Security Behaviour of System Professionals on their Home Computer.

Jiby Jacob

A dissertation submitted to the University of Dublin
in partial fulfillment of the requirements for the degree of
MSc in Management of Information Systems

15th August, 2013

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university. I further declare that this research has been carried out in full compliance with the ethical research requirements of the School of Computer Science and Statistics.

Signed: ___________________

Jiby Jacob
15th August, 2013

Permission to lend and/or copy

I agree that the School of Computer Science and Statistics, Trinity College may lend or copy this dissertation upon request.

Signed: ___________________

Jiby Jacob
15th August, 2013

Acknowledgement

I would like to thank my supervisor Susan Leavy for her advice, availability and encouragement throughout this work. Susan was very approachable and her suggestions were thought provoking.

Many thanks to members of the Advanced Support Team for their participation in this research. Special thanks to my employer for giving me this opportunity.

Thanks to all the staff, lectures and colleagues at Trinity College Dublin for their advice, knowledge sharing and team work.

Finally I would like to thank my wife Johncymol, daughter Anna and new born son Leo for their understanding and encouragement. Without their support this would not have been possible.

Abstract

Home computers play crucial role in the security of cyberspace. It is considered as the weakest link in internet security. It is believed that lack of security awareness is the main reason behind unsafe security practices. This research is aimed at finding out the security behavior of system professionals who are aware of computer security and security best practices.

This single case study research used convenience sampling of system professionals working in a multinational company in Ireland to answer the research question “How do system professionals manage their home computer security?” The data collected using the qualitative and quantitative methods was analysed and found that awareness doesn’t change the security practices. The participants exhibited similar security behaviors like a novice home user. However, when it comes to high severity security practices, security professionals showed increased security behavior compared to the low severity security practices.

This research showed that manufacture-enforced security settings play an important role in ensuring home computer security. However, it is observed that knowledgeable users tend to disable these settings for their convenience. So this research recommends more studies on the effectiveness of self-auditing security implementations for home computers.

Table of Contents

List of Tables and Diagrams

Abbreviations

AST	Advanced Support Team
EEC	Enterprise Expert Centre
HBM	Health Belief Model
PMT	Protection Motivation Theory
TTAT	Technology Threat Avoidance Theory
ISA	Information System Awareness
PC	Personal Computer
TPB	Theory of Planned Behaviour
US-CERT	United States Computer Emergency Response Team

1 Introduction

1.1 Background of the Study

We live in an era where unprotected home computers and networks pose a serious threat to global security. To minimize the security threat, governmental agencies and organisations around the globe have developed various programs to promote security awareness for home users. Technology companies have developed mandatory information security training for their employees to make them aware of threats and the importance of best practices. These organisations have enforced IT security to keep their environment safe and secure. However we don’t know how these employees who are aware of security best practices manage their home computer security. Also there isn’t any study conducted on how information system professionals who are aware of computer security manage their home computer security where security is not enforced.

This research is a case study research to study the security practises of information system professionals in their home computer environments. Buchanan *et al* (2007) point out that the people who are knowledgeable about computer security issues are more efficient in implementing and managing security. This study is aimed at finding out how system professionals who are aware of security threats manage their home computer environment where security is not enforced. Analysis will be based on the findings obtained from the primary and secondary data collection.

Information technology is an integral part of our life. According to International Telecommunication Union (2011) 2.3 billion internet users accessed the internet in 2011. This is an astronomical number considering the lack of internet penetration in emerging countries. This poses a real threat as there are lots of organized cybercriminals out there who are trying to steal data and money from these users. Huigang and Yajiong (2009) consider information technology as a double-edged sword which can be used for good or evil. As cited by Tsohou *et al* (2008) one of the biggest threats to information security is lack of awareness.

1.2 The Rationale of the Study

In spite of awareness initiatives like National Cyber Security Awareness Month (NCSAM), cybercrimes are increasing rapidly. According to International Organisation for Standardisation (2005) "All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function."

Organisations invest heavily to make users aware of the importance of security practices and also enforce security to keep their environment safe and secure. There isn't any study on how information systems users who are aware of computer security manage their home computer environments where security is not enforced.

1.3 Research Questions

The main research question for this dissertation is:

How do information systems professionals who are aware of information security best practices manage their home computer security?

The objectives of this research are to find out:

1) How do the security behaviours of system professionals differ from novice home users?

2) How does the attitude towards security influence the security practices of system professionals in home computing?

3) How do system professionals respond to manufacture enforced security settings in home computers?

1.4 Importance of this Study.

Due to the proliferation of the technology more and more users connect to the internet. The number of reported cybercrimes has doubled in the recent past. Information systems experts believe that awareness can safeguard people from cyber security threats to a large extent. However, there is no study conducted on the security behaviours of people who are aware of security, especially the system professionals who work with customers to resolve their security issues.

This research will help us to evaluate the security practices of information systems professionals who are aware of the importance of computer security.

1.5 The Scope and Boundaries

This single case study research is applicable to the entire system professional’s community. Since it is practically impossible to sample all professionals, a convenience sampling is selected. The convenience sample selected for this study is the Advanced Support Team (AST) in a multinational company in Ireland. This company has $50 billion revenue and is based in South Dublin. AST, which is a part of the Enterprise Expert Centre (EEC), consists of 46 highly experienced system professionals who work as the last level of support for customers for their complex information technology issues. This team was formed in 2002 with seven support professionals and due to the continuous growth of the business the team expanded and has currently 46 members. The AST has professionals from 11 different nationalities. This team is highly experienced and certified. Employees working in other sectors of the business are not considered for this study as it is important that the participants of this study are very advanced computer users

This case study research is aimed at focusing on how advanced system users who are aware of home computer security practices manage their home computer environments. The primary source of the data for this research is an online survey that is conducted among at AST. Semi-structured interviews will be conducted to validate the results of the online survey. This will be used as secondary source of data. Extensive literature reviews are conducted to give a theoretical acceptance of the subject and this will be used as secondary data.

