confident users of technology.

Towards the development of the toolkit several learning theories were taken into consideration in an effort to create a piece that is user-friendly and at the same time achieved learning retention. In fact, different people learn and retain learning differently. There are people who prefer instructor led training, while others are more favorable to the e-learning approach. Also differences in age or culture may result in significant differences in the preferred learning style. While all people are able to learn through a variety of media different generations many have different preferences in learning (Cekada, 2012; Arshavskiy, 2013). Having in mind this challenge, the toolkit was created as a successful learning experience geared towards all generations by incorporating a variety of activities that utilize all learning styles.

Finally, having developed a working prototype of the toolkit, the thesis proceeded with the implementation and evaluation of its effectiveness. By testing the toolkit using three representative focus groups, a group of experts involved in learning processes and a group of IT Experts, it was concluded that the security toolkit is a valuable resource in an effort to establish a sufficient level of security awareness amongst the online population.

Following the research aims and objectives highlighted in Chapter 1, the achievements against each objective can be summarized as follows:

a. Understand the current information security landscape, and appreciate the importance of the human factor.

The research conducted has realized that the changes in the IT environment have brought additional challenges and implications to information security. Despite the presence and variety of physical and technical controls, technology is designed to run without people but *managed* and *used* by people (Schultz, 2005). People's behavior has to be taken into serious consideration when designing an efficient information security strategy. An appropriate level of awareness in respect to the risks associated with the use of technology can greatly contribute towards this goal.

b. Investigate the changing trends in the domain of Information Security that lead to the importance of security awareness.

The research identified that the technological advances have brought significant changes in the Information Security domain, bringing even greater challenges into the scene. One of these involve the growth and complexity of cyber threats which have made organizations consider not only the integration of technology and processes but also people. This growing appreciation of the importance of the human factor brought the necessity to make users aware of everyday issues concerning information security in an effort to achieve a change in their behavior.

c. From a thorough literature review, understand the issues surrounding effective information security awareness and the establishment of an appropriate security culture.

The review of the relevant literature signified that developing and implementing an effective security awareness program is the first step on providing computer and information security, and is considered a critical

success factor. Also, Security culture is one of the major building blocks of a security awareness program. Significant organizational culture change is a necessity for security implementation as it affects many security practices and behavior.

d. Investigate the potential of raising security awareness within existing education systems as a first step towards a security awareness initiative for the online population.

Both survey results presented in Chapter 4 demonstrate the level of information security awareness and practices. In summary both surveys indicate that students do not arrive at the university with sufficient security knowledge in order to be considered efficient technology users and their engagement in normal university studies does not develop the required degree of further security knowledge. They also signify the need for a more structured approach towards achieving an appropriate level of information security awareness.

e. Propose, define and develop a novel model called the "Information Security Toolkit" in an effort to raise the level of security awareness and help establish a security aware culture.

The results of the surveys conducted signify the need of an additional approach which can help users develop and add to their knowledge in lacking areas over time. The development of the information security toolkit forms the basis for general technology users to understand the challenges associated with secure use of information technology. Also, it further helps them assess their current knowledge, identify lacks and weaknesses and acquire the required knowledge in order to be competent and confident users of technology.

f. Evaluate the toolkit validity by piloting a prototype and assessing its effectiveness.

The toolkit was tested using three representative focus groups which were exposed to its different elements and their thoughts were discussed and presented. Further to that, toolkit effectiveness was tested using a group of experts from institutions of higher education and a group of IT experts, by exposing them to the toolkit and measuring their opinions through a survey. From all testing methods, the toolkit was considered a valuable resource in an effort to establish a sufficient level of security awareness amongst the online population.

7.2 Research Limitations

The research has a number of limitations which are indicated below:

- The surveys conducted in Chapter 4 were addressed to the student population of a private educational institution in Greece offering both undergraduate and graduate degrees. The surveys were conducted using undergraduate level students. Concerning the first survey that was assessing pre-university awareness levels, the survey was conducted over a strict period of time since it was important for this group of students to answer the questionnaire before they were actually exposed to any formal information security education. For that reason, effort was made to keep the questionnaire as short as possible in order to achieve a representative sample of responses. Also, because there was a necessity to compare the results of both surveys, a similar questionnaire was used for the second survey.

- Research derived from both surveys was quantitative where user experiences, perceptions and behaviors were captured by using questionnaires only. Due to time constraints and sample composition (pre-university students are not so friendly towards other forms of collecting data) no other forms of interaction that could further interpret the results (such as focus groups and personal interviews) were used.
- Concerning the toolkit development, because of the time spent to evaluate potential software solutions and the period required to become familiar with the chosen software development platform, a representative prototype of the toolkit involving two modules was developed. In that respect the sounds and graphics used, were developed using the researcher's own means and relevant Internet sources, without involving other more sophisticated means of production and content creation (e.g. professional sound recording and production systems, graphic designers, content editors, etc.).
- In spite of these points, the research is still considered to have made a valid contribution. Indeed, the findings arising from it are relevant in the context of informing awareness-raising practices, and as a foundation for future research. Also the concept of the user profile in the toolkit which objective is to contain personal user information and be amended as the toolkit engagement continues to include user progress history, has not been fully developed in this prototype version of the toolkit.

7.3 Future Research

Research could be further expanded and improved in the future by considering the following suggestions:

- Based on the results of both surveys it is evident that although students spent a significant time online, they enroll in university education without the appropriate information security knowledge. Also this knowledge does not significantly change as they become established university students and reach the level of entering the workforce leaving a big knowledge gap necessary to be covered by businesses and organizations. The research conducted could form the basis for an appropriately developed information security curriculum across different educational levels and different educational disciplines. This could serve as the foundation for a security aware society that not only understands the threats associated with information technology but also behaves in a security aware manner.
- The security toolkit was used as the basis for the general technology user to understand the challenges associated with secure use of information technology and help him become competent and confident with the use of technology. There is significant potential to further enhance it by including additional topics so from a working prototype it evolves to a complete set capable of assessing and establishing an appropriate level of awareness. Additional related disciplines (e.g. interface designers, content creators, etc.) could further assist towards this effort.
- The implementation of an information security awareness programme for an organization is the first step towards controlling the risk associated with the users' lack of knowledge and wrong behavior. However, information security awareness initiatives reach a stage of maturity and efficiency when they are accompanied by appropriate measurement efforts that evaluate the resulting security culture. The security toolkit has been identified as an efficient awareness raising initiative that could help

towards achieving an appropriate level of security culture. There is a large potential for further research that will establish a holistic approach that continuously measures the resulting security culture and amends awareness efforts accordingly.

7.4 Information Security Awareness … a continuum

In many parts of this thesis, it is expressed that information security is a widely accepted discipline since its value is recognized by everyone. Indeed it is the advances of information technology and its proliferation in all aspects of our everyday lives that has brought this broad acceptance of security. So all efforts towards security awareness and should be continuous and updated in order to protect the online population.

As their dependence only seems likely to increase, the online population should be provided with the means that will help them not only appreciate the use of information technology, but also understand the potential dangers associated with its use so they behave in a secure way. Academic institutions can further contribute to this cause by preparing a security aware workforce capable of protecting critical infrastructures. The research conducted has taken into consideration this enhanced need for security awareness and proposed means that can contribute to its improvement.

References

1. A. T. Kearney (2013). "The Mobile Economy 2013." Retrieved Aug. 10, 2014, from http://www.gsmamobileeconomy.com/GSMA%20Mobile%20Economy%202013.pdf.
2. Adams, A. and Sasse, A. M. (1999). "Users are not the Enemy. Why users compromise computer security mechanisms and how to take remedial measures." Communications of the ACM **42**(12): 41-46.
3. Alessi, S. and Trollip, S. (2000). Multimedia for Learning: Methods and Development, Pearson.
4. Aloul, F. (2012). "The Need for Effective Information Security Awareness." Journal of Advances in Information Technology **3**(3): 176-183.
5. Anderson, C. L. and Agarwal, R. (2010). "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions." MIS Quarterly **34**(3): 613-643.
6. Anttila, J., Savola, R., Kajava, J., Lindfors, J. and Röning, J. (2007). Fulfilling the Needs for Information Security Awareness and Learning in Information Society. 6th Annual Security Conference, Las Vegas, NV, Global Publishing, Washington DC, USA.
7. Arshavskiy, M. (2013). Instructional Design for ELearning: Essential guide to creating successful eLearning courses, CreateSpace Independent Publishing Platform.
8. Ashenden, D. (2005). "Looking out into a world of threat." Computer Fraud & Security **2005**(3): 13-15.
9. Bacon, T. and Tikekar, R. (2003). "Experiences with developing a computer security information assurance curriculum." Journal of Computing Sciences in Colleges **18**(4): 254-267.
10. Barbour, R. and Kitzinger, J. (1999). Introduction: the challenge and promise of focus groups. Developing Focus Group Research. R. Barbour and J. Kitzinger. London, Sage**:** 1-20.
11. Behaviorism (2014). Retrieved March 25, 2014, from http://en.wikipedia.org/wiki/Behaviorism.
12. Berg, B. (2001). Qualitative research methods for the social sciences. Needham Heights, MA, Allyn and Bacon.
13. BERR (2008). "2008 Information Security Breaches Survey." Retrieved Jan. 12, 2009, from http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html.
14. Bishop, M. (2000). Academia and Education in Information Security: Four Years Later. Fourth National Colloquium on Information Systems Security Education. Washington, DC.
15. Bishop, M. and Frincke, D. (2005). "A Human Endeavour: Lessons from Shakespeare and Beyond." IEEE Security & Privacy **3**(4): 49-51.
16. Boshoff, R. and Van Niekerk, J. (2011). Defining a "generic" end-user: An Information Security perspective. 6th International Conference on Pervasive Computing and Applications (ICPCA). Port Elizabeth, IEEE**:** 476 - 483.

17. Branson, K. and Rayner, T. (1975). Interservice procedures for instructional systems development. C. f. E. T. F. S. University. Springfield, VA.
18. Brinkmann, S. and Kvale, S. (2014). InterViews: Learning the Craft of Qualitative Research Interviewing, SAGE Publications.
19. Broderick, J. S. (2001). "Information Security Risk Management - When should it be Managed?" Information Security Technical Report **6**(3): 12-18.
20. BSI (2013). "Self-assessment questionnaire, How ready are you for ISO/IEC 27001:2013?" ISO/IEC 27001:2013 Information Security Management System. Retrieved Sep. 22, 2014, from http://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISOIEC27001-Assessment-Checklist-UK-EN.pdf.
21. Bush, L. (n.d.). "Focus Groups." Retrieved Feb. 18, 2014, from http://www.elon.edu/docs/e-web/org/percs/Focus%20group%20module.pdf.
22. Carr, N. G. (2003). "IT Doesn't Matter." Harvard Business Review at Large: 5-12.
23. CDC (2013). "A guide for creating quality electronic learning." Retrieved Nov. 5, 2014, from http://stacks.cdc.gov/view/cdc/13702.
24. Cekada, T. (2012). "Training a multigenerational workforce. Understanding key needs & learning styles." Professional Safety(57): 40-44.
25. Chang, S. and Lin, C.-S. (2007). "Exploring organizational culture for information security management." Industrial Management & Data Systems **107**(3): 438-458.
26. Chun-I Lin (2009). Raising security awareness among higher education recipients. Cheney, Washington, Eastern Washington University. **MSc Thesis**.
27. Cialdini, R. (2001). "Harnessing the science of persuasion." Harvard Business Review **79**: 71-79.
28. Ciampa, M. (2014). Security Awareness: Applying Practical Security in Your World, Cengage Learning.
29. Clark, R. and Mayer, R. (2011). e-Learning and the Science of Instruction: Proven Guidelines for Consumers and Designers of Multimedia Learning, Pfeiffer.
30. Computer Science and Telecommunications Board-National Research Council (2002). Cybersecurity Today or Tomorrow: Pay Now or Pay Later. Washington, DC, National Academy Press.
31. Council of European Professional Informatics Societies (CEPIS) (2014). "Assisting EU citizens with reliable ICT security information." Retrieved Sep. 22, 2014, from http://www.cepis.org/media/Assisting_EU_citizens_with_reliable_ICT_security_information1.pdf.
32. Cox, A., Connolly, S. and Currall, J. (2001). "Raising information security awareness in the academic setting." VINE(123): 11-16.
33. Cranor, L. F. (2008). A framework for reasoning about the human in the loop. Proceedings of the 1st Conference on Usability, Psychology, and Security. San Francisco, California, USENIX Association**:** 1-15.
34. CSCAN (2014). "The Essential Guide to Protecting Yourself Online." Retrieved Oct. 20, 2014, from www.cscan.org/passwordstrength/ProtectingYourselfOnline.pdf.

35. Dahlstrom, E., Walker, J. D. and Dziuban, C. (2013). "ECAR Study of Undergraduate Students and Information Technology." Retrieved November 7, 2013, from https://net.educause.edu/ir/library/pdf/ERS1302/ERS1302.pdf.
36. Danchev, D. (2006). "Reducing "Human factor" mistakes." Retrieved Feb. 4, 2009, from http://www.windowsecurity.com/articles/Reducing_Human_Factor_Mistakes.html.
37. Davidson, M. A. (2005). "Leading by example: The case of IT security in academia." EDUCAUSE Review **40**(1): 14-22.
38. Davis, P. (2008). "Measuring the Effectiveness of Information Security Awareness Training." Retrieved July 12, 2014, 2014, from http://www.saiglobal.com/Compliance/resources/WhitePapers/how-to-measure-information-security-training.htm.
39. Denning, D. (2006). Information Warfare and Security, Addison Wesley.
40. Desman, M. (2003). "The Ten Commandments of Information Security Awareness Training." Security Management Practices **11**(6): 39-44.
41. Dick, W. and Carey, L. (1996). The Systematic Design of Instruction. New York NY, Longman.
42. Ditch the Label (2013). Annual Cyberbullying Survey. Brighton, UK.
43. Dodge, R., Carver, C. and Ferguson, A. (2007). "Phishing for user security awareness." Computers & Security **26**(1): 73-80.
44. EDUCAUSE (2013). "Information Security Awareness Video & Poster Contest." National Cyber Security Awareness Month. Retrieved March 18, 2014, from http://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-initiative/community-engagement/information-security-awareness-.
45. Educause (2014). "About cybersecurity initiative." Retrieved Sep. 30, 2014, from http://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-initiative/about.
46. Egan, M. (2005). "Information Security and the Human Factor." Information Systems Control Journal **3**.
47. Eliot & Associates (2005). "Guidelines for Conducting a Focus Group." Retrieved Feb. 18, 2014, from http://assessment.aas.duke.edu/documents/How_to_Conduct_a_Focus_Group.pdf.
48. ENISA (2007). Information Security Awareness initiatives: Current practice and the measurement of success, ENISA. **July 2007**.
49. ENISA (2010). The new Users' Guide: How to Raise Information Security Awareness, ENISA. **November 2010**.
50. ENISA (2011). ENISA launches information security awareness videos in 23 European languages. I. Santa and U. Bergstrom.
51. ENISA (2013). Brokerage model for Network and Information Security in Education, case studies. D. Catalui.
52. Ernst & Young (2008). Achieving a Balance of Risk and Performance. Tenth Annual Global Information Security Survey. London, Ernst & Young.
53. Ernst & Young (2013). Under cyber attack. EY's Global Information Security Survey 2013. London, Ernst & Young.
54. European Commission (2009). Europe's Digital Competitiveness Report. Main achievements of the i2010 strategy 2005-2009. Luxembourg, Publications Office of the European Union. **Volume 1:** 199.