1.6 The Road-Map of Subsequent Chapters

Chapter1: Introduction: This chapter gives an overview of the research question and the background information regarding this research. This chapter also defines the scope and boundary of this research.

Chapter 2: Literature Review: This chapter gives the theoretical background of the research study. The aim of this chapter is to give a critical review of the relevant literature.

Chapter 3: Research Methodology and Field Work: This chapter explains what methodology was used to answer the research question. This explains why a particular research model was used in this research. Also the development of questionnaire and conduct of the data collection are detailed in this chapter.

Chapter 4: Findings and Analysis: This chapter details how the data was analysed and interpreted. Data from different sources are analysed and overall details are given in this section.

Chapter 5: Conclusions and Future Work: The purpose of this chapter is to discuss the conclusions of the findings of this case study research to answer the research question. This chapter also contains important observations and future research sections.

2 Literature Review

2.1 Introduction

Home computers play a crucial role in cyberspace security. As more and more home users adapt to doing business online, home computer security is a real concern. Home computer security issues can affect the business community and wider stake holders. In 2011 BAE Systems Detica who delivers information intelligence solutions for governmental institutes reported that there were around 2.5 billion home users on the internet. This figure is expected to double in the near future. Along with the growth of the internet, security incidents are also growing at an alarming rate. According to United Nations Office on Drugs and Crime (2013) between 2005 and 2012, references to cybercrime news has increased 600 times compared to 80 times for other crimes. This is a worrying trend that can derail the confidence in internet business.

Theoretically, users can protect their home systems using a firewall, up to date anti-spyware, anti-virus and regular operating system and browser updates. Nowadays most operating systems come with built-in security settings to protect the computers. Also these systems are shipped with preinstalled trial version of antivirus software. Software venders like Microsoft who have the largest market share in home computer operating systems, supply operating systems with built-in firewall, antivirus software and regular automatic updates for the operating system and browser. However, users should ensure that these settings are not tampered with and follow best practices in computer security and this is why information security awareness is important.

According to a survey conducted by McAfee and National Security Alliance (2012) PCs around the globe revealed that more than 17% of computers worldwide had no antivirus protection and in the United States this was above 19%. Governmental agencies and organisations take security awareness seriously. The Australian government, with the help of the business community has been promoting National Cyber Security Awareness Week in every city. Also the Australian government has developed a web site (www.staysmartonline.com) to provide necessary knowledge for people to stay safe online. The United States government declared each October as National Cyber Security Awareness month. In the United States, the Cyber

Security Alliance with the help of the business community set up a website (www.staysafeonline.org) to educate users on the best practices of online safety. This is a very important first step. Ernst and Young (2004) identified security awareness as the most important activity to overcome the dangers of information security.

2.2 Security Practice and Security Awareness

Several studies recommend information systems awareness as the one stop solution for home computer security issues. A number of studies have been conducted on the importance of the security awareness and capability of home users to defend against computer security threats. Furnell *et al* (2007) conducted research on the security perception of home computer users. Their aim was to find out if the home users possess adequate knowledge to protect their home computer from cyber security incidents. The research was conducted in the UK by publishing the questionnaires on 24 different lifestyle websites. Among the 415 respondents, 43% considered themselves as advanced computer users and 50% considered themselves as intermediate computer users. One of the interesting things among respondents was that the educational qualifications varied from GCSE level to Doctorate. This represents a very good sample of general internet users and the results coming out of such research would be reflective of reality. Furnell *et al* (2007) found that home users who claim to have advanced IT expertise or knowledge were not following security best practises like installing operating system security updates, internet browser updates and security software updates. These results pose many questions.

People would expect that users who claim to have advanced IT expertise to behave more responsibly. Furnell *et al* (2007) suggested that all home users be given specialised training to address this issue. However the research failed to suggest the type and nature of the training. The researcher failed to test these if respondents really possessed “Advanced IT Expertise”. Any user who worked on a home computer for some time would consider themselves an IT expert. They many not necessarily have the required knowledge and experience of an IT specialist. If the researcher had some means to test respondents their “Advanced IT Expertise” claims this research would have been more complete. In this research professionals working in a multinational company are selected to avoid this drawback. During the survey, specific details of the IT certifications and the years of work experience will be collected to show the expertise of the respondents.

Furnell *et al* (2008) studied the security beliefs and barriers of internet users. According to Furnell *et al* (2008) in spite of experiencing security incidents, users weren’t bothered to protect their home system from external threats. This is an unexpected result. Based on the qualitative analysis of the responses they found that bad experiences don't change the majority of the home user’s security practices. This shows that they are not learning from their past experiences. Furnell *et al* (2008) concluded their research with two suggestions. The first one was to take away the responsibility of selecting the correct security settings away from the end user and enforcing through the manufacturer of the operating system and the second one was to give the users full access to the system only if the computer is compliant and up-to-date with the latest updates and patches. These are great suggestions that could guarantee improved security in home computers. However all these suggestions are not easy to implement. Most of the operating system and applications nowadays come with automatically updated features. This takes away the responsibility from the end user and can ensure that as and when security issues are addressed the customers can received them immediately.

Culnan (2008) conducted research among full-time employees who use computers at work and have a home computer. Their study could not find any relationship between awareness training and home computer security.

2.3 Security Awareness and Health Belief Model

LaRose *et al.* (2008) conducted research and found that increasing users threat susceptibility can improve users security behaviour. Their research revealed that increased threat susceptibility encouraged the respondents to install operating system and browser updates and conduct regular spyware and virus scanning. Computer users make a self-assessment of the cost of safe and unsafe practices. (LaRose, *et al.* 2008). Davinson and Silence (2010) supported these findings. In a study conducted by Davinson and Silence (2010) to predict user’s behaviour based on user’s perception on cost, threat, benefit and control found that by increasing the awareness of the user’s susceptibility, users behave more securely while doing online transactions. They recommend “seemingly tailored” risk messages for this. Their study was mainly based on the Health Belief Model (HBM). According to HBM a person will take care of health care seriously if the negative effects can be avoided.

The claim that says increased threat susceptibility encouraged the respondents to install operating system and browser updates and conduct regular spyware and virus scanning needs further research. The research was conducted in 2008 and by then manufactures implemented the auto update feature on most of the available operating systems. It may not be possible to say that this happened because of increased threat susceptibility.

There are many security tools available in the market to protect computers. Security companies and operating system manufactures develop security tools to protect home computers. However, computer users are reluctant to accept these security tools. West (2008) considers this as a major problem in information security. Users do not think that they are at risk. People often have “this won’t happen to me” attitude towards security.

Claar (2011) also conducted research to understand the home users computer security adaption behaviour using the Health Belief Model to identify the factors that affect the security behaviour. They adapted HBM to their research model and considered that humans use similar methods to protect one's health and protect a computer from attack. Claar (2011) also recommended security awareness as the way to address home computer security. Governments and private firms have been actively engaged in online security awareness trainings. Schools have been teaching the importance of computer security for the past decade. However more and more security issues are reported every day. It appears that security awareness alone cannot make the difference.

Anderson and Agarwal (2010) conducted research to explain home users computer security behavioural intentions. They conducted two studies in this research. The first one was to explain what really drives home users to perform security related behaviours. They used Protection Motivation Theory (PMT) and psychological ownership concepts to study the behaviour. According to PMT, the protection behaviours are based on the severity of the threat, the perceived probability of the occurrence, the effectiveness of the preventive action and the perceived self-efficacy. Based on the survey conducted among 594 users, Anderson and Agarwal (2010) found that the user’s security related behaviours are influenced mainly by the combination of three components: social, cognitive and psychological and the factors influencing the behaviour can easily be influenced by “message cues”.

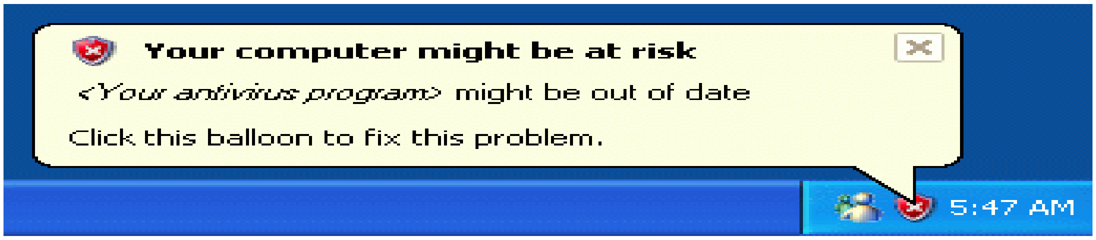
These are two conflicting findings. In the research that was conducted by Anderson and Agarwal (2010), they concluded that the factors that are influenced by the users behaviours can be easily influenced by message cues, whereas Davinson and Silence (2010) found that users behaviours can be changed by increasing the awareness of the user’s susceptibility. The main difference between these two studies is that, Anderson and Agarwal (2010) used Protection Motivation Theory whereas Davinson and Silence (2010) used the Health Belief Model to give theoretical underpinnings for their study.

2.4 Security Awareness and Protection Motivation Theory

Johnston and Warkentin (2010) conducted research on the effect of fear appeals on home user’s security actions. They conducted this research based on the Protection Motivation Theory (PMT). Their research revealed that fear appeal has some level of impact on users behavioural action to follow the recommended security action.

There are many studies conducted on the effectiveness of fear appeal and user behaviour. Software application and operating system venders have been using persuasive warnings in their products as pop-up dialog boxes to gather user’s attention and thus enable users to choose the right decision. These findings are implemented in modern day operating systems and in applications. However these haven’t been able to make home users more responsible in their choices. The positive effects of the safe practices can be as self-evident as the negative practices. People who have experienced the product flows in antivirus products would be hesitant to use it. Also installing an antivirus or anti-spyware often slows the computer and people would consider this as a nuisance and uninstall them. The regular software updates can really come in the way of user experience.

Siponen (2000) also stated that the use of persuasion in computer security tools and in applications can affect user’s attitudes towards security in a positive way. According to Witte (1992) as cited by Johnston & Warkentin (2010): “Fear appeals are persuasive messages designed to scare people by describing the terrible thing that will happen to them if they do not do what the message recommends”. Witte & Allan (2000) pointed out that the fear appeal can be considered effective only if the fear appeal helped the user to do the right thing. Roskos-Ewolden *et al* (2004) stated that the main purpose of a fear appeal in security management is to influence the user through persuasion. Microsoft has adapted the fear appeal and pervasion theory in their operating systems. They introduced a feature called Windows Action centre (previously called Security Centre) from operating systems starting with Windows XP. Figure 2.1 shows an example of fear appeal in Windows XP. If a computer is without security product or the antivirus software’s it gives below message to prompt users to take action.



Your computer might be at risk

<Your antivirus program> might be out of date

Click this balloon to fix this problem.

FIGURE 2.1 – Picture of fear appeal in Windows XP (Source: Microsoft 2011)

Microsoft controls more than 90% of the home PC market (Market Share Statistics for Internet Technologies, 2013). In spite of using a fear appeal and pervasion they still couldn’t make users do the right thing. A large percentage of Microsoft operating systems are still unprotected. (Microsoft Security Report 2013). It not clear how significantly fear appeal can influence users.

2.5 Security Behaviour and Technology Threat Avoidance Theory

Liang and Xue (2009) developed an IS theory that explains the threat avoidance behaviour of IT users. They named the theory, Technology Threat Avoidance Theory (TTAT). Historically IS theories were based on the adaption behaviour of IT users even though the ultimate goal of IT security is to avoid the threat. TTAT managed to explain the avoidance behaviour of IT users that other IS theories failed to explain. As the theory explains threat avoidance behaviour it contributed largely to the Information Systems Awareness. TTAT recommended that IT users not only be trained on the prospect of being infected by Malicious IT, but also the problems that they have to face if the IT gets compromised. (Liang and Xue, 2009).