55. European Travel Commission (2014). "Internet Usage Europe." Retrieved Aug. 1, 2014, from http://etc-digital.org/digital-trends/connectivity/internet-usage/regional-overview/europe/.
56. Everett, C. (2009). "Social networking - a risk to information security?". Retrieved July 1st, 2014, from http://www.infosecurity-magazine.com/view/2503/social-networking-a-risk-to-information-security.
57. Fielder, A., Gardner, W., Nairn, A. and Pitt, J. (2007). Fair game? Assessing commercial activity on children's favourite websites and online environments. National Consumers Council.
58. Finch, J., Furnell, S. and Dowland, P. (2003). Assesing IT Security Culture: System Administrator and End-User Perspectives. Proceedings of ISOneWorld Conference, Las Vegas, USA.
59. Forcht, K., Pierson, J. and Bauman, B. (1988). Developing awareness of computer ethics. Proceedings of the ACM SIGCPR conference on management of information systems personnel.
60. Forest, E. (2014, Jan. 29, 2014). "The ADDIE Model: Instructional Design." Retrieved April 18, 2014, from http://educationaltechnology.net/the-addie-model-instructional-design/.
61. Foster, A. (2004). "Insecure and Unaware." The Chronicle of Higher Education **50**(35).
62. Frost & Sullivan (2013). The 2013 (ISC)2 Global Information Security Workforce Study, Frost & Sullivan.
63. Furnell, S. (2004). "Qualified to help: In search of the skills to ensure security." Computer Fraud & Security **2004**(12): 10-14.
64. Furnell, S. (2005). "Why users cannot use security." Computers & Security **24**(4): 274-279.
65. Furnell, S., Bryant, P. and Phippen, A. (2007). "Assessing the security perceptions of personal Internet users." Computers & Security **26**(5): 410-417.
66. Furnell, S. and Clarke, N. (2005). Organisational Security Culture: Embedding Security Awareness, Education and Training. Proceedings of the 4th World Conference on Information Security Education, WISE 2005, Moscow, Russia.
67. Furnell, S., Gennatou, M. and Dowland, P. (2002). "A prototype tool for information security awareness and training." International Journal of Logisitics Information Management **15**(5): 352-357.
68. Furnell, S. and Phippen, A. (2007). "Raising a generation at risk?". Retrieved March 22, 2009, from http://www.bcs.org/server.php?show=ConWebDoc.10312.
69. Gartner (2014). Gartner Says Worldwide Traditional PC, Tablet, Ultramobile and Mobile Phone Shipments On Pace to Grow 7.6 Percent in 2014. Android to Surpass One Billion Users Across all Devices in 2014. Stamford, Conn.
70. Gathany, N. (2012). The Impact of Accessibility Requirements on E-Learning Instructional Strategies, Capella University. **Doctor of Philosophy**.
71. Gaunt, N. (2000). "Practical approaches to creating a security culture." International Journal of Medical Informatics **60**(2): 151-157.
72. Gill, P., Steward, K., Treasure, E. and Chadwick, B. (2008). "Methods of data collection in qualitative research: interviews and focus groups." British Dental Journal **204**(6): 291-295.

73. Gritzalis, D., Theodoridou, M. and Kalimeri, E. (2005). Towards an interidisciplinary information security education model. 4th World Conference on Information Security Education (WISE4), Moscow.
74. Hansche, S. (2001a). "Designing a Security Awareness Program: Part 1." Information System Security **10**(1): 14-22.
75. Hansche, S. (2001b). "Information System Security Training: Making It Happen, Part 2." Information System Security **10**(3): 51-70.
76. Hasebrink, U., Livingstone, S. and Haddon, L. (2008). EU Kids Online: Comparing children's online opportunities and risks a cross Europe. LSE, London: EU Kids Online.
77. Hentea, M., Dhillon, H. and Dhillon, M. (2006). "Towards Changes in Information Security Education." Journal of Information Technology Education **5**.
78. Hern, A. (2014, Aug. 12, 2014). "'Internet of things' is the most over-hyped technology, say analysts." Retrieved Sep.10, 2014, 2014, from http://www.theguardian.com/technology/2014/aug/12/internet-of-things-most-over-hyped-technology.
79. Herold, R. (2005). Managing and Information Security and Privacy Awareness and Training Program. Boca Raton, FL, Auerbach Publications.
80. Hinde, S. (2004). "Hacking gains momentum." Computer Fraud & Security **2004**(11): 13-15.
81. Hudson, C. (2006). Establishing a Successful Security Awareness Program. Information Security Management Handbook. Harold F. Tipton and Micki Krause. London, UK, AUERBACH Publications. **3:** 295-304.
82. IBIS (2013). "IBIS Capital Ltd: Global e-Learning Investment Review." Retrieved May. 25, 2014, from http://www.smarthighered.com/wp-content/uploads/2013/02/IBIS-Capital-e-Learning-Lessons-for-the-Future.pdf.
83. IBM (2013a). Finding a strategic voice. Insights from the 2012 IBM Chief Information Security Officer Assessment. I. C. f. A. Insights.
84. IBM (2013b). IBM Security Services Cyber Security Intelligence Index Analysis of cyber attack and incident data from IBM's worldwide security operations. IBM Global Technology Services.
85. IBM (2014). IBM Security Services 2014 Cyber Security Intelligence Index Analysis of cyber attack and incident data from IBM's worldwide security operations. IBM Global Technology Services.
86. ICANN (2015). "ICANN Security Awareness Resource Locator." Retrieved Jan 12, 2015, from https://www.icann.org/resources/pages/security-awareness-resource-2014-12-04-en.
87. Identity Theft 911 (2009). "The Big Higher Education Security Dilemma - Universities a Hacker's Dream ". Retrieved Feb 27, 2011, from http://identitytheft911.biz/articles/article.ext?sp=10970.
88. Information Security Forum (2002). Effective Security Awareness-Workshop Report. London UK, Information Security Forum.
89. International Organization for Standardization (ISO) (2005). ISO/IEC 27002, Information technology - Security Techniques - Code of practice for IS security management, second edition.
90. International Organization for Standardization (ISO) (2013). ISO/IEC 27002, Information technology - Security Techniques - Code of practice for information security controls.

91. ISACA (2012). COBIT 5 COBIT 5 for Information Security. Rolling Meadows, IL 60008 USA, ISACA.
92. ISACA (2013). Transforming Cybersecurity using COBIT 5. Rolling Meadows, IL 60008 USA, ISACA.
93. ISACA (2014). "ISACA Glossary of Terms." Retrieved Aug. 1, 2014, from http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf.
94. ITGI (2007). "COBIT Security Baseline: an information security survival kit." IT Governance Institute 2nd edition. from www.itgi.org.
95. ITRC (2014). "Identity Theft Resource Cemter: 2014 Data Breaches." Retrieved July 10, 2014, from http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html.
96. Jarvis, D. (2013). "INFOGRAPHIC: The Future of Information Security." Retrieved Sep. 1, 2014, from http://securityintelligence.com/infographic-the-future-of-information-security/#.VB6tHhZWojY.
97. Jenkins, J., Alexandra Durcikova and Burns, M. (2012). Forget the Fluff: Examining How Media Richness Influences the Impact of Information Security Training on Secure Behavior. 45th Hawaii International Conference on System Sciences, Maui, Hawaii USA
98. Johnson, E. and Goetz, E. (2007). "Embedding Information Security into the Organization." IEEE Security and Privacy **5**(3): 16-24.
99. Karjalainen, M., Siponen, M., Puhakainen, P. and Sarker, S. (2013). "One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions." PACIS 2013 Proceedings. Paper 98.
100. Kaspersky Lab (2013). "Global Corporate IT Security Risks: 2013." Retrieved July 1st, 2014, 2014, from http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf.
101. Katsikas, S. (2000). "Health care management and information systems security: awareness, training or education?" International Journal of Medical Informatics **60**(2): 129-135.
102. Killmeyer, J. (2006). Information security architecture: an integrated approach to security in the organization, Auerbach Publications; 2nd edition.
103. Koskosas, I., Kakoulidis, K. and Siomos, C. (2011). "Information Security: Corporate Culture and Organizational Commitment." International Journal of Humanities and Social Science **1**(3): 192-198.
104. Kraemer, S. and Carayon, P. (2007). "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists." Applied Ergonomics **38**(2): 143-154.
105. Kroll Advisory Solutions. (2012). "HIMSS Analytics Report: Security of Patient Data." Retrieved July 19, 2014, 2012, from http://www.krollcybersecurity.com/Kroll_HIMSS_Webinar_Security_of_Patient_Data_May_2012.pdf.
106. Krueger, R. and Casey, M. A. (2008). Focus Groups: A Practical Guide for Applied Research, SAGE Publications.
107. Kruger, H., Drevin, L. and Steyn, T. (2010). "A vocabulary test to assess information security awareness." Information Management & Computer Security **18**(5): 316-327.

108. Kruger, H. and Kearney, W. (2006). "A prototype for assessing information security awareness." Computers & Security **25**(4): 289-296.
109. Lacey, D. (2009). Managing the human factor in Information Security. West Sussex, UK, John Wiley & Sons Inc.
110. Lacohee, H., Phippen, A. and Furnell, S. (2006). "Risk and restitution: Assessing how users establish online trust." Computers & Security **25**(7): 486-493.
111. Li, Y. and Siponen, M. (2011). A call for research on home users' information security behaviour. Pacific Asia Conference on Information Systems, Brisbane, Australia.
112. Livingstone, S. and Haddon, L. (2009). EU Kids Online: Final report. LSE, London: EU Kids Online.
113. Luo, X. R., Brody, R., Seazzu, A. F. and Burd, S. D. (2011). "Social Engineering: The Neglected Human Factor for Information Security Management." Information Resources Management Journal **24**(3): 1-8.
114. Mahbubani, K. (2012, Sep. 2012). "The Global Village has arrived. Interconnectivity is growing by leaps and bounds." IMF, Finance & Development 49(3). Retrieved Aug. 1, 2014, 2014, from http://www.imf.org/external/pubs/ft/fandd/2012/09/pdf/mahbuban.pdf.
115. Malamed, C. (2014). "Realistic Graphics and Learning: What's most effective?". Retrieved June 1, 2014, 2014, from http://theelearningcoach.com/media/graphics/realistic-graphics-and-learning/.
116. Marczak, M. and Sewell, M. (2005). "Using Focus Groups for Evaluation." Retrieved Feb. 18, 2014, from http://ag.arizona.edu/sfcs/cyfernet/cyfar/focus.htm.
117. Martins, A. and Eloff, J. H. P. (2002). Information Security Culture. Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives, Kluwer, B.V.**:** 203-214.
118. May, C. (2003). "Dynamic Corporate Culture Lies at the Heart of Effective Security Strategy." Computer Fraud & Security **2003**(5): 10-13.
119. McGettrick, A. (2013). Toward Curricular Guidelines for Cybersecurity. Report of a Workshop on Cybersecurity Education and Training Association for Computing Machinery.
120. McIlwraith, A. (2006). Information Security and Employee Behavior: how to reduce risk through employee education, training and awareness. Hampshire, UK, Gower Publishing Limited.
121. Meier, D. (2000). The Accelerated Learning Handbook. New York, McGraw-Hill.
122. Mellor, M. and Noyes, D. (2006). Awareness and Accountability in Information Security Training. 5th Security Conference, Las Vegas, Nevada, The Information Institute, Washington DC, USA.
123. Microsoft Corporation (2014). "Microsoft Security Awareness Toolkit." Retrieved April 22, 2014, from https://www.microsoft.com/en-us/download/details.aspx?id=11428.
124. Morgan, D. and Krueger, R. (1993). When to use focus groups and why. Successful Focus Groups: Advancing the State of the Art. D. Morgan, Sage**:** 3-20.
125. National Initiative for Cybersecurity Careers and Studies. (2013). "Explore Terms: A Glossary of Common Cybersecurity Terminology." Retrieved May 3, 2013, from http://niccs.us-cert.gov/glossary.

126. National Institute of Standards and Technology (NIST) (1998). "Information Technology Security Training Requirements: A Role- and Performance-Based Model, Special Publication 800-16." Retrieved September 3, 2007, from http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.
127. National Institute of Standards and Technology (NIST) (2003). "Building and Information Technology Security Awareness and Training Program, Special Publication 800-50." Retrieved September 13, 2007, from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.
128. National Institute of Standards and Technology (NIST) Technology Administration U.S. Department of Commerce (1995). "An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12." Retrieved September 2, 2007, from http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.
129. NCSA (2014). "Staysafe online.org." Retrieved April 16, 2014, from http://staysafeonline.org.
130. NIST (2014). "Framework for Improving Critical Infrastructure Cybersecurity." Retrieved May 10, 2014, 2014, from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
131. Nonaka, I. and Takeuchi, H. (1995). The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation, Oxford University Press, USA.
132. Northcutt, S. (2007). "The Risk of Default Passwords." Security Laboratory: Methods of Attack Series. Retrieved Oct. 20, 2014, from http://www.sans.edu/research/security-laboratory/article/default-psswd.
133. Norton Corporation (2013). "2013 Norton Report." Retrieved Aug. 13, 2014, from http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.pdf.
134. Ólafsson, K., Livingstone, S. and Haddon, L. (2013). Children's Use of Online Technologies in Europe. A review of the European evidence base. LSE, London: EU Kids Online.
135. Olzak, T. (2006). "Strengthen Security with an Effective Security Awareness Program ". from http://adventuresinsecurity.com/Papers/Build_a_Security_Awareness_Program.pdf.
136. Oxford University Press . (2014). from http://www.oxforddictionaries.com/definition/english/tacit?q=tacit.
137. Peltier, T. (2002). Security Awareness Program. Information Security Policies, Procedures, and Standards-Guidelines for Effective Information Security Management, Auerbach Publications.
138. Pew Research Center (2014). "The Web at 15." Retrieved Aug. 1, 2014, from http://www.pewinternet.org/files/2014/02/PIP_25th-anniversary-of-the-Web_0227141.pdf.
139. Plessis, L. d. and von Solms, R. (2002). Information Security Awareness Baseline Education and Certification. ISSA2002. Muldersdrift.
140. Ponemon Institute (2012a). "2011 Cost of Data Breach Study - United States." Retrieved March 1, 2013, from http://bit.ly/xBF6vr.
141. Ponemon Institute (2012b). "The Human Factor in Data Protection." Retrieved March 18, 2013, from http://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf.