In an attempt to provide a more suitable frame work for the analysis of Malicious IT and Information Systems Awareness (ISA) Mejias (2012) developed a research model that was developed based on the avoidance component of the TTAT and the positive feedback loops from the system dynamics and cybernetic theory. Their research revealed the importance of including technical knowledge, security impact and assessment of the damage to the Information Systems Awareness training. (Mejias, 2012). These findings are in par with Liang and Xue (2009) study. These suggestions are conclusive and can make awareness training more effective. When users are more knowledgeable about different aspects of technology and the dangers of Internet Security issues, they would be more prepared to protect their computers from these risks (Buchanan *et al,* 2007). Sriramachandramurthy, *et al* (2009) also stated that knowledgeable users are confident in adapting different methods to protect their computers.

D'Arcy (2009) proposed three security counter measures for organizational security.

1. User awareness of security policy
2. Security awareness and training
3. Information systems monitoring

This is type of a security measures are practically possible in an organisation. Since security is not enforced on home computers and monitoring is very limited; such measures won't be practically possible in home systems. Is it possible to give comprehensive security training to home users? This could be possible in an organisation setting. Even in organisations security awareness training alone cannot make a difference

We have seen that muchresearch was conducted on user's security adaption behaviour. However no one could explain why good users make bad choices when it comes to security. There are many security tools available in the market to protect computers. Security companies and operating system manufactures develop security tools to protect computers. However, computer users are reluctant to accept these security tools. West (2008) considers this a major problem in information security. According to a survey conducted by McAfee and the National Security Alliance on PCs around the globe, more than 17% of computers worldwide had no antivirus protection and in the United States this was above 19%.

Users do not think that they are at risk. People often have a “this won’t happen to me” attitude towards security. It is shocking to know that 64% of smartphone users do not use a security software or application to protect their smartphone (Davis, 2012).

2.6 Security Behaviour and Theory of Planned Behaviour

Another theory that was prominent in predicting the security behaviour is the Theory of Planned Behaviour (TPB). The theory states that attitudes toward behaviour, subjective norms, and perceived behavioural control together shape an individual’s intentions and behaviours (Ajzen, 1991). The different constructs used in this can be explained as follows:

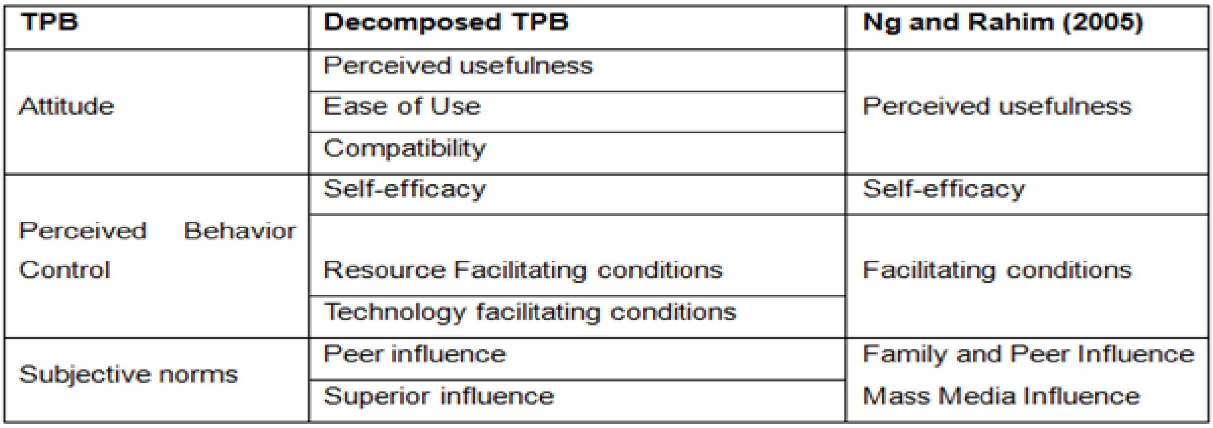
Attitude toward behaviour: This explains user’s willingness to perform a particular action. And why they adapt that behaviour.

Perceived behavioural control: How capable the person thinks he/she is to perform the specific behaviour or action.

Subjective norm: Subjective norm deals with the social influence. What do other users do when they are in such a situation?

Ng and Rahim (2005) developed a model for home computer user’s intention to practice safe security actions based on TPB and the Decomposed TPB.

TABLE 2.1 – Difference between TPB and Decomposed TPB



TPB	Decomposed TPB	Ng and Rahim (2005)
Attitude	Perceived usefulness	Perceived usefulness
	Ease of Use	
	Compatibility	
Perceived Behavior Control	Self-efficacy	Self-efficacy
	Resource Facilitating conditions	Facilitating conditions
	Technology facilitating conditions	
Subjective norms	Peer influence	Family and Peer Influence
	Superior influence	Mass Media Influence

To access their model Ng and Rahim (2005) surveyed 233 undergraduate students who were home users and asked 75 questions pertaining to security. The questions were developed based on the recommendations of United States Computer emergency response team co-ordination centre and were based on updating of antivirus software, backing up of critical data and firewall usage. The survey results supported their model. However if we go through the survey questions one would question the results of the research. Many questions in the questionnaire were about updating the antivirus software and the researchers did not take it to account that a most antivirus programs update their software automatically. For example, they asked the question “FC1: I have the time to update my anti-virus software regularly within the forthcoming month. (Agree/disagree)” to measure the “Facilitating Conditions”. For this reason in this research the option to select “Antivirus is set to update automatically” is added as a choice to get accurate analysis.