142. Posthumus, S. and Von Solms, R. (2004). "A framework for the governance of information security." Computers & Security **23**(8): 638-646.
143. Prescott, C. (2014). Internet Access – Households and Individuals 2014. Statistical Bulletin. Newport, South Wales, Office for National Statistics.
144. Privacy Rights Clearinghouse (2014). "Chronology of Data Breaches. Security Breaches 2005 - Present." Privacy Rigts Clearinghouse. Retrieved April 10, 2014, 2014, from https://www.privacyrights.org/data-breach.
145. Puhakainen, P. (2006). A design theory for information security awareness. Faculty of Science, Department of Information Processing Science, University of Oulu.
146. Puhakainen, P. and Siponen, M. (2010). "Improving employees' compliance through information systems security training: an action research study." MIS Q. **34**(4): 757-778.
147. PWC (2010). "Revolution or evolution?" Technology Strategy Board-Driving Innovation. Retrieved Jun. 08, 2014, from http://www.pwc.co.uk/audit-assurance/publications/revolution-or-evolution-information-security-2020.jhtml.
148. PwC (2013a). "Key findings from The Global State of Information Security Survey 2014." Defending yesterday. Retrieved Jul. 12, 2014, from http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml.
149. PwC (2013b). "Raising security awareness in your employees." The human factor in information security. Retrieved Jul. 12, 2014, from http://www.pwc.ch/en/dyn_output.html?content.void=51537&collectionpageid=8240&containervoid=46459&comefromcontainer=true.
150. PWC (2014). "2014 Information Security Breaches Survey." Retrieved Jun. 08, 2014, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307296/bis-14-767-information-security-breaches-survey-2014-technical-report-revision1.pdf.
151. Rasmussen, J. (1982). "Human errors. A taxonomy for describing human malfunction in industrial installations." Journal of Occupational Accidents **4**(2-4): 311-333.
152. Reason, J. (1997). Managing the Risks of Organizational Accidents, Ashgate Publishing.
153. Richardson, R. (2008). CSI Computer Crime and Security Survey. CSI/FBI, Computer Security Institute.
154. Richardson, R. (2010). 15th Annual 2010/2011 Computer Crime and Security Survey. CSI, Computer Security Institute.
155. Rivera, J. and Meulen, R. v. d. (2013). Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020. STAMFORD, Conn, Gartner.
156. Ruighaver, A., Maynard, S. and Chang, S. (2007). "Organizational security culture: Extending the end-user perspective." Computers & Security **26**(1): 56-62.
157. SANS (2006). "Mistakes people make that lead to security breaches." Retrieved March 24, 2009, from https://www2.sans.org/resources/mistakes.php?portal=f94a311a055434720eafa6a3830ff5e7.

158. SANS (2014). "Securing the Human." Retrieved April 12, 2014, from http://www.securingthehuman.org.
159. Schein, E. H. (2004). Organizational Culture and Leadership, 3rd Edition. San Francisco, CA, Jossey-Bass.
160. Schlienger, T. and Teufel, T. (2003). Information Security Culture - From Analysis to Change. Proceedings of ISSA 2003, Johannesburg, South Africa.
161. Schneiner, B. (2000). Secrets and lies: digital security in a networked world, John Wiley & Sons Inc.
162. Schultz, E. (2004). "Security training and awareness-fitting a square peg in a round hole." Computers & Security **23**(1): 1-2.
163. Schultz, E. (2005). "The human factor in security." Computers & Security **24**(6): 425-426.
164. Seidman, I. (2012). Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences, Teachers College Press.
165. Siponen, M. (2000). "A conceptual foundation for organizational information security awareness." Information Management & Computer Security **8**(1): 31-41.
166. Siponen, M. (2001). "Five dimensions of Information Security Awareness." ACM SIGCAS Computers and Society **31**(2): 24-29.
167. Siponen, M. and Kajava, J. (1998). Ontology of Organizational IT Security Awareness - From Theoretical Foundations to Practical Framework. Proceedings of the 7th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, Palo Alto, CA, USA.
168. Skinner, B. (1965). Science and human behavior, Free Press.
169. Smith, M. and Sainfort, P. (1989). "A balance theory of job design for stress reduction." International Journal of Industrial Ergonomics **4**(1): 67-79.
170. Spears, J. L. (2006). Defining Information Security. 5th Security Conference, Las Vegas, Nevada, The Information Institute, Washington DC, USA.
171. SplashData (2014). "Worst passwords of 2013 - our annual list updated." Retrieved Oct. 15, 2014, from http://splashdata.blogspot.gr/2014/01/worst-passwords-of-2013-our-annual-list.html.
172. Spurling, P. (1995). "Promoting security awareness and commitment." Information Management & Computer Security **3**(2): 20-26.
173. Stahl, S. (2006). Beyond Information Security Awareness Training: It Is Time To Change the Culture. Information Security Management Handbook. Tipton Harold and K. Micki, CRC Press. **Volume 3:** 285-294.
174. Stanton, J. M., Stam, K. R., Mastrangelo, P. and Jolton, J. (2005). "Analysis of end user security behaviors." Computers & Security **24**(2): 124-133.
175. stopthinkconnect.org (2014a). "Keeping the web a safer place for everyone." Retrieved April 22, 2014, from http://www.stopthinkconnect.org/.
176. stopthinkconnect.org (2014b). "Stop, Think, Connect Resource Guide." Retrieved April 22, 2014, from http://www.stcguide.com/.
177. Streff, K. and Zhou, Z. (2006). "Developing and enhancing a computer and network security curriculum." Journal of Computing Sciences in Colleges **21**(3): 4-18.

178. Symantec Corporation (2014a). "Internet Security Threat Report 2014." Volume 19. Retrieved Aug. 13, 2014, from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.
179. Symantec Corporation (2014b). "Internet Security Threat Report 2014, Appendix A: Threat Activity Trends." Volume 19. Retrieved Aug. 13, 2014, from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_appendices_v19_221284438.en-us.pdf.
180. Talib, S., Furnell, S. and Clarke, N. (2010). An Analysis of Information Security Awareness within Home and Work Environments. International Conference on Availability, Reliability and Security, Krakow, Poland.
181. Thomson, K. L., von Solms, R. and Louw, L. (2006). "Cultivating an organizational information security culture." Computer Fraud & Security **2006**(10): 7-11.
182. Thomson, L. K. and von Solms, R. (2005). "Information security obedience: a definition." Computers & Security **24**(1): 69-75.
183. Thomson, M. E. and von Solms, R. (1998). "Information Security Awareness: educating your users effectively." Information Management & Computer Security **6**(4): 167-173.
184. Trustwave (2014a). "2014 Security Pressures Report." Retrieved Sep, 12, 2014, from http://www2.trustwave.com/rs/trustwave/images/2014%20Trustwave%20Security%20Pressures%20Report.pdf.
185. Trustwave (2014b). "2014 Trustwave Global Security Report." Retrieved June, 28, 2014, from http://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf.
186. Tucker, T. (2002). Security Awareness Index Report: The State of Security Awareness among Organizations Worldwide. Houston, Texas, Pentasafe Security Technologies.
187. U.S. Department of Education (2013). "Digest of Education Statistics, 2012 (NCES 2014-015)." National Center for Education Statistics Chapter 3.
188. UK Department for Business Innovation and Skills (BIS) (2014). Cyber Security Skills: Business perspectives and Government's next steps. H. Government. London, UK, Department for Business, Innovation and Skills.
189. von Solms, B. and von Solms, R. (2004a). "The 10 deadly sins of information security management." Computers & Security **23**(5): 371-376.
190. von Solms, B. and von Solms, R. (2004b). "From policies to culture." Computers & Security **23**(4): 275-279.
191. von Solms, R. (1998). "Information Security Management(1): why information security is so important." Information Management & Computer Security **6**(4): 174-177.
192. Watson, J. and Rayner, R. (1920). "Conditioned Emotional Responses." Journal of Experimental Psychology **3**: 1-14.
193. White House (2003a). "The National Strategy to Secure Cyberspace, Appendix: Actions and Recommendations Summary." Retrieved September 10, 2007, from http://www.whitehouse.gov/pcipb/appendix.pdf.
194. White House (2003b). "The National Strategy to Secure Cyberspace, Priority III: A National Cyberspace Security Awareness and Training

Program." Retrieved September 10, 2007, from http://www.whitehouse.gov/pcipb/priority_3.pdf.
195. Whitman, M. and Mattord, H. (2004). Principles of Information Security. Boston, MA, Thomson - Course Technology.
196. Whittaker, Z. (2010). "Searching for the weak link in university network security." Retrieved Feb. 27, 2011, from http://www.zdnet.com/blog/igeneration/searching-for-the-weak-link-in-university-network-security/3963.
197. Williams, A. and Katz, L. (2001). "The Use of Focus Group Methodology in Education: Some Theoretical and Practical Considerations." International Electronic Journal for Leadership in Learning. Retrieved June, 20, 2014, from http://iejll.journalhosting.ucalgary.ca/iejll/index.php/ijll/article/viewFile/496/158.
198. Wilson Mark and Hash Joan (2003). "Building an Information Technology Security Awareness and Training Program, (NIST), Special Publication 800-50." Retrieved September 11, 2007, from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.
199. Wired Safety (2014). "The world's first Internet safety and help group." Retrieved April 12, 2014, from https://www.wiredsafety.org/.
200. Wood, C. (1995). "Information security awareness raising methods." Computers Fraud & Security Bulletin **June**: 13-15.
201. Yasinsac, A. (2002). "Information Security Curricula in Computer Science Departments: Theory and Practice." Journal of Information Security **1**(2).
202. Yurcik, W. and Doss, D. (2000). Information Security Educational Initiatives to Protect E-Commerce and Critical National Infrastructures. In *The Proceedings of ISECON 2000*, Philadelphia.
203. Zeltser, L. and Skoudis, E. (2013). "Security Awareness Terms. Top Terms in Simple English." Retrieved May 3, 2013, from http://www.securingthehuman.org/resources/security-terms.
204. Zickuhr, K. and Madden, M. (2012). Older adults and internet use Washington, D.C., Pew Research Center's Internet & American Life Project.

Appendices

Appendix I – 1st Security Awareness Survey

The purpose of this survey was to investigate the level of security awareness amongst the online population in an effort to justify the need of raising security awareness within existing education systems. Data from a university environment was used in order to examine the state of information security awareness in the academic sector and investigate the awareness needs of students in order to (1) support them during their time of study, (2) prepare them for the workplace, and (3) protect them in their wider personal use of IT systems.

More specifically, the survey was distributed to 1st year college students (e.g. new entrants) who registered for the introductory course in information systems (a common requirement for all students irrespective of their academic area).

Participant Information Sheet

Research Title

Establishing an Information Security Awareness and Culture

You are being invited to take part in a research study. Before you decide it is important for you to understand why the research is being done and what it will involve. Please take the time to read the following information carefully.

Background and purpose of the study

The range of threats that people may encounter in their day-to-day use of information technology (IT) has been increasing and, as a result, awareness of information security issues is considered important either for home or business users.

The importance of security awareness in academia is evident as the lessons learnt there should be applied in both personal and professional lives.

The purpose of this study is to investigate security awareness needs of students in order to (1) support them during their time of study, (2) prepare them for the workspace, and (3) protect them in their wider personal use of IT systems. The aim is to study also how these needs change as students progress in their academic life, until they reach the stage of entry in the workspace.

Participants

There will be approximately 200 participants in total in this study, all of them currently enrolling at CS1070 – Introduction to Information Systems course at the American College of Greece. It is up to you to decide whether or not to take part. If you do decide to take part you will be asked to sign a consent form. If you decide to take part you are still free to withdraw at any time and without giving a reason.

What will happen to me if I take part?

If you decide to take part you will be asked to answer a few brief questions regarding information security. A few demographic questions will precede the actual information security questions. The survey would take you approximately 10 minutes to complete.

The survey is completely anonymous. No one is grading you on your answers, nor is anyone going to know who filled out the questionnaire. On the analysis of survey results, all participants will be referred to as User1, User2 etc.

The results will be used to identify security awareness needs for students. The survey is part of a research project leading to the degree of Doctor of Philosophy at the University of Plymouth, (School of Computing, Communications and Electronics, Faculty of Technology).

Contact for Further Information

If you want any further information about this study you can contact me via e-mail at peter.korovessis@plymouth.ac.uk. In case you have any concerns about the way in which the study has been conducted, you can contact the Faculty of Technology

Business Manager, who is secretary of the Faculty of Technology Research Ethics Committee. Their current contact details are:

Sarah Tilley
Faculty of Technology Business Manager
University of Plymouth
Drake Circus
Plymouth
PL4 8AA

Phone: 01752 233311
Email: sarah.tilley@plymouth.ac.uk

Thank you for taking the time to read this information sheet.

16 September 2008

SECURITY AWARENESS QUESTIONNAIRE

Dear participant, I am a research student conducting a survey in order to investigate information security awareness and understanding amongst students. I would appreciate if you could spare 10 minutes to answer a few brief questions regarding information security. Please answer the questions honestly and to the best of your ability. No one is grading you on your answers, nor is anyone going to know who filled out the questionnaire.

Section 1: Background Information

1. What is your gender?
   - ☐ Male
   - ☐ Female

2. Please indicate your college year.
   - ☐ Entering Freshman (0 credits)
   - ☐ Freshman
   - ☐ Sophomore
   - ☐ Junior
   - ☐ Senior

3. Are you currently employed?
   - ☐ Yes
   - ☐ No

4. What is your major?
   - ☐ Associate in Arts / Bachelor of Arts
   - ☐ Associate in Business / Bachelor in Business
   - ☐ Associate in Applied Science (Office Technologies and Management)
   - ☐ Undecided
   - ☐ Other _____

5. Please indicate the age group that you belong to:
   - ☐ <20 years old.
   - ☐ 21 – 23 years old.
   - ☐ 24 – 26 years old.
   - ☐ >26 years old.

Section 2: Multiple Choice

1. Where do you use a computer (choose all that apply)?
   - ☐ At home.
   - ☐ At the office.
   - ☐ At school (public access labs, library, etc).
   - ☐ Internet café.
   - ☐ Other _____

2. How do you access the Internet (choose all that apply) ?
   - ☐ Using a dial-up connection.
   - ☐ Using a DSL (broadband) connection.
   - ☐ Using the Company/School Internet.
   - ☐ Using a mobile device (e.g. mobile phone).

3. On average, how much time do you spend on the Internet per day?
   - ☐ < 1 hour.
   - ☐ 1-3 hours.
   - ☐ 3-6 hours.
   - ☐ 6-8 hours
   - ☐ > 8 hours

4. Please identify your uses of the Internet. (Please choose 3 options)
   - ☐ E-mail.
   - ☐ Educational purposes.
   - ☐ Chat rooms.
   - ☐ Games.
   - ☐ Web Browsing (excluding social networking).
   - ☐ Shopping.
   - ☐ Banking/Paying bills.
   - ☐ Instant messaging.
   - ☐ Social Networking (e.g. MySpace, Facebook).

5. Other. _____I am concerned about the safety of my information assets (computer, peripherals, electronic data, etc.) while I am online. *(An Information Asset may be defined as a piece of information, stored in any manner which is recognized as 'valuable' and is not easily replaceable. At the same time, the loss of it may be a threat either on a personal or organizational level).*

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

6. I possess the necessary knowledge in order to protect my information technology assets.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

7. Do you have any of the following in place in order to protect your computer and electronic data? (Please select all that apply).
   - ☐ Antivirus software
   - ☐ Firewall
   - ☐ Anti-spam filter.
   - ☐ Good passwords. (e.g. 8+ characters, using a mixture of letters and numbers, and not based upon personal information or dictionary words).
   - ☐ Regular backups
   - ☐ Regular software updates (e.g. via the Automatic Updates feature in Windows).
   - ☐ Other _____.