Culnan *et al* (2008) conducted a study to measure the attitude and behaviour of home users who were exposed to organisational security awareness training and who were not. They asked questions based on antivirus updates, firewall use and installation of software updates and they also found that those underwent such trainings were involved in behaviours that help to protect home computers. Culnan *et al* (2008) provided two recommendations in addition to the organisational awareness training. They recommended that organisations should implement steps to reduce the “risk of breach” and provide direct technical support to home users. They suggested the following steps.

Reduce the risk of breach:

- Provide secure connectivity to organisational network.
- Limit the amount of data stored on home computer.
- Enforce password protection whenever there is a need to store data locally.

Technical support to home computers:

- Provide phone or e-mail support for employees home computers.
- Employees to bring their home computer to helpdesk upon security issues for repair.
- E-mail alerts and websites to warn users on new threats and provide security tips.

These look like very effective recommendations however the cost involved in implementing such suggestions could be enormous. At a time where businesses are trying to reduce cost of operations, IT Executives may not get sufficient budgets to implement such costly recommendations.

2.7 Psychology of Security Behaviour

Why do good users behave badly when it comes to security? Academics have been trying to answer this question. Designers of security products must understand why people ignore their warnings and choose unsafe settings. West (2008) pointed out that people often have “this won’t happen to me” attitude towards security. He identified eight reasons why people behave this way such as:

- Users do not think they are at risk
- Users are unmotivated
- Safety is an in abstract concept
- Feedback and learning from security related decisions
- Evaluating the security/cost trade-off
- Making trade-off between risks, losses and gains

- Users are more likely to gamble for a loss than accept a guaranteed loss.
- Losses perceived disproportionally to gain

West (2008) recommends below four actions to improve user's behaviour.

- Reward pro-security behaviour
- Improve the awareness of risk
- Catch security policy violators
- Reduce the cost of implementing security.

Users do not consider security that is a priority for them. Users do not think that they are at risk. People often have a relaxed attitude towards security. In a survey conducted by AOL and the National Cyber Security Alliance reported that 72% of home users did not configure their firewall and only one-third had up-to-date anti-virus signatures. Some researchers used a Folk model to identify why users behave badly. A Folk model is a culturally based way of perceiving or understanding something. It is considered as a mental model as it helps us to understand how users think about a problem. (Johnson-Laird *et al*, 1998). Using the Folk model, Wash (2010) conducted research to identify home users security behaviour. He studied two research questions. 1) Potential threat: How do home users conceptualize the intermediate security threats that they face? 2) Security response: How do home computer users apply their mental model of security threats to make security relevant decisions? Wash conducted semi-structured interviews in two different intervals. First he interviewed 23 people and then 10 people. Participants were selected via a snowball sample of home users in three different cities in the USA. They were asked questions about their "Perception of threat" and "defensive action".

From the research Wash (2010) identified four folk models regarding virus models such as Bad, Buggy Software, Mischief and Crime. From his analysis he found out that people who regarded viruses as "Bad" and "Buggy software" were less concerned than people who considered viruses as Mischief and Crime who were more concerned about viruses and the percentage of people in this category was less. Wash (2010) concluded that most home users use these folk models to identify security and since they are not bothered about these threats they would not take preventive action against them.

2.8 Security Best practices for Home Computers

Security best practices to secure home computers are taken from Australia and United States stay safe initiatives and the United States Computer Emergency Response Team (US-CERT). Some of those best practices that are applicable for this research are detailed below. Implementing a password authentication is the most inexpensive way to enforce security. Even though many other forms of security are available, password authentication became a popular and widely used authentication method. (Zhenag *et al* 2009). The United States computer emergency readiness team set out a number of recommendations for effective password security. According to US-CERT (2013) hackers use a number of programs to crack user's weak passwords and they recommend users to use strong password to counter this threat.

Passwords are the most commonly used authentication method. (Zhang *et al* 2009). Passwords act as the first level of security and often times the last level of security. Since they are cost effective and easy to implement most IT organisations use them as their authentication method. Even though password authentication is popular it is subjected to directory attacks, password hacking attacks and numerous other forms of security attacks. (Frank 2008). Organisations implement strict password policies to ensure security of their information technology resources. However these are not enough. Many users use the same or weak passwords (Computerweekly 2009). According to a study conducted (MacGibbon and Phair, 2011) among Australians to understand their password:

1) 60 % of Australian internet users use same or common password for multiple online accounts.
2) Half of Australians change their password; only when the system asks them to do so.

These findings suggest that home users underestimate the threat from hackers who know this behaviour. Hackers steal passwords from one site and use it on other sites to gain access. Passwords are not categorised as strong if it is shorten than eight letters. Microsoft (2013) recommends that a password must contain at least eight characters and it should be a combination of uppercase/lower case and alpha numeric characters. McCrohan et al (2009) stated that effective password usage is an indication of user's security awareness and commitment towards effective security.

Tam *et al* (2010) studied the psychology of password management among computer users. The aim of their study was to study following research questions:

a) Do users understand what constitutes a secure password and good password management?
b) What are the motives behind password selection and password management behaviours?
c) Are there any differences in password management behaviours for different types of accounts?

For this research Tam *et al. (2012)* used university students as samples. They analysed survey results from 130-150 users. They concluded that users understand what constitutes a good password and the consequences of having bad password behaviours. With respect to the motivation research question, Tam *et al.* (2010) stated that the password selection behaviours are very complex and it is the "convenience-security trade off" that decides the password quality. For the third research question they concluded that users password behaviours change with the nature of the account that they use the password for. Tam *et al.* (2010) found that users tend to show better password management behaviors when there is a "personal" or "privacy" element involved. Based on their findings Tam *et al.* (2010) recommended security awareness training.

The above literature offered a great deal of insight to this study. Their study has many similarities to this research. The main similarity is both these research studies are about the behaviors of home users. There are some significant differences also between these two studies and the main one is that Tam *et al.* (2010) used university students as samples whereas for this study systems professionals are surveyed.