8. Assume that you receive an e-mail with a file attached to it. In which case(s) would you open the file attachment?
   - ☐ If the mail originates from a person that I know.
   - ☐ If the mail originates from an authority (i.e. university, government) that I know.
   - ☐ If the e-mail successfully passes the security checks of my computer.
   - ☐ Always.
   - ☐ Never.
   - ☐ Other (please explain)

     _____
     _____

9. To which of the following people would you reveal our password if requested to do so?
   - ☐ A fellow student.
   - ☐ A college professor.
   - ☐ The network administrator.
   - ☐ Anyone.
   - ☐ No one.
   - ☐ Other (please explain)

     _____
     _____

10. Which of the following password would you feel are acceptable and safe to choose as your password?
    - ☐ My college id number.
    - ☐ My name.
    - ☐ Something that I easily remember.
    - ☐ A combination of letters and digits in upper and lower case.
    - ☐ My birthday.
    - ☐ Other (please explain)

      _____
      _____

11. I am confident that I would recognize a security incident if I saw one (e.g. computer intrusion, information theft, data loss, etc.).

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

12. Please indicate your level of familiarity with the following terminology (in this context, familiarity means something you have heard of and understand):

	Not at all Familiar	Least Familiar	Somewhat Familiar	Familiar	Very Familiar
Spyware					
Phishing					
Dumpster Diving					
Shoulder Surfing					
Whooping					
Identity Theft					
Spam					
Trojan					
Virus					
Worm					
Adware					
Social Engineering					
Content Filtering					

13. Information security training is considered very important for me
    - ☐ Strongly disagree.
    - ☐ Agree.
    - ☐ Neutral.
    - ☐ Agree.
    - ☐ Strongly agree.

14. There is nothing wrong with downloading music, videos, or programs for free without permission.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

15. Which of the following sources provide you with information on how to protect your computer assets from potential dangers? (Choose all that apply).
    - ☐ Radio
    - ☐ TV Ads
    - ☐ Friend/colleague/college professor
    - ☐ Newspapers/Magazines
    - ☐ Internet news feeds
    - ☐ Received e-mails
    - ☐ Other _____

16. Please indicate your level of agreement with the following statements:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If my data is encrypted, it is safe from hackers.					
If my computer is behind a firewall, it is safe from hackers.					
Despite its popularity, hacking is very rare.					
I have very little to lose if a hacker invades my computer					
The greatest threat to electronic information comes from hackers					

Section 3: True/False

Directions: Please circle T or F if the answer to the question is True or False. If you are not sure about the answer, please circle N.

1. T F N I have used the Internet to download music or programs using file-sharing programs (e.g. Kazaa, eMule, torrents) or file repositories (e.g. RapidShare).

2. T F N When I have an important document for school, I save it in more than one location.

3. T F N I have bought things online.

4. T F N I use the same password for everything that needs a password.

5. T F N I use instant messaging programs like MSN Messenger, Yahoo, ICQ.

6. T F N I can understand if a website is secure to give information to.

If you answered TRUE to Q6, please provide a short explanation on how you judge a website as being secure:

_____

_____

_____

_____

_____

_____

Thank you very much for your participation

Appendix II – 2nd Security Awareness Survey

The purpose of this research is to investigate security awareness among students in order to (1) support them during their time of study, (2) determine how to best prepare them for the workspace, and (3) protect them in their wider personal use of IT systems. The aim is also to study how these needs change as students' progress in their academic life, until they reach the stage of entry in the workspace.

Survey questions were delivered to higher education students (1st year and final year ones) via the web aiming to determine their level of information security awareness. Prior to completing the survey, participants will be asked to watch a short presentation that will introduce them to the basic information security concepts, describe the threats and risks associated with it and provide a range of methods that may be considered useful as a safeguard in their day-to-day use of information technology.

Student Invitation E-mail

Dear student,

You are cordially invited to participate to a web based survey concerning information security awareness among students. The survey is part of a research study leading to the degree of Doctor of Philosophy (PhD). The purpose of this study is to investigate security awareness needs of students in order to (1) support them during their time of study, (2) prepare them for the workspace, and (3) protect them in their wider personal use of IT systems. The aim is to study also how these needs change as students progress in their academic life, until they reach the stage of entry in the workspace.

There will be approximately 200 participants in total in this study, all of them currently enrolling as first year students (up to 30 credits) and final year students (90 or more credits) at the American College of Greece-DEREE. It is up to you to decide whether or not to take part. If you decide to take part you are still free to withdraw at any time and without giving a reason. The survey is completely anonymous.

In order to better understand some basic concepts that govern information security issues, you are invited to watch a short e-learning unit by **following this link**.

After completing the e-learning unit, a link will be presented in order to continue with the survey questionnaire. Please click on the link or copy/paste it to your browser.

This survey has been approved by the ethics committees of both Deree College and University of Plymouth.

Thank you for your participation.

Participant Information Sheet

Research Title

Establishing of an Information Security Awareness and Culture

You are being invited to take part in a research study. Before you decide it is important for you to understand why the research is being done and what it will involve. Please take the time to read the following information carefully.

Background and purpose of the study

The range of threats that people may encounter in their day-to-day use of information technology (IT) has been increasing and, as a result, awareness of information security issues is considered important either for home or business users.

The importance of security awareness in academia is evident as the lessons learnt there should be applied in both personal and professional lives.

The purpose of this study is to investigate security awareness needs of students in order to (1) support them during their time of study, (2) prepare them for the workspace, and (3) protect them in their wider personal use of IT systems. The aim is to study also how these needs change as students' progress in their academic life, until they reach the stage of entry in the workspace.

Participants

There will be approximately 200 participants in total in this study, all of them currently enrolling as first year students (up to 30 credits) and final year students (90 or more credits) at the American College of Greece-DEREE. It is up to you to decide whether or not to take part. If you decide to take part you are still free to withdraw at any time and without giving a reason.

What will happen to me if I take part?

If you decide to take part you will be asked to answer a few brief questions regarding information security. A few demographic questions will precede the actual information security questions. The survey would take you approximately 10 minutes to complete.

The survey is completely anonymous. No one is grading you on your answers, nor is anyone going to know who filled out the questionnaire. On the analysis of survey results, all participants will be referred to as User1, User2 etc.

The results will be used to identify security awareness needs for students. The survey is part of a research project leading to the degree of Doctor of Philosophy at the University of Plymouth, (School of Computing, Communications and Electronics, Faculty of Technology).

Contact for Further Information

If you want any further information about this study you can contact me via e-mail at peter.korovessis@plymouth.ac.uk. In case you have any concerns about the way in which the study has been conducted, you can contact the Faculty of Technology Business Manager, who is secretary of the Faculty of Technology Research Ethics Committee. Their current contact details are:

Paula Simson
Smeaton 009
Faculty of Science and Technology
Plymouth University
Drake Circus
Plymouth
PL4 8AA
Phone: 01752 584503
Email: paula.simson@plymouth.ac.uk

Thank you for taking the time to read this information sheet.

May 2012

SECURITY AWARENESS QUESTIONNAIRE
Paper-based version

Dear participant, I am a research student conducting a survey in order to investigate information security awareness and understanding amongst students. I would appreciate if you could spare 10 minutes to answer a few brief questions regarding information security. Please answer the questions honestly and to the best of your ability. No one is grading you on your answers, nor is anyone going to know who filled out the questionnaire.

Section 1: Background Information

1. What is your gender?
   - ☐ Male
   - ☐ Female

2. Please indicate your college year.
   - ☐ Entering Freshman (0 credits)
   - ☐ Freshman
   - ☐ Sophomore
   - ☐ Junior
   - ☐ Senior

3. Are you currently employed?
   - ☐ Yes
   - ☐ No

4. What is your major?
   - ☐ Bachelor of Arts
   - ☐ Bachelor in Business
   - ☐ Undecided
   - ☐ Other _____

5. Please indicate the age group that you belong to:
   - ☐ <=20 years old.
   - ☐ 21 – 23 years old.
   - ☐ 24 – 26 years old.
   - ☐ >26 years old.

Section 2:

1. Where do you use a computer (choose all that apply)?
   - ☐ At home.
   - ☐ At the office.
   - ☐ At school (public access labs, library, etc).
   - ☐ Internet café.
   - ☐ On the move via a mobile device.
   - ☐ Other _____

2. How do you access the Internet (choose all that apply) ?
   - ☐ Using a broadband connection (e.g. aDSL, cable).
   - ☐ Using the Company/School Internet.
   - ☐ Using a mobile device (e.g. mobile phone).

3. On average, how much time do you spend on the Internet per day?
   - ☐ < 1 hour.
   - ☐ 1-3 hours.
   - ☐ 4-5 hours.
   - ☐ 6-8 hours
   - ☐ > 8 hours

4. Please rank your main uses of the Internet. (Please choose 3 options)
   - ☐ E-mail.
   - ☐ Educational purposes.
   - ☐ Chat rooms.
   - ☐ Games.
   - ☐ Web Browsing (excluding social networking).
   - ☐ Shopping.
   - ☐ Banking/Paying bills.
   - ☐ Instant messaging.
   - ☐ Social Networking (e.g. MySpace, Facebook).

5. Please rank your main uses of the Internet. (You may choose more than one options)
   - ☐ Loss of access to computer and data.
   - ☐ Loss of work not backed up.
   - ☐ Loss of productivity.
   - ☐ Personal liability and/or responsibility E-mail.

6. I possess the necessary knowledge in order to protect my information technology assets.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

7. Do you have any of the following in place in order to protect your computer and electronic data? (Please select all that apply).
   - ☐ Antivirus software
   - ☐ Firewall
   - ☐ Anti-spam filter.
   - ☐ Good passwords. (e.g. 8+ characters, using a mixture of letters and numbers, and not based upon personal information or dictionary words).
   - ☐ Regular backups
   - ☐ Regular software updates (e.g. via the Automatic Updates feature in Windows).
   - ☐ Other _____.

8. Do you generally open e-mail attachments?
   - ☐ Yes
   - ☐ No

9. Assume that you receive an e-mail with a file attached to it. In which case would you open the file attachment? (Please select all that apply)
   - ☐ If the mail originates from a person that I know.
   - ☐ If the mail originates from an authority (eg. university, government, my bank) that I know.
   - ☐ If the mail successfully passes the security checks of my computer.
   - ☐ Other (Please specify): _____

10. Do you feel comfortable revealing your password if requested to do so?
    - ☐ Yes
    - ☐ No

11. To which of the following people would you reveal our password if requested to do so?
    - ☐ A fellow student.
    - ☐ A college professor.
    - ☐ The network administrator.
    - ☐ Anyone
    - ☐ Other (Please specify):_____

12. Which of the following password would you feel are acceptable and safe to choose as your password? (Please select all that apply)
    - ☐ My college ID number.
    - ☐ My name.
    - ☐ Something that I easily remember.
    - ☐ A combination of letters in upper and lower case, digits and special characters that have a special meaning for me.
    - ☐ My birthday.
    - ☐ None of the above
    - ☐ Other (Please specify): _____

13. Which of the following may be a potential premise for a phishing attempt? (Please select all that apply)
    - ☐ Invitations to see photos of family or friends.
    - ☐ Pleas for disaster relief assistance.
    - ☐ Urgent email threatening loss of access to accounts if username and password are not provided.

14. Please indicate your level of familiarity with the following terminology (in this context, familiarity means something you have heard of and understand):

	Not at all Familiar	Least Familiar	Somewhat Familiar	Familiar	Very Familiar
Spyware					
Phishing					
Dumpster Diving					
Shoulder Surfing					
Whooping					
Identity Theft					
Spam					
Trojan					
Virus					
Worm					
Adware					
Social Engineering					
Spear Phishing					

15. Information security training is considered very important for me
    - ☐ Strongly disagree.
    - ☐ Agree.
    - ☐ Neutral.
    - ☐ Agree.
    - ☐ Strongly agree.

16. Peer-to-peer networks are considered a convenient and safe way to search and download files over the web
    - ☐ Strongly Disagree
    - ☐ Disagree
    - ☐ Neutral
    - ☐ Agree
    - ☐ Strongly Agree

17. Which of the following do you consider a good habit when visiting a social networking site like Facebook, MySpace and Twitter
    - ☐ Disclose very few details about yourself and only with people you trust.
    - ☐ Don’t accept invitations and offers from people you do not know and trust.
    - ☐ Avoid installing programs and plugins that are not verified.
    - ☐ Check privacy settings and read the policy that governs the degree of sharing personal information

18. Which of the following sources provide you with information on how to protect your computer assets from potential dangers? (Choose all that apply).
    - ☐ Radio
    - ☐ TV Ads
    - ☐ Friend/colleague/college professor
    - ☐ Newspapers/Magazines

- ☐ Internet news feeds
- ☐ Received e-mails
- ☐ Web sites
- ☐ Other (Please specify):_____

19. Please indicate your level of agreement with the following statements: Please choose the appropriate response for each item:

    Strongly Disagree
    Disagree
    Neutral
    Agree
    Strongly Agree

Statement	SD	D	N	A	SA
If my data is encrypted, it is safe from hackers.					
If my computer is behind a firewall, it is safe from hackers.					
Despite its popularity, hacking is very rare.					
I have very little to lose if a hacker invades my computer.					
The greatest threat to electronic information comes from hackers.					

Section 3: True/False

Directions: Please choose Yes or No if the answer to the question is True or False. If you are not sure about the answer, please choose No Answer.

1. I have used the Internet to download music or programs using file-sharing programs (e.g. LimeWire, eMule, torrent software) or file repositories (e.g. RapidShare, MegaUpload, FileServe).

Yes	No	No Answer

2. When I have an important document for school, I save it in more than one location.

Yes	No	No Answer

3. I have bought things online.

Yes	No	No Answer

4. I use the same password for everything that needs a password.

Yes	No	No Answer

5. Instant messaging is a secure method for sharing university data.

Yes	No	No Answer

6. I can understand if a website is secure to give information to.

Yes	No	No Answer

7. Since you answered Yes to the previous question, please provide a short explanation on how you judge a website as being secure:

   Please write your answer here:

   _____
   _____
   _____
   _____
   _____
   _____

8. Using the option “remember password” in your web browser or email program is an acceptable method for easily remembering a password.

Yes	No	No Answer

9. There is nothing wrong with downloading commercial music, videos, or programs for free without permission

Yes	No	No Answer

Thank you very much for your participation

Appendix III – Focus Group Questionnaire

The purpose of this short questionnaire distributed to the participants, was to determine their information security experience in order to prepare them for the subject and at the same time welcome and facilitate an atmosphere of mutual exchange of opinions.

The questionnaire was used at three distinct groups:

- A group of college undergraduate students with not more than thirty course credit hours completed (first year students).
- A group of college undergraduate students with ninety course credit hours or more completed (last year students or students towards graduation).
- A group of workers employed at various administrative positions.

#	Question	Answer Choices
1	Do you own a computer at home?	• Yes • No
2	Do you have a personal Internet connection?	• Yes • No
3	How much time do you spend online per day?	• < 1 hour, • 1-3 hours, • 4-5 hours, • 6-8 hours, • >8 hours
4	Please rank your main uses of Internet?	• E-Mail, • Educational purposes, • Chat rooms, • Games, • Web Browsing (excluding social networking), • Shopping, • Banking/Paying bills, • Instant messaging, • Social Networking
5	I possess the necessary knowledge in order to protect my information technology assets.	• Strongly Disagree, • Disagree, • Neutral, • Agree, • Strongly Agree
6	Do you have any of the following in place in order to protect your computer and electronic data?	• Antivirus Software, • Firewall, • Anti-spam filter, • Good Passwords, • Regular Backups, • Regular Software updates
7	To which of the following people would you reveal our password if requested to do so?	• A fellow student, • A college professor, • The network administrator, • Anyone, • No one • Other
8	Which of the following password would you feel are acceptable and safe to choose as your password?	• My college ID number. • My name. • Something that I easily remember. • A combination of letters in upper and lower case, digits and special characters that have a special meaning for me. • My birthday. • None of the above

		• Other
9	Which of the following may be a potential premise for a phishing attempt	• Invitations to see photos of family or friends. • Pleas for disaster relief assistance. • Urgent email threatening loss of access to accounts if username and password are not provided
10	Level of familiarity with the following terminology	• Spyware • Phishing • Dumpster Diving • Shoulder Surfing • Identity Theft • Spam • Trojan • Virus • Worm • Adware • Social Engineering • Spear Phishing
11	Information security training is considered very important for me.	• Strongly Disagree • Disagree • Neutral • Agree • Strongly Agree
12	Which of the following do you consider a good habit when visiting a social networking site like Facebook, and Twitter	• Disclose very few details about yourself and only with people you trust. • Don’t accept invitations and offers from people you do not know and trust. • Avoid installing programs and plugins that are not verified. • Check privacy settings and read the policy that governs the degree of sharing personal information
13	I use the same password for everything that needs a password	• Yes • No
14	Using the option “remember password” in your web browser or email program is an acceptable method for easily remembering a password.	• Yes • No

Appendix IV – Information Security Toolkit Expert Validation

The toolkit effectiveness was tested using a group of individuals from institutions of higher education. The participants were involved in the learning process from various positions such as librarians, technology specialists, teaching and learning staff and instructional designers. This testing was done by exposing this group of experts to the toolkit and their opinions were measured and analyzed through a survey.

The participants had to go through:

- The pre-assessment part whose purpose was to determine the participant's knowledge on specific information security topics (through multiple-choice questions) and determine whether additional training is needed.
- The main e-learning unit that introduced essential everyday information security skills and provided guidance on how users can protect their computers, mobile devices and data from attacks, followed by a post-assessment unit that measured the knowledge assimilated.

Finally, after the completion of the above parts, participants were asked to evaluate the effectiveness and usability of the toolkit as a whole by completing a short survey.

Participant Invitation E-mail

Dear AMICAL colleague,

You are cordially invited to take part in a research study relating to information security awareness for IT users. Before you decide whether or not to do so, it is important for you to understand why the research is being done and what it will involve. Please take the time to read the following information carefully.

Background and purpose of the study

The range of threats that people may encounter in their day-to-day use of information technology (IT) has been increasing and, as a result, awareness of information security issues is considered important either for home or business users. This research proposes the development of an Information Security Toolkit in order to help users to achieve appropriate information security behavior.

The security toolkit as a form of awareness raising method was developed to enable self-paced learning.

Specific Purpose

The purpose of this study is to investigate the effectiveness of the proposed information security toolkit. The toolkit is comprised of the following parts:

(1) the pre-assessment part,

The objective of the pre-assessment unit is to determine the participant's knowledge on specific information security topics and determine whether additional training is needed. Pre-assessment takes place in the form of multiple-choice questions. In this version of the pre-assessment unit, two information security areas are covered: (1) Introduction to information security concepts and (2) Human Aspects of Information Security.

Please visit the pre-assessment unit by using the following link

http://cscan.students.acg.edu/test

(2) the main e-learning unit and (3) the post-assessment part.

The objective of the main e-learning unit, that follows the pre-assessment unit, is to introduce to participants to essential everyday information security skills and at the same time help them to be able to protect their computers, mobile devices

and data from attacks. This stage again addresses the two themes of 'Introduction to information security concepts' and 'Human Aspects of Information Security'.

Please visit the eLearning unit by using the following link

http://cscan.students.acg.edu

It will take you approximately 40 minutes to fully complete it

When finished please follow this link in order to **evaluate the effectiveness and usability of the information security toolkit** as a whole. The evaluation is comprised of a few multiple choice questions and will take at most five minutes to complete.

Information Security Toolkit evaluation
http://forms.acg.edu/limesurvey/index.php/744282/lang-en

Contact for Further Information

I would greatly appreciate if you complete the relevant parts explained above by **June 20, 2014**. If you want any further information about this study you can contact me via e-mail at peter.korovessis@plymouth.ac.uk

Thank you

Peter Korovessis
E-mail: peter.korovessis@plymouth.ac.uk

May 2014

Information Security Toolkit, Effectiveness and Usability Paper-based version

Information Security Toolkit Effectiveness

After completing "Unit 1 – Introduction to Information Security" of the toolkit, I feel that

Question	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. The learning area objectives are clear					
2. I have clearly understood why there is a need for Information Security Awareness					
3. The definition of Information Security is clear to me along with its goals.					
4. The examples used to describe the goals of Information Security are easy to understand.					
5. I have understood the issues in respect to Information Security that affect me.					
6. I have understood what are the consequences of poor Information Security					
7. I have gained a basic understanding of the Information Security terms and definitions.					
8. I understand the different types of attackers along with their characteristics.					
9. I have gained a basic understanding about the areas that need protection.					
10. I consider this unit as a good basis for promoting information security awareness.					
11. The quiz area questions reflect the material presented.					
12. The quiz area questions can be easily answered if the toolkit material is sufficiently covered.					

Please write down any particular comments or suggestions you have in relation to this unit

After completing "Unit 2 – Human Aspects of Security" of the toolkit, I feel that

Question	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. The examples that describe common human errors in respect to information security are clear to me.					
2. I understand the importance of using passwords.					
3. I understand the characteristics of a weak password.					
4. I understand the rules I have to follow when choosing a password.					
5. I have understood the rules behind the use of Biometric passwords.					
6. I have understood how to test the strength and suitability of my chosen password.					
7. I understand how to deal with passwords safely.					
8. I understand what is meant by the term "Social Engineering"					
9. I have gained a basic understanding of social engineering approaches and related terms.					
10. I understand what is a phishing attack, along with its variations.					
11. I understand what is meant by the term 'dumpster diving'.					

12. I understand what is meant by the term ‘shoulder surfing’.					
13. I have gained a basic understanding of the techniques, a social engineer will use to obtain personal information.					
14. I have gained a basic understanding of the risks of visiting social networking sites.					
15. Facebook security recommendations are clear to me.					
16. I understand the rules that I have to follow when visiting social networking sites.					
17. The system has the appropriate topic coverage and depth from a security perspective.					
18. I consider this unit as a good basis for promoting information security awareness.					
19. The quiz area questions reflect the material presented.					
20. The quiz area questions can be easily answered if the toolkit material is sufficiently covered.					

Please write down any particular comments or suggestions you have in relation to this unit

Information Security Toolkit Usability

Please indicate your level of agreement with the following statements.

Question	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. The presentation and vocabulary of the system is clear and easy to understand.					
2. Information is arranged in a natural and logical order.					
3. The system is easily controlled by me and all necessary navigation buttons and/or hyperlinks are present and easily used.					
4. The system does not react in a manner that surprises me and it does not do anything unexpected.					
5. The information on each page is not too much to confuse or distract me.					
6. The appearance of the system (colors, graphics, screen layouts, etc.) is consistent.					
7. Objects that have to be used such as hyperlinks, linked graphics and menus are easy to recognize.					
8. The application is easy to use.					
9. The content keeps me engaged and is relevant to what is to be learned.					
10. I was satisfied with the system.					

Please write down any particular comments or suggestions you have in relation to the usability of the whole toolkit.

Overall Toolkit Satisfaction

Please indicate your level of agreement with the following statements.

Question	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. The material specified in the eLearning unit objectives was covered.					
2. I consider the toolkit useful for presenting basic everyday information security principles.					
3. I would recommend this eLearning unit to other users who want to familiarize themselves with basic everyday security principles.					
4. The pace of the eLearning unit helped me understand the material.					
5. The material is sufficiently presented through examples and illustrations.					
6. Overall, I am satisfied with the eLearning unit.					

Additional Feedback
How would you characterize your job function?

- ☐ Library staff
- ☐ Technology specialist
- ☐ Instructional designer
- ☐ Distant learning specialist
- ☐ Teaching and learning staff
- ☐ Faculty
- ☐ Administrative staff
- ☐ Other: _____

I would like to be contacted for further discussing the effectiveness and usability of this toolkit if this is considered necessary.

- ☐ Yes
- ☐ No

Please type below your email address.

Thank you very much for your participation

Appendix V – Information Security Toolkit IT Expert Validation

The toolkit effectiveness was tested using a group of individuals that are considered experts in the IT field. The participants are closely involved in the IT function from various positions such as IT system administrators, IT managers, IT consultants and security experts. This testing was done by exposing this group of IT experts to the toolkit and their opinions were measured and analyzed through a survey.

The participants had to go through:

- The pre-assessment part whose purpose was to determine the participant's knowledge on specific information security topics (through multiple-choice questions) and determine whether additional training is needed.
- The main e-learning unit that introduced essential everyday information security skills and provided guidance on how users can protect their computers, mobile devices and data from attacks, followed by a post-assessment unit that measured the knowledge assimilated.

Finally, after the completion of the above parts, participants were asked to evaluate the effectiveness and usability of the toolkit as a whole by completing a short survey.

Participant Invitation E-mail

Dear IT Expert,

You are cordially invited to take part in a research study relating to information security awareness for IT users. Before you decide whether or not to do so, it is important for you to understand why the research is being done and what it will involve. Please take the time to read the following information carefully.

Background and purpose of the study

The range of threats that people may encounter in their day-to-day use of information technology (IT) has been increasing and, as a result, awareness of information security issues is considered important either for home or business users. This research proposes the development of an Information Security Toolkit in order to help users to achieve appropriate information security behavior.

The security toolkit as a form of awareness raising method was developed to enable self-paced learning.

Specific Purpose

The purpose of this study is to investigate the effectiveness of the proposed information security toolkit. The toolkit is comprised of the following parts:

(1) the pre-assessment part,

The objective of the pre-assessment unit is to determine the participant's knowledge on specific information security topics and determine whether additional training is needed. Pre-assessment takes place in the form of multiple-choice questions. In this version of the pre-assessment unit, two information security areas are covered: (1) Introduction to information security concepts and (2) Human Aspects of Information Security.

Please visit the pre-assessment unit by using the following link

http://cscan.students.acg.edu/test

(2) the main e-learning unit and (3) the post-assessment part.

The objective of the main e-learning unit, that follows the pre-assessment unit, is to introduce to participants to essential everyday information security skills and at the same time help them to be able to protect their computers, mobile devices

and data from attacks. This stage again addresses the two themes of 'Introduction to information security concepts' and 'Human Aspects of Information Security'.

Please visit the eLearning unit by using the following link

http://cscan.students.acg.edu

It will take you approximately 40 minutes to fully complete it

When finished please follow this link in order to **evaluate the effectiveness and usability of the information security toolkit** as a whole. The evaluation is comprised of a few multiple choice questions and will take at most five minutes to complete.

Information Security Toolkit evaluation
http://forms.acg.edu/limesurvey/index.php/298351/lang-en

Contact for Further Information

I would greatly appreciate if you complete the relevant parts explained above by **June 30, 2015**. If you want any further information about this study you can contact me via e-mail at peter.korovessis@plymouth.ac.uk

Thank you

Peter Korovessis
E-mail: peter.korovessis@plymouth.ac.uk

June 2015

Information Security Toolkit, Effectiveness and Usability
IT Experts Group - Paper-based version

Information Security Toolkit Effectiveness

After completing "Unit 1 – Introduction to Information Security" of the toolkit, I feel that

Question	Strongly Agree	Agree	Neither Agree not Disagree	Disagree	Strongly Disagree
1. The learning area objectives are clear.					
2. The unit clearly describes why there is a need for Information Security Awareness.					
3. The definition of Information Security is clear along with its goals.					
4. The examples used to describe the goals of Information Security are easy to understand.					
5. The issues in respect to Information Security that affect users are clearly understood.					
6. The consequences of poor Information Security are clearly understood					
7. The participant will gain a basic understanding of the Information Security terms and definitions.					
8. The different types of attackers along with their characteristics are clearly understood.					
9. The areas that need protection are clearly understood.					
10. I consider this unit as a good basis for promoting					

information security awareness.					
11. The quiz area questions reflect the material presented.					
12. The quiz area questions can be easily answered if the toolkit material is sufficiently covered.					

Please write down any particular comments or suggestions you have in relation to this module

After completing "Unit 2 – Human Aspects of Security" of the toolkit, I feel that

Question	Strongly Agree	Agree	Neither Agree not Disagree	Disagree	Strongly Disagree
1. The examples that describe common human errors in respect to information security are clear.					
2. The importance of using passwords is clearly understood.					
3. The characteristics of a weak password are clearly understood.					
4. The rules a user has to follow when choosing a password are clear.					
5. The participant will understand how to test the strength and suitability of his chosen password.					
6. The participant will understand how to deal with passwords safely.					
7. The participant will understand what is meant when using the term "Social Engineering"					
8. The participant will gain a basic understanding of social engineering approaches and related terms.					
9. The participant will understand, what is a phishing attack, along with its variations.					
10. The participant will understand what is meant by the term 'dumpster diving'.					

11. The participant will understand what is meant by the term 'shoulder surfing'.					
12. The participant will gain a basic understanding of the techniques, a social engineer will use to obtain personal information.					
13. The participant will gain a basic understanding of the risks of visiting social networking sites.					
14. Facebook security recommendations are clear.					
15. The rules a user has to follow when visiting social networking sites are clear.					
16. The system has the appropriate topic coverage and depth from a security perspective.					
17. I consider this unit as a good basis for promoting information security awareness.					
18. The quiz area questions reflect the material presented.					
19. The quiz area questions can be easily answered if the toolkit material is sufficiently covered.					

Please write down any particular comments or suggestions you have in relation to this module

Information Security Toolkit Usability

Question	Strongly Agree	Agree	Neither Agree not Disagree	Disagree	Strongly Disagree
1. The system uses a language that is natural, easily understood and similar to one that may be used in a day-to-day or study environment.					
2. I am not confused by the use of terms and the way symbols, icons or images are presented.					
3. Information is arranged in a natural and logical order.					
4. The system is easily controlled by me and all necessary navigation buttons and/or hyperlinks are present and easily used.					
5. The system does not react in a manner that surprises me and it does not do anything unexpected.					
6. The information on each page is not too much to confuse or distract me.					
7. Colors, graphics, icons and images are used in a consistent way throughout the system.					
8. There is consistency in screen layouts, use of font types and sizes.					
9. Objects that have to be used such as hyperlinks, linked graphics and menus are easy to recognize.					

10. The application is easy for novice users to use.					
11. The content keeps me engaged and is relevant to what is to be learned.					
12. I was satisfied with the system.					

Please write down any particular comments or suggestions you have in relation to the usability of the whole toolkit.