Campbell *et al*. (2011) conducted a study among undergraduate students to find out the effect of a restrictive password composition policy. Using an experimental research method they found that the restrictive password selection policy did not have any effect on the password selection. While analyzing the results, Campbell *et al*. (2011) found that it is a common practice among users to use the same passwords and passwords similar to directory listed words. However thy failed to explain why users behave this way. Campbell *et al.* (2011)

concluded the research by suggesting that organisations should stop using restrictive a password policy as it doesn't have any effect on password selection.

The suggestion for not using a "restrictive password policy" may not be widely acceptable. It warrants more studies to see if the results of a research study conducted among college students can be directly applicable in an organisational setting where these changes can cause unforeseen consequences. The results would have been more conclusive if the study was conducted among employees.

E-mails are an effective and popular method for communication. This makes them a target for attackers. According to Temple (2012) there are almost 204 million e-mails sent around the world. This is a massive number. Due to the efficiency of anti-spam software most of these e-mails do not reach users inboxes. US-CERT advises citizens to be careful when they send, receive and open e-mails. They advise people to check the sender and the subject before they open e-mails. Also when it comes to attachments; US-CERT advises their citizens to open them only if they know it is legitimate.

It was found that more than 80% of internet e-mails are either scams or spam. Phishing e-mails are very common nowadays. Phishing is also called spoofing, where spoofers send out e-mails that appear to be from financial institutions or governmental agencies to a large number of recipients to steal their valuable information which can be used for identity theft. Financial institutions and security experts have been warning users not to provide personal information online. And also check for the "https" before clicking on the web link. In spite of all this advise phishing is on the rise.

Operating system updates play a crucial role in keeping computers safe and secure. Operating system manufactures realise the importance and have created an automatic schedule to download and install updates from their location. It is recommended to keep the operating system up-to-date. Security software removes the malicious content from the computer and stops it from damaging personal information. Like operating systems it is important to keep the security software up-to-date and perform regular scans to make sure the home computer is safe. Antivirus manufactures offer an automatic updates service to facilitate this.

2.9 Conclusion

There is a common agreement among academic researchers on the importance of security awareness training. Almost all researches recommended such training. There are conflicting findings on how home users who underwent security training behave in the home computer environment. Also there isn't any convincing study conducted on how users with "Advanced IT skills" manage their home computers. Those researchers who study this failed to test users "Advance IT skills" claim. Fear appeals and threat susceptibility are some of the recommendations that came out of research. Some researchers pointed out that users have a relaxed attitude towards security and when they think or hear security issues they often think that "this won't happen to me" and ignore security warnings.

There is not any study conducted on how system professionals who are aware of security best practises manage their home computers. For this study we selected systems professionals who are working as support engineers as the focus group as these engineers have expertise in implementing and troubleshooting security practises. The reason for us to select support engineers is that they fall under the category of advanced system users and are aware of security best practices. Also there is a higher chance that these professionals underwent organisational information security training.

3 Research Methodologies and Fieldwork

3.1 Introduction

This chapter details the method that is used in this research to find answers to research questions. This chapter discusses different types of research methodologies and the reason for using them in this research.

Saunders *et al.* (2009) developed a concept called a “research onion” to explain different steps that need to be carried out in research. Figure 3.1 shows the picture of research onion. The concept of the research onion model acts as a great tool for researchers in planning their research. In this chapter the research onion concept is used to explain the research methodology.

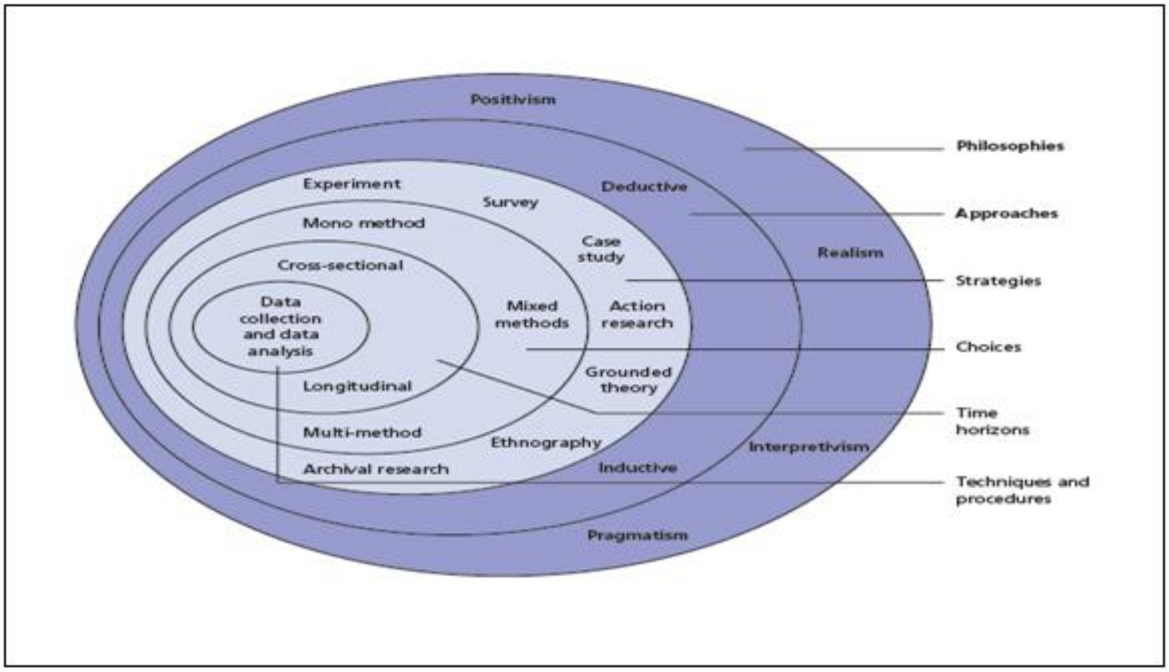


FIGURE 3.1- Picture of Research Onion (Source: Saunders *et al.* (2009))

3.2 Research Philosophy

Philosophy is the first layer of Saunders' research onion. While doing research it is important to choose the right philosophy because a researcher's psychological assumptions are very critical in research (Klenke 2010). Also assumptions that researchers make as part of research philosophy support the research strategy and the research method (Saunders *et al.* 2009). According to Collier (1974) as cited by Dobson (2002) the alternate to philosophy is not "no" philosophy, but bad philosophy. Saunders *et al*. (2009) consider the following three as the main philosophies of research: ontology, epistemology and axiology. According to them ontology is the researcher's view of the nature of reality or being, epistemology is the researcher's view regarding what constitutes acceptable knowledge, and axiology is the researcher's view of the role of values in research.