Thank you very much for your participation

Appendix VI – Publications

Information Security Awareness in Academia

Peter Korovessis, University of Plymouth, UK, and The American College of Greece-DEREE, Greece

ABSTRACT

Information security has become an established discipline as more and more businesses realize its value. Many surveys have indicated the importance of protecting valuable information and an important aspect that must be addressed in this regard is information security awareness. The academic sector is one that regularly addresses information security awareness. Because many successful security intrusions are the result of either social engineering or user complacency, there is a need for students in non IT-related disciplines to become as security literate as possible. The proposed research investigates the level of security awareness amongst the online population. For this reason sample data from a university environment was used in order to examine the state of information security awareness in the academic sector and investigate the awareness needs of students. Since information technology grows at a rapid pace, it is important for the academic sector to identify new trends and developments in information security and adapt the curricula appropriately.

Keywords: *Academia, Behavior, Information Security Awareness, Security Perception, Security Practices, Training*

INTRODUCTION

One of the major challenges of managing an information system and its resources is to provide appropriate measures to protect these systems. Information security has become an established discipline as more and more businesses realize its value. Many surveys have indicated the importance of protecting valuable information and an important aspect that must be addressed in this regard is information security awareness. Information security awareness is about enabling all participants in the information security function to clearly understand the role they play and are aware of the rules and regulations they are expected to adhere to.

Recent research indicates that life has become more interconnected than ever. As reported by the Pew Internet and American Life Project (Kennedy et al., 2008) the traditional American nuclear family now have the highest concentration of interconnected gadgets and devices. A similar situation exists in the UK and Europe (Staksrud et al., 2007) where children are growing up with Web 2.0 and the interactive web while, on the other hand, adults are still struggling to understand and incorporate their use in their lives. At the same time, the volume and nature of information security threats have evolved targeting mainly the weakest link,

DOI: 10.4018/jksr.2011100101

which is the end-user (Schneiner, 2000; Hinde, 2004; ENISA, 2008). It is understood that good security cannot be achieved by technical means alone. Online users, in order to protect themselves, must have a solid understanding of the required security measures (Shuhaili et al., 2010).

There are several sectors where information security awareness has received increased attention, namely government, industry and academia (Bishop, 2000; Yasinsac, 2002). The academic sector is one that regularly addresses information security awareness. This sector consists of academic institutions (colleges, universities, technical schools, schools of secondary education or high schools, etc.), that belong to public or private education, and have as their primary aim to provide learners with all the necessary skills and knowledge for their future occupations. These may include information security as their primary or secondary focus. The role of academic institutions in information protection is vital and has received a lot of attention from researchers worldwide (Williams, 2004). Since the use of information technology is an essential requirement for all university students, the information security curriculum must be designed to support the needs of students undertaking non-IT courses who are interested in learning how to protect their information assets and resources (Hentea et al., 2006). There are a lot of non-computing disciplines that are closely related with the protection of information (Bishop et al., 2005). Because many successful security intrusions are the result of either social engineering or user complacency, there is a need for students in non IT-related disciplines to become as security literate as possible. Therefore, it is important to investigate the potential of raising security awareness within the existing education systems.

As a first step towards this goal, the proposed research investigates the level of security awareness amongst the online population. For this reason sample data from a university environment was used in order to examine the state of information security awareness in the academic sector and investigate the awareness needs of students in order to (1) support them during their time of study, (2) prepare them for the workplace, and (3) protect them in their wider personal use of IT systems. The paper starts with a background section that reviews current activity in the information security awareness domain and public awareness initiatives. Then the survey results are presented and interpreted using the following sub-sections: (1) background information, (2) use of IT and the Internet, (3) security knowledge and perceptions, and (4) security practices and behaviors. The paper completes with a discussion and conclusion section.

Since information technology grows at a rapid pace, it is important for the academic sector to identify new trends and developments in information security and adapt the curricula appropriately. There is a need to integrate security awareness into education. As a first step towards this process, it is important to investigate the level of awareness amongst the online population. This will ensure that learners are kept up to date with new developments and trends in information security.

CURRENT ACTIVITY AT THE INFORMATION SECURITY AWARENESS DOMAIN

The importance of information security awareness and training in order to secure critical organizational or personal information resources has been raised by many organizations.

The European Network and Information Security Agency (ENISA) has published a new users' guide on how to raise information security awareness (ENISA, 2008). The guide recognizes that awareness of the risks and available safeguards are the first line of defense in an effort to secure information systems and networks and provides practical advice on how to raise information security awareness. The same agency has also published a lengthy report based on an investigation of the existing information security awareness programs in the

EU (ENISA, 2006), along with best practices according to target groups used by specific EU countries. The report indicates that there is a requirement for member states to continue to promote and develop a "culture of security".

The UK GetSafeOnline site - a free and independent resource - provides detailed advice for home and business users that will allow them to use the Internet confidently, safely and securely. There are sections that contain information on how to protect your PC and provide the foundation knowledge for online safety, a section that contains advice on how to use the Internet safely and sections providing security advice for small businesses, young people, teachers and parents.

The European Computer Driving Licence Foundation (ECDL) as the leading European authority for computer skills certification recognizes the importance of information security awareness, and for this reason has included relevant preparation modules in their curriculum. The introductory EqualSkills program although it provides vary basic IT knowledge, addresses security issues like the distribution of viruses through the use of e-mail and the security risks involved with opening certain file attachments in e-mail. The e-Citizen certification program moves deeper into the issues of security awareness by helping the candidate appreciate some of the issues and risks associated with using the Internet, such as reliability of information, secure access, viruses, unsolicited e-mail, security of personal data and parental control to access, and be able to take some precautionary measures. Finally the more advanced ECDL/ICDL programs are for anyone who wishes to become fully competent in the use of a computer and common applications. More specifically, Module 1 (concepts of ICT) explain what ICT is and how it fits to everyday life and examines the safety issues in relation to using computers along with legal issues in relation to copyright and data protection. Also, Module 7 (Web Browsing and Communication), helps candidates appreciate some of the security considerations in respect to the usage of online resources

The above represent only a small number of the information security awareness initiatives undertaken across the European Union. It clearly shows not only the common belief that information security is seen as a high priority but also the importance of training as the most effective technique to keep awareness levels high (ENISA, 2007). This paper will move one step further by investigating the security awareness levels at a university environment so curricular enhancements are introduced appropriately in order to identify new trends and developments in information security.

INFORMATION SECURITY AWARENESS IN A UNIVERSITY ENVIRONMENT

Experts in computer security agree that, computer security tends to be weaker at universities (Identity Theft 911, 2009; Whittaker, 2010). Audits of university security systems reveal a large number of weaknesses including a lack of student awareness of computer security and ethics. In order to investigate the security awareness level of students, a survey was conducted to investigate the awareness needs of students in order to (1) support them during their time of study, (2) prepare them for the workplace, and (3) protect them in their wider personal use of IT systems.

METHOD

The survey was conducted using a sample size of one hundred and sixty (160) students who have registered for CS1070 – Introduction to Information Systems course at The American College of Greece. Course sections were selected from both the undergraduate divisions of the American College of Greece that are Deree College and Junior College. The College offers baccalaureate degrees in the liberal arts and in business administration. The main entrance requirements are sufficient level of English plus average or above average academic performance at the high school level. The Ju-

nior College offers two year associate degrees with an option for students to transfer to Deree College after the end of their associate degree studies. Junior College accepts students with a lower level English language or lower high school GPA provided that they attend special preparation courses through a carefully designed advising system. The reason behind choosing this module is that the CS1070 – Introduction to Information Systems course is a general education requirement for all students and is co-taught for both Deree and Junior College students. Most students are required to register for this course during their first semester of studies irrespective of their chosen area of study, in order to get an understanding of IT concept at an early stage. The course is complemented by a lab and has the objective to teach students basic information systems concepts like computer hardware and software, data acquisition, storage and manipulation, data communications, the Internet and the Web, present and future trends in information technology and the social impact of IT.

RESULTS

A concise questionnaire of 28 questions was used consisting of three sections. The purpose of the first part was to collect demographic information from the student participants (e.g., gender, college year, academic discipline, age, and employment status). The second part was the main part of the survey measuring the level of security awareness of students by examining opinions and habits like the use of Internet, level of security knowledge, password usage, methods used for protecting computer and electronic data, use of e-mail, awareness of the various threats to computer assets, etc. Most questions were multiple choice with some allowing the user to choose more than one answer. The last part of the questionnaire included true/false questions where students were asked to indicate their level of agreement with a specific information security issue/statement.

The results are presented and interpreted in the following four sections: Background Information; Use of IT and the Internet; Security Knowledge and Perceptions and Security Practices and Behaviors.

Background Information

Although this was not intentional, the participants of the survey were almost equally distributed between males (46%) and females (54%).

The majority of survey respondents are students who have just entered the college (63%) with the second biggest category being students with at least one semester enrollment (28%). All other categories have non- significant values, and no senior students have actually participated. Therefore the survey results represent the level of security awareness at the start of higher education.

Almost one third of the survey participants are currently employed (31%). It would be interesting to measure at a later stage the awareness level of this group of students and examine whether their employment status has a significant contribution to their awareness level.

Students majoring in Business Administration represented the highest percentage of those that participated in the survey (36%) with the second largest category being students who have not declared their major yet (30%) (Figure 1).

The last question from the background information section indicates that most survey participants (88%) are under 21 years old. This is an expected outcome taking into consideration that most students enter the college immediately after they finish normal high-school.

Use of IT and the Internet

The following section presents the survey findings related with the use of IT and the Internet (Figure 2). Concerning computer usage, the two most dominant answers are at home (96%) and at school (71%). A significant portion of these groups have chosen both at home AND at school (72% of the students that use a computer at home, also use it at school). Significant lower

Figure 1. College academic area

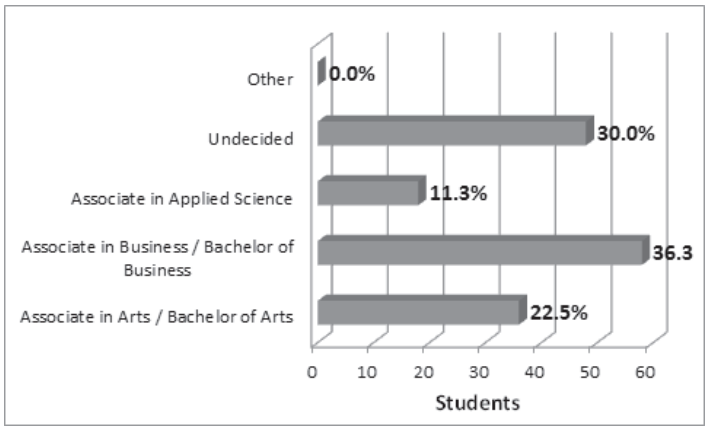
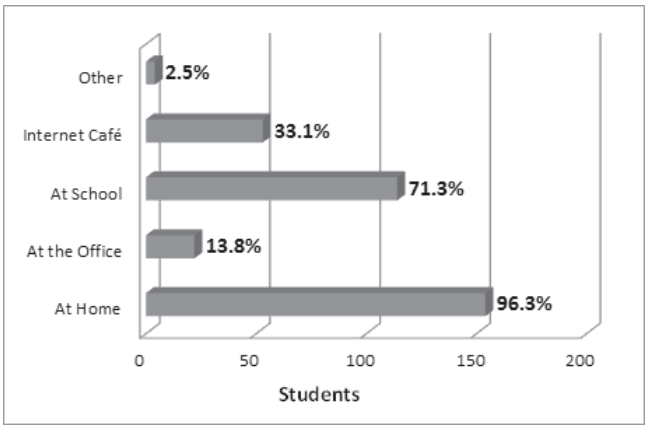


Figure 2. Locations from which respondents use a computer



numbers use a computer either at an Internet Café (33%) or at work (14%).

Most users access the Internet using a DSL broadband connection (84%). A significant portion of the respondents access the Internet using either the school or the company Internet connection (58%). At the same time, the users that access Internet both using a DSL line and a school/office connection are 59%. It is important to mention that a 15% of the respondents access Internet using a mobile device (e.g., mobile phone) and a very small percentage (13%) use a dial-up connection.

Concerning Internet usage (Figure 3), 54% of the respondents spend one to three hours on line per day. A smaller percentage (but still significant) spend four to five hours per day (20%). Internet speed plays an important role on the time that users spend online every day. From the users that spend between one and three hours per day, 89% use a broadband connection. The same applies for the users that spend four to five hours online per day (almost 100% use DSL broadband).

By comparing the survey findings with the European Union (EU) Internet usage, where at least half of the EU population consists of regular internet users (European Commission, 2009), we conclude that the sample is well above the EU average and that the sample population are the most intensive internet users.

To measure respondent's use of the Internet they were asked to choose three answers from a list of common Internet applications. The essence behind this question was to record their three most common Internet uses without any

Figure 3. Time spent online per day

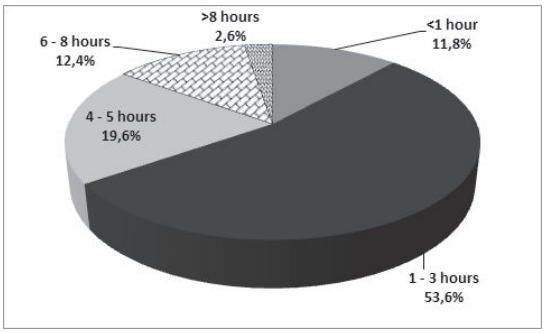


Table 1. Internet usage

Internet Usage	#	ALL	Employed	Unemployed
E-mail	110	69%	59%	73%
Educational Purposes	62	39%	29%	43%
Chat Rooms	31	19%	29%	15%
Games	49	31%	49%	23%
Web Browsing (excluding social networking)	50	31%	37%	29%
Shopping	9	6%	8%	5%
Banking/Paying Bills	3	2%	2%	2%
Instant Messaging	66	41%	27%	48%
Social Networking (e.g., MySpace, Facebook)	77	48%	39%	52%

ranking or prioritization. A significantly low number in a specific usage example does not necessarily mean low usage but rather non-main usage.

It can be seen from Table 1 that the most popular use of Internet among students is e-mail (69%) with social networks (48%), instant messaging (41%) and education (39%) being the other most popular choices. It sound strange that web browsing is ranked fifth (31%) among the most popular choices. At the same time, and since we are referring to students, the number of people that use Internet for educational purposes (39%) may be considered low. This may be explained by the fact that the sample involved mostly incoming college students who are not yet familiar on how to use the Internet for educational purposes. It is likely though that this will change significantly as students' progress with their studies and register in courses that require them to do independent literature reviews and assignments. The figures do not significantly change if we isolate the employed students from the non-employed ones.

It is useful at this point to compare the answer to this question with the answers to relevant true/false questions presented later at the survey.

Although 31% of respondents reported that web browsing is one of their main Internet usages, at a later T/F question, (not surprisingly) almost all (92%) report that they have used the Internet in order to download music and programs from file-sharing programs or file repositories, which often requires web usage. This does not contradict at all with the user's perception on downloading music, videos, or programs without permission presented later on the paper.

It should be also clarified here that the very low percentage of respondents that buy things online (6%), represents that this option is the least favorable internet usage among the options presented at this question. It does not necessarily mean that students do not at all buy things online which is clearly represented at a later question where half of the respondents report that they have been engaged in such activity (50%). The same case appears with the use of instant messaging programs (90%).