3.3 Research Paradigm

According to Kuhn (2010) a paradigm is the understanding, assumption and intellectual structure on which the research in a field is based. In social research there exist many research paradigms. According to Blaikie (2007) there are four research paradigms, such as Positivism, Critical Rationalism, Classical Hermeneutics and Interpretivism. However Saunders *et al*. (2009) considered Positivism, Realism, Interpretivism and Pragmatism as the four paradigms.

According to Wynn *et al*. (2012) the majority of research in Information Systems has been conducted either in positivism or in interpretivism. Saunders *et al.* (2009) explains that in interpretivism the researcher is a part of the research and cannot be separated from the research whereas in positivism, the researcher is independent of the research subject that is being studied.

TABLE 3.1 - Comparison of four research philosophies in management research

	Positivism	Realism	Interpretivism	Pragmatism
Ontology: The researchers view of the nature of reality of being	External, objective and independent of social actors	Is objective. Exists independently of human thoughts and beliefs or knowledge of their existence	Socially constructed, subjective, may change, multiple	External, multiple, view chosen to best enable answering of research question
Epistemology: the researcher's view regarding what constitutes acceptable knowledge	Only observable phenomena can provide credible data, facts. Focus on causality and law like generalisations.	Observable phenomena provide credible data, facts. Insufficient data means inaccuracies in sensations (direct realism).	Focus upon the details of situation, a reality behind these details, subjective meanings motivating actions	Focus on practical applied research, integrating different perspectives to help interpret the data
Axiology: The researchers view of the role of values in research	Research is undertaken in a value-free way, the researcher is independent of the data and maintains an objective stance	Research is value laden; the researcher is biased by world views, cultural experiences and upbringing.	Research is value bound, researcher is part of what is being researched, cannot be separated and so will be subjective	Values play a large role in interpreting results, the researcher adopting both objective and subjective points of view.
Data collection techniques most offer used	Highly structured, large samples measurement, quantitative, but can use qualitative	Methods chosen must fit in the subject matter, quantitative or qualitative	Small samples, in-depth investigations, qualitative	Mixed or multiple method designs, quantitative and qualitative

Source: Saunders *et al*. (2009:116): Comparison of four research philosophies in management research.

In selecting the appropriate research paradigm for this research both Positivism and Interpretivism were considered. The main difference between the Positivism and Interpretivism is Positivism is scientific and used to prove a theory or universal law whereas Interpretivism about is about studying the reality or behaviours. (Tuli 2011) Interpretivism is therefor considered as the most appropriate for this research as human behavior is studies here.

3.3 Research Approach

There are mainly two types of research approaches used in information system research namely inductive and deductive. (Blaikie, 2009). A deductive approach is used when the researcher intends to establish a hypothesis using a theory, whereas the inductive approach is used when a theory is developed as an outcome of the data analysis. Also an inductive approach is more flexible as there is no pre-determined theory to collect data. (Saunders *et al.* 2009). Deductive research is the method used for positivism philosophies (Gill and Johnson, 2002).

In this research, an inductive research approach is selected as the research method. The main reason for selecting an inductive approach is that, in this case study research security behaviors of system professionals are observed using data samples and semi-structured interviews. No hypothesis or theory is tested in this study. Also an inductive method that is more aligned to the interpretivist philosophy is selected as the research philosophy for this research.

3.4 Research Strategy

Strategy is the third layer in Saunders' research onion. To identify the correct research strategy for this research, prominent works were reviewed on research methods. Some of the strategies that are reviewed were: experiment, survey, case study, action research, grounded theory, ethnography and archival research. (Saunders *et al*. 2009).

Of these, case study research strategy is selected for this research. The reason for the selection of a case study is that it is the suitable research strategy that can be used to study the behavior of a group of people. In this research the researcher intended to study the security behaviors of information system professionals. Robson (2002) defines a case study as “strategy for doing research which involves an empirical investigation of a particular contemporary phenomenon within its real life context using multiple sources of evidence”. Also a case study strategy is more suitable to answer the why, what and how research questions as it supports detailed investigations that are essential to answer these questions (Yin 2003). Another reason to choose a case study research strategy was its flexibility. Different types of data collection can be used in a case study research to explain or study the phenomena or behavior. (Benbasat, 1987). Since a case study supports multiple data collection methods, such as interviews, distribution of questionnaires etc. it gives the researcher extra flexibility in data collection. Data collection for this research is performed using a combination of conducting interviews and distribution of the questionnaire. A detailed data collection process is explained in the data collection methods section of this chapter.

According to Yin (2003) there are four types of case study research strategies that are considered in two different dimensions; such as the single case v. multiple cases or the holistic case v. embedded case. We have adapted a single case strategy for this research as it is suitable for unique phenomena that are not considered before. Moreover we considered this as a single case as we are considering all samples in our research as systems professionals.

3.5 Research Choices

In academic research there are mainly three research choices that exist such as the mono method, multiple methods and mixed method. In the mono method only single data collection and analysis method are used. In multiple methods and multi-methods more than one data collection techniques are used. The difference between these two is that in the multi-method one cannot mix quality and quantity data collection and analysis where as in mixed-methods the research can mix both them for data and analysis. (Saunders *et al.* 2009). Brown *et al.* (2012) also confirm the use of both qualitative as well as quantitative methods independent or dependent on mixed method.