From the results presented above (how students use IT and the Internet, where they use their computer, the way they access Internet and for how long and the most common Internet usage applications), there is a clear need for safe and secure Internet usage.

Security Knowledge and Perceptions

The next question is actually the first question that deals with respondent's security knowledge and perception (Figure 4). Approximately 64% of the respondents were concerned about the safety of their information assets (combined percentages of those who answered agree or strongly agree), 28% were neutral while the number of people who are least concerned is almost 9%.

The next question tried to identify whether the respondents possessed the necessary knowledge in order to protect their information technology assets (Figure 5). The question is rather subjective and does not ask the respondent to justify their answer. The question tried to measure their feeling based on a subjective judgement of whether their knowledge of information security issues was enough to protect their technology resources. Approximately 66% of the respondents felt that they possessed the necessary knowledge to protect their information resources (combined percentages of those who answered agree or strongly agree). 8% did not feel comfortable with their information security knowledge.

The next question tried to measure the respondent's confidence in recognizing security incidents (Figure 6). Again this question was rather subjective and did not ask the respondent to justify their answer. 51% of the respondents felt that they would easily recognise a security incident. Another 33% were neutral. The figures do not significantly change if we isolate the employed students from the non-employed ones.

Up to this point the survey considered issues of information security like password selection and use, e-mail usage habits along with the subjective opinion of users about their level of information security literacy. The next question presented the respondents with a list of information security terminology and asks them to indicate their level of familiarity. The list also contained an option that did not exist (whooping) in order to measure whether the respondents were providing considered responses. From Table 2 it is clear that most respondents were very familiar with traditional malware terms, like "virus" (80%), "trojan" (60%), "spyware" (54%), "spam" (54%), and "worm" (44%). However, it seems that other serious information security terms like "phishing", "social engineering" and "shoulder surfing" are not recognised by the survey respondents.

As far as the imaginary term is concerned ("whooping") a small number of respondents (12%) claimed to be familiar (or very familiar) with the term. In order to identify how this group of respondents affects the results of the survey, their answers to main questions were reviewed separately. More specifically the questions that were examined were the ones that deal with methods of protecting their data, perceived knowledge in identifying a security incident, password habits and habits concerning e-mail attachments. It was found that those students do not significantly affect the survey results and their opinion was therefore included in the survey findings.

Information security training is considered a must for the vast majority of users (74%) (Figure 7).

Figure 4. Responses to the statement 'I am concerned about the safety of my information assets'

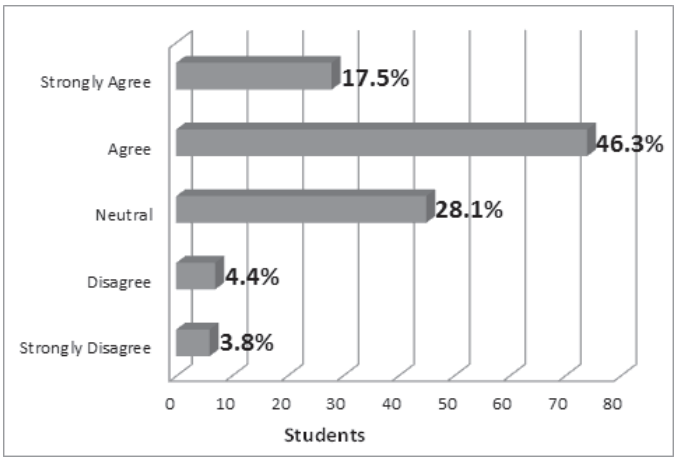


Figure 5. Responses to the statement 'I possess the necessary knowledge in order to protect my information technology assets'

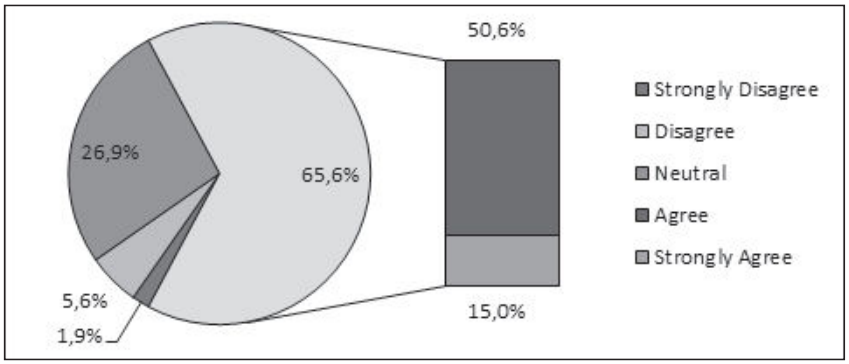


Figure 6. I am confident that I would recognize a security incident if a saw one

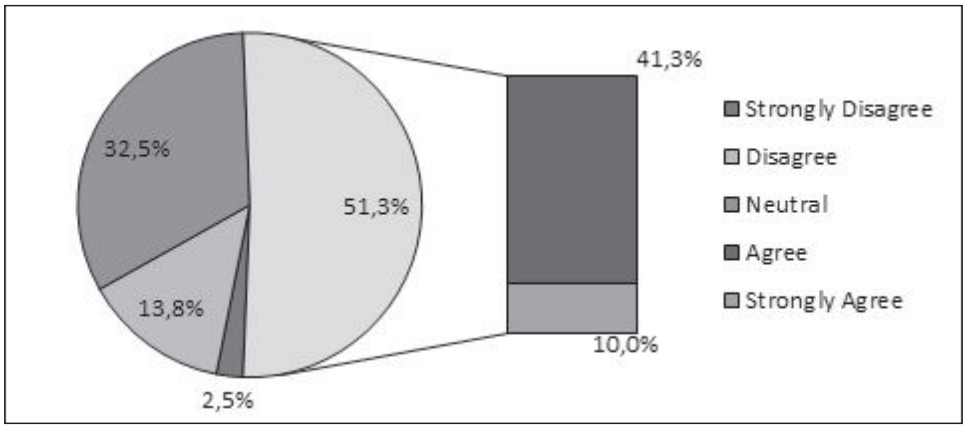


Table 2. Perceived level of familiarity with specific information security terminology

	1	2	3	4	5	
IS Terminology	**Not At All Familiar**	**Least Familiar**	**Somewhat Familiar**	**Familiar**	**Very Familiar**	**Sum of 4 and 5**
Spyware	12,4%	17,6%	15,7%	22,9%	31,4%	54,2%
Phishing	61,4%	23,5%	7,2%	2,6%	5,2%	7,8%
Dumpster Diving	69,9%	19,6%	4,6%	4,6%	1,3%	5,9%
Shoulder Surfing	54,2%	19,6%	13,7%	9,2%	3,3%	12,4%
Whooping	60,1%	19,0%	8,5%	8,5%	3,9%	12,4%
Identity Theft	28,1%	13,7%	20,3%	15,0%	22,9%	37,9%
Spam	14,4%	11,8%	20,3%	16,3%	37,3%	53,6%
Trojan	20,3%	9,8%	9,8%	13,1%	47,1%	60,1%
Virus	5,2%	2,6%	12,4%	18,3%	61,4%	79,7%
Worm	24,8%	14,4%	16,3%	16,3%	28,1%	44,4%
Adware	29,4%	18,3%	17,0%	13,1%	22,2%	35,3%
Social Engineering	34,0%	20,9%	20,3%	20,3%	4,6%	24,8%
Content Filtering	28,8%	13,1%	24,8%	19,0%	14,4%	33,3%

The next question, asked respondents where they obtained their information security knowledge and how they protected their computer assets from potential dangers (Figure 8). Respondents were allowed to choose more than one answer from a list of the most popular sources available for information protection. It is evident from the survey responses that participants are more confident in using informal and more "personal" sources of advice, such as friends, colleagues and college professors (73%). Other sources of information for protection of information assets included Internet news feeds (43%), newspapers and magazines (35%) and received e-mails (31%).

The last question concerning knowledge and perceptions asked the respondents to indicate their level of agreement with specific statements that concern information security threats from hacking/hackers (Table 3).

A high number of respondents believe that data encryption (45%) and the use of a firewall (37%) is not sufficient protection against hackers. Half of the respondents believe that (1) hacking is not rare, (2) a hacker's invasion is of considerable importance (63%) and (3) the greatest threat to electronic information comes from hackers (54%).

Finally using T/F questions, it appeared that the opinion of respondents concerning the importance of backups is equally balanced. Almost half of the students (53%) did not keep important information in more than one place. Also, 33% of the students believe that they will understand if a website is secure to give information but at the same time very few (less than 2%) could provide accurate answers about what constitutes a secure site.

Security Practices and Behaviors

The last section of survey findings deals with user's security practices and behaviors.

By presenting a list of common information security procedures, the next question tried to identify what type of protection was preferred by students in order to protect their computer and electronic data (Figure 9). The participants were able to select more than one answer. It is clear that antivirus software is considered the

Figure 7. Information security training is considered very important for me

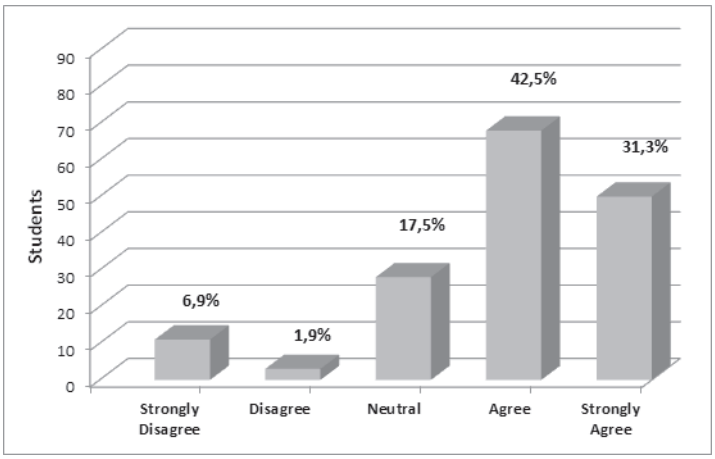


Figure 8. Sources of information for protection of computer assets

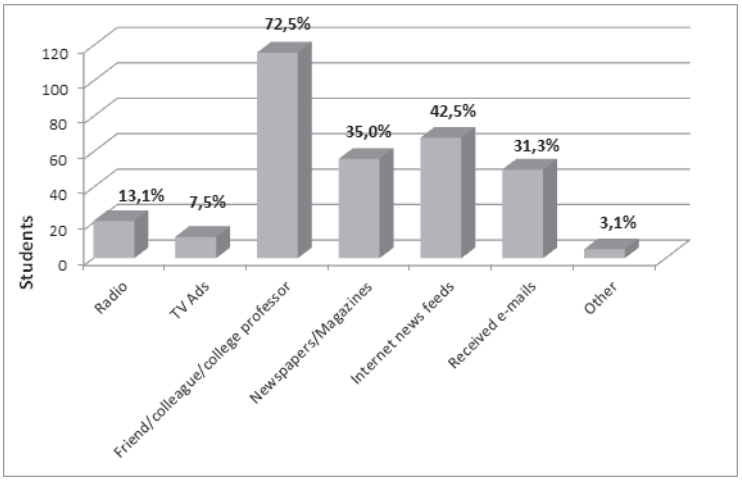
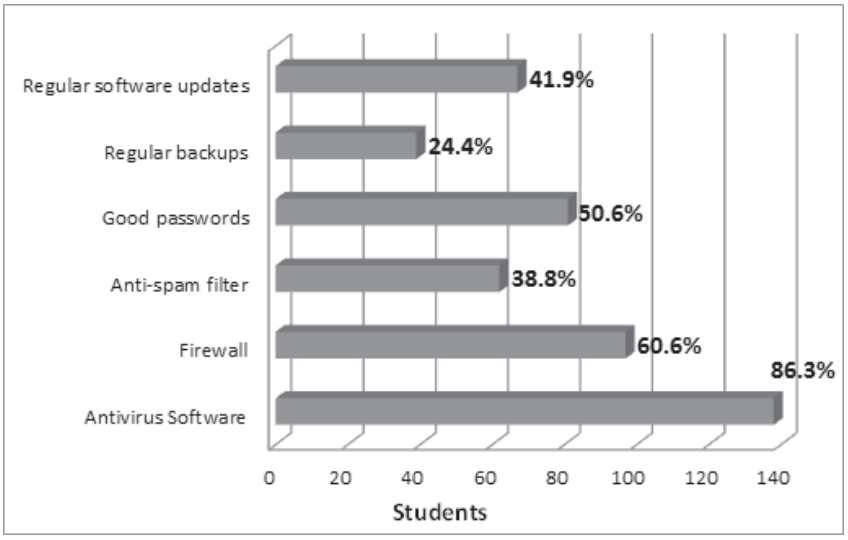


Table 3. Opinions concerning hacking

IS Statement Concerning Hacking	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1-If my data is encrypted, it is safe from hackers	8,5%	36,6%	32,0%	19,0%	3,9%
2-If my computer is behind a firewall, it is safe from hackers	11,8%	25,5%	34,0%	26,8%	2,0%
3-Despite its popularity, hacking is very rare	19,6%	29,4%	17,6%	26,1%	7,2%
4-I have very little to lose if a hacker invades my computer	32,7%	30,1%	15,0%	15,7%	6,5%
5-The greatest threat to electronic information comes from hackers	7,2%	15,0%	24,2%	34,6%	19,0%

Figure 9. Do you have any of the following in place in order to protect your data and electronic data?



most popular protection mechanism used by students (87%). Second and third most popular choices were the use of a firewall (61%) and the use of good passwords (51). At the same time 65% of the students who chose antivirus as their means of protection also chose the use of a firewall as additional protection. Furthermore, 38% of the students who chose antivirus as their means of protection complemented it with the use of firewalls and implementation of good passwords. It seems from the respondent data that regular backups were not considered as a popular method of protection.

Taking into consideration that the use of e-mail has been previously identified as the most popular Internet application, the next question tried to identify their security habits concerning e-mail attachments. Although one-third of the respondents (31%) chose the "correct" answer (if the e-mail successfully passes the security checks of my computer), a significant number of students would always open the e-mail or will open it if it originated from an authority that they know (e.g., university, government), or if it originated from a person they knew (54% in total). This clearly indicates that a large number of students may be subject to attacks. On the other hand it is helpful at this point to compare the security habits concerning email attachments between employed and unemployed students. From Table 4, it seems that students that are currently employed have a significantly higher level of security awareness concerning e-mail attachment behavior that those who are not.

Password usage is strongly associated with information security precautions. It is widely accepted that good passwords represent the first line of defense against internal or external attacks. The next question tried to identify the password awareness needs of students by examining the cases under which they would reveal their passwords (Figure 10). Although 60% of respondents would never reveal their passwords to anyone, a significant number (40%) would reveal their password to various groups of people (e.g., college professors, fellow students, network administrators). If these figures are compared against employed and unemployed students, the figures change significantly showing a higher level of security awareness among those in employment. Only 27% of students in employment feel confident to reveal their password as compared to 41% of those who are not employed. Still this is a significant percentage making those respondents susceptible to social engineering attacks. This is particularly important as it is not just

Table 4. E-mail attachments behavior

Assume that you receive an e-mail with a file attached to it. In which case(s) would you open the file attachment?	#	All	Emp	Unemployed
If it originates from a person that I know	56	35,0%	19,1%	42,3%
If it originates from an authority (i.e., University) that I know	22	13,8%	8,5%	16,2%
If the e-mail successfully passes the security checks of my computer	49	30,6%	38,3%	27,9%
Always	9	5,6%	10,6%	3,6%
Never	19	11,9%	23,4%	7,2%
Other	5	3,1%	4,1%	2,7%

Figure 10. To which of the following people would you reveal your password if requested to do so?

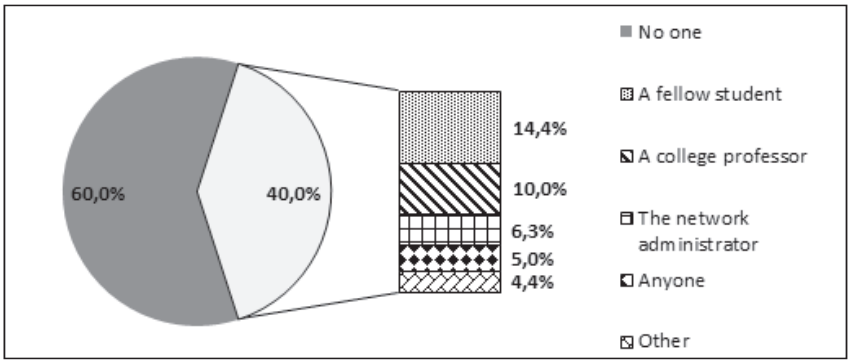
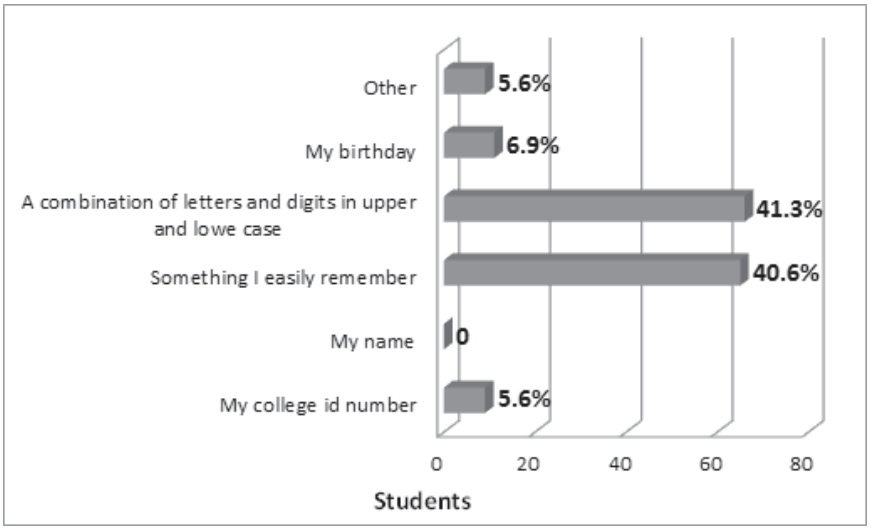


Figure 11. Which of the following password would you feel are acceptable and safe to choose as your own?



the security of their personal assets at risk, but their employer's as well.

The next question continued the examination of password usage as a method of security attack prevention (Figure 11). In this case, the users are presented with a list of choices and they are asked to choose which of these were acceptable and safe to choose as their password. 41% of the respondents would choose a combination of letters and digits in upper and lower case which represents a fairly safe choice. At the same time a similar number would choose something that was easily remembered. Although such a choice cannot be fully considered as a security flaw, it is questionable whether something easily remembered is considered a strong password. If these figures are compared against employed and unemployed students, it is rather unusual to report that 49% of non-employed students would choose a safe and strong password (combination of letters and digits in upper and lower case) compared with only 27% of those in employment.

When asked about password usage, 38% used the same password for everything that needed a password, with 56% reporting that they did not re-use passwords.

DISCUSSION

The participants in this survey represented a group of young individuals registered for an introductory course in information systems during their first year of their degree. The population sample was varied from many study disciplines, and the results exemplify the rule stated by recent publications that Information Security is not strictly a technical issue but rather an issue of concern among many disciplines. (Wood, 2004; Hentea et al., 2006). Information security curricula should include both technical and non-technical issues. Information security is widely recognized as technical as well as non-technical (Solms von Basie et al., 2004). However, along with the feeling that information security is strictly a science or engineering discipline, there are many instances where technical information security issues overshadow the non-technical ones. Many non-technical security issues (e.g., security policy and procedures, ethical and legal issues) are identified as missing from the information security curricula (Bacon et al., 2003).

Although from the survey findings appears that participants have a good level and understanding of information security issues, the problem of achieving security awareness among the online population still remains; especially when discussion is about secure use of e-mail, password, and internet usage habits. The recent years broadband adoption (also reflected within the respondent group) along with its always-on nature combined with the significantly increased speed of service means that users are significantly more exposed than their dial-up counterparts (Furnell et al., 2007). At the same time, the large number of respondents that use a computer at school (second higher after home), indicate the role that academia has to play in information protection. A good and solid understanding of information security issues acquired at school will provide the foundation of an acceptable security awareness level at home and at the work environment.

The majority of respondents engage in a range of applications for which security ought to be a consideration (Table 1). Despite the fact that many respondents perceive that they are aware of potential threats and risks, and believe they pose the necessary security knowledge, their practice does not always evidence this. Often there is a considerable gap between what user know about information security terms, concepts, measures and practices and what they actually do in reality (Kruger et al., 2006; Dodge et al., 2007). Although they argue that they possess the necessary knowledge to protect their information assets, they are willing to open an e-mail attachment if it originates from a trusted source (e.g., Friend or university authority), or feel comfortable to reveal their password if they are asked to do so. At the same time they are ready to engage themselves in non-secure practices like downloading music and programs using file sharing programs or file repositories.

One factor that may influence a user's security behavior is whether security was emphasized or somehow "presented" and communicated when they bought a system and start using it to get online. Surveys indicate that the wide majority of users do not receive any security-related information or advice when they purchase a computer or an Internet connection (Furnell et al., 2007). The survey attempted to assess where advice might be sought after the original purchase and during the use of the equipment. It seems that informal and more "personal" sources of advice, such as friends, colleagues and college professors are the most popular than other categories. This finding is also supported by the Trustguide project (Lacohee et al., 2006) which indicates that individuals build trust with a service through the experimental use of it. Thereafter, in cases where protection of computer assets from potential dangers comes into question, it is clear that information communicated by a peer or a college professor was more valued than other more formal sources. At the same time, the awareness efforts of official and mass media sources to educate the online population seem to lack in engagement and impact.

Finally, from the survey responses it appears that there is a need for information security training in order to achieve an acceptable level of awareness and user practice. As illustrated in Table 2, among others, a large number of respondents lack knowledge for important InfoSec terms like "phising", "social engineering", and "trojans". Although the lack of knowledge for basic security terminology like "shoulder surfing" and dumpster diving" is not considered a weakness, their perceived knowledge of information security principles seems a little bit mixed and imbalanced. They mostly feel that they possess the necessary knowledge in order to protect their information assets (66%) but they are ready to reveal their password to friends and relatives or open e-mail attachments. They claim to be able to understand if a website is secure but they cannot describe what constitutes a secure site although they are very confident with online shopping. At the same time a considerable 49% are NOT confident with recognizing a security incident. Fortunately, the wide majority of respondents is concerned about the safety of their information assets (64%) and is very friendly towards the importance of information security training (74%). This would make it easier to integrate information security concepts in the curriculum in a more structured and systematic way.

SUMMARY AND CONCLUSION

It is widely understood that academia plays an important role in information protection. Not only does it introduce students to information security concepts and how to protect vital data and information resources, but it also equips them with the necessary security skills in order to succeed in their future careers and their wider personal use of IT systems. The aim of this paper was to investigate the need for more general security awareness amongst the online population. For this sample data was used from a University environment in order to investigate the level of security awareness of students currently registered on an introductory course in information systems. The aim was to examine opinions and habits covering students' use of the Internet, their level of security knowledge, password habits, methods used for protecting computer and electronic data, use of e-mail, etc.

As this course is a general education requirement for all students (art, science and business students), the students in each class have a broad range of ability, interest, and technology skill. At the same time, as VanderClock and Gorgone (2004) mention in a similar survey, some students may express hostile attitudes towards technology or many of them may have the opinion that they know enough either from high school or personal experience and cannot conceive the need to know more. At the same time they use the Internet for downloading and communicating with fellow students and at many instances are subject to security risks like viruses, and worms as a result of their limited knowledge for information protection.

The survey showed that the majority of students use a broadband Internet connection and as a result they spend more time online. E-mail, social networking and instant messaging are considered the most popular Internet applications among students, but they are not yet accustomed to using the Internet for educational purposes. The use of proper passwords is considered one of the most effective ways to secure unauthorized access to computer resources with 51% of the students feeling that the use of good passwords (among other measures) is essential. Other more popular choices include the use of antivirus software and firewalls. Despite this, 40% of the survey participants were prepared to reveal their password to fellow students, college professors or network administrators.

The use of e-mail is widely accepted among students. Almost 70% of them stated it as their primary Internet application. At the same time, 54% of them are confident with opening an attachment if the e-mail originates from an authority (e.g., university, government, etc) or a person they know.

Among the methods used for protection of electronic data, although the use of antivirus software, firewalls and choice of good passwords are among the most popular choices, it seems that many students are unaware of the importance of keeping backups of critical data and information or performing regular software updates.

It seems that there is a serious problem concerning what the students perceive as acceptable use of information systems. The vast majority of users (92%) have used the Internet to download music or programs, while 56% of them feel that there is nothing wrong with such a practice.

Information security course content should be structured in such a way that the needs identified by both industry and government sectors are met. Learners that have successfully completed a course containing information security content should have the ability not only to adapt easily to the requirements of their new position but also to train co-workers in basic information security concepts. Further to that, information security curricula should link theory with practice so learners will be able to apply information security principles to real-world scenarios (Bishop, 2000; Bishop et al., 2005).

As mentioned before, information security is relevant not only to computer science and information systems disciplines but also to a variety of other study fields. Because of its multidisciplinary nature information security should be integrated with a variety of other study fields (e.g., the legal environment). At the same time, extra care should be taken with the design of awareness raising content when it is built into different study fields so the needs of every particular field are properly suited (Gritzalis et al., 2005).

One of the challenges of today's rapidly changing technological environment is for academia to prepare professionals that can protect critical infrastructure and investments in people, equipment and information assets (Yurcik et al., 2000). Academia is the starting point in producing professionals who are information security literate, so focus has to be placed upon what can be achieved there. From the survey conducted, it seems clear that although a large proportion of respondents claimed knowledge of security measures, did not demonstrate effective security practices. Taking into consideration people's increasing adoption of technology, security awareness, education, and training are one of the most effective solutions to prevent attacks or enforce acceptable use of information systems. More specifically awareness and training on security along with awareness of ethical issues will help students to be prepared to secure information assets for their future careers or social encounters with information technologies.

As academic institutions are the key areas to educate not only future information security professionals but also security aware citizens, further research should be conducted in order to establish a common body of knowledge (CBK) to serve as a tool that groups the necessary skills and essential knowledge of this field.

In addition, further research can investigate how information security awareness, training

and education can have a positive impact on people's attitudes and behavior. The role of cultural change as a means of establishing acceptable behavior should be further researched. This will be used to feed into the development of a novel model that will help an organization move forward from a security awareness raising initiative to a security culture establishment.

REFERENCES

Bishop, M. (2000). Academia and education in information security: Four years later. In *Proceedings of the Fourth National Colloquium on Information Systems Security Education*.

Bishop, M. (2000). Education in information security. *IEEE Concurrency*, *8*(4), 4–8. doi:10.1109/4434.895087

Bishop, M., & Frincke, D. (2005). A human endeavour: Lessons from Shakespeare and beyond. *IEEE Security & Privacy*, *3*(4), 49–51. doi:10.1109/MSP.2005.87

Dodge, C. R. Jr, Carver, C., & Ferguson, A. (2007). Phishing for user security awareness. *Computers & Security*, *26*(1), 73–80. doi:10.1016/j.cose.2006.10.009

ENISA. (2006). *A users' guide: How to raise information security awareness*. Crete, Greece: Author.

ENISA. (2007). *Information security awareness: Local government and Internet service providers*. Crete, Greece: Author.

ENISA. (2008). *A new users' guide: How to raise information security awareness*. Crete, Greece: Author.

European Commission. (2009). *Europe's digital competitiveness report: Main achievements of the i2010 strategy 2005-2009*. Brussels, Belgium: European Commission.

Furnell, S., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, *26*(5), 410–417. doi:10.1016/j.cose.2007.03.001

Gritzalis, D., Theodoridou, M., & Kalimeri, E. (2005). Towards an interidisciplinary information security education model. In *Proceedings of the 4th World Conference on Information Security Education*, Moscow, Russia.

Hentea, M., Dhillon, H., & Dhillon, M. (2006). Towards changes in information security education. *Journal of Information Technology Education*, 5.

Hinde, S. (2004). Hacking gains momentum. *Computer Fraud & Security*, (11): 13–15. doi:10.1016/S1361-3723(04)00136-8

Identity Theft 911. (2009). *The big higher education security dilemma - Universities a hacker's dream.* Retrieved from http://www.idtheft-encompassinsurance.com/articles/article.ext?sp=10970

Kennedy, T., Smith, S., Wells, L., & Wellman, B. (2008). *Networked families*. Washington, DC: Pew Internet & American Life Project.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296. doi:10.1016/j.cose.2006.02.008

Lacohee, H., Phippen, A. D., & Furnell, S. M. (2006). Risk and restitution: Assessing how users establish online trust. *Computers & Security*, *25*(7), 486–493. doi:10.1016/j.cose.2006.09.001

Schneiner, E. (2000). *Secrets and lies: Digital security in a networked world*. New York, NY: John Wiley & Sons.

Shuhaili, T., Furnell, S., & Clarke, N. (2010). An analysis of information security awareness within home and work environments. In *Proceedings of the International Conference on Availability, Reliability and Security*, Krakow, Poland.

Staksrud, E., Livingstone, S., & Haddon, L. (2007). *What do we know about children's use of online technologies? A report on data availability and research gaps in Europe*. London, UK: EU Kids Online Network.

Whittaker, Z. (2010). *Searching for the weak link in university network security.* Retrieved from http://www.zdnet.com/blog/igeneration/searching-for-the-weak-link-in-university-network-security/3963

Williams, J. (2004). IT education: More specialized in 2010. *IT Professional*, *6*(6), 18–20. doi:10.1109/MITP.2004.86

Wood, C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. *Computer Fraud & Security*, (1): 16–17. doi:10.1016/S1361-3723(04)00019-3

Yasinsac, A. (2002). Information security curricula in computer science departments: Theory and practice. *Journal of Information Security*, *1*(2).

Yurcik, W., & Doss, D. (2000). Information security educational initiatives to protect e-commerce and critical national infrastructures. In *Proceedings of the Conference on Information Systems Education*, Philadelphia, PA.

Peter Korovessis is a PhD student at the University of Plymouth, Centre for Security, Communications and Network Research. He is also the Executive Director for Information Resources Management at The American College of Greece – DEREE. His current research is mainly concerned with Information Security awareness and the establishment of an Information Security Culture.