In this study, a mixed research choice is selected as both qualitative and quantitative methods for data collection and analysis were used for this research. According to (Teddlie and

Tashakkori, 2009) the mixed methods research has the capacity to test confirmatory and exploratory research questions simultaneously.

3.6 Research Time Horizons.

Time horizon is the second inner layer in the research onion. There are two types of time horizons, longitudinal and cross sectional. In the longitudinal study the researcher observed the phenomena for an extended period of time where as in the cross-sectional one the time is limited or fixed. (Saunders *et al.* 2009).

For this research a cross-sectional time horizon had been selected as there is limited time for this research.

3.7 Population

A research population is the total number of individuals or objects that are the main focus of the study. This single case study research, which accesses the behaviour of system professionals on their home computers is applicable to the entire community. Since it is not possible to collect information from the entire population sampling is considered.

3.8 Sampling

Sampling was used on the subset of the population that are participating in the study. There mainly two types of sampling. Probability sampling and Non-Probability sampling.

- Probability sampling:
  With this type of sampling the randomness of the selection of participants is known.
- Non-probability sampling.
  In non-probability sampling the randomness of the selection of participants is unknown. There are mainly three types of non-probability sampling such as Quota sampling, Snowball sampling and Convenience sampling. For this research Convenience sampling is selected.

3.9 Convenience Sampling

This is a popular method of sampling. However the main drawback for this method is that it is highly unlikely to be representative of the population. This is more useful when there is little variation in characteristics of the population. For this research convenience sampling is used because it is not practically possible to include the entire systems community. Care has been given to select a convenience sample of system professionals that represent the characteristics of the population.

For this reason this study is carried out among the entire population of system professionals in a multinational company in Ireland. A team called the Advanced Support Team is conveniently selected for this study and all the team members are the subject of the study. This team consists of 46 highly experienced system professionals who have professional experience ranging from 8 to 25 years. All professionals were surveyed and 42 responses received and 41 of them were valid. Therefore this matches the population of interest as it provides a good mix of highly skilled, sampling frames from different nationalities, cultures and experience.

3.10 Generalisability of the Findings

The purpose of this research is to identify how people who have advanced computer knowledge who are aware of computer security manage their home computers. For this reason the participants must have a high level of systems knowledge. Because of this the population for this research are System Professionals. The reason for selecting system professionals is because our aim is to study how knowledgeable users, people who are aware of security manage it. For this, participants must possess high level of computer knowledge and thorough working experience. The sampling method used in this research is convenience sampling as it is impossible to sample the entire community. The main drawback of this type of sampling is generalizability.

The team of professionals identified for this study work in a multinational in Ireland that has $50 billion revenue. The survey request was sent to the entire 46 member Advanced Support Team. Out of the 46 team members, 42 of them completed the survey questionnaire validly with a participation rate of 91%. The participants of this research are people with extensive knowledge and experience. The overall work experience of the participants varies between 8 to 25 years. Also all of them have completed 2 or more years with their current employer and have undergone organisational IT security awareness training, because of the drawback in the convenience sampling the results cannot be generalised.

3.11 Conduct of the Research

This section details the process carried out to conduct the research of the home computer security behaviour of system professionals working in a multinational company in Ireland. Section 3.7.1 details the literature review carried out to find the academic research that is carried out in this area. The complete literature review is available in Chapter 2 and it is used as secondary data.

3.11.1 Literature Review

A comprehensive literature review is available in Chapter 2. The literature review was conducted to get a theoretical underpinning of the research subject. A wide range of books, peer-reviewed journal articles and internet articles were reviewed to study the research subject. The literature review provided a base for the development of a questionnaire and face-to face interviews.

3.11.2 Population selected for this study

For this research, convenience sampling is adapted. An team of system professionals is selected for this study. AST, which is a part of the Enterprise Expert Centre (EEC), consists of 46 highly experienced system professionals who work as the last level of support for customers for their complex technology issues. The team was formed in 2002 with seven support professionals and due to the continuous growth of the business the team expanded and has currently 46 members. The AST has professionals from 11 different nationalities. This team is highly experienced and well certified.

Therefore this matches the population of interest as it provides a good mix of highly skilled, sampling frames from different nationalities, cultures and experiences.

3.11.3 Triangulation

Triangulation is the process of validating the findings by incorporating several viewpoints and methods. (Yeasmin and Rehman, 2012). Triangulation is used in case study research to provide further clarity and validity in the research findings as it enables us to use data collected from multiple sources. (Blumberg *et al.* 2005). As cited by Hussein (2009) the use of triangulation originated in 1959 from Campbell and Fiske (1959). The combination of the usage of different data collection methods like literature reviews, online surveys and unstructured interviews enable the researcher to validate findings against each other (Oslon, 2004). There are different types of triangulation, for this research Methodological Triangulation is chosen as it is about using more than one research method or data collection technique.

In this research, triangulation is used to compare the analysis of the findings of the questionnaires with the theme of the comments that are taken during the face-to-face interview on specific behaviors and the findings of the literature review.

3.11.4 Data collection

This section details the process involved in the collection of primary data for this research. This section details the development of the questionnaire, distribution of the questionnaire and conduct of the face to face interview.

- Development of the survey questionnaire

The questionnaire was developed with the help of different academic sources and the security best practices that were set out by the Australian and American government to secure home computers as detailed in the literature review. The number of questions in this survey is 23. These questions are divided in to two sections. Section A and Section B. Each section is further divided in to following categories.

a) Attitude towards security incidents
b) E-mail and online security
c) Password usage and management
d) Security software usage
e) Operating system updates
f) Proactive security behaviour.

a) Attitude towards security incidents: This section contains one question and is aimed at collecting the attitude of participants on security incidents. What do they think when they hear or read of a particular cyber security incident and the choices were: This won't happen to me, I think security is someone else's responsibility, and I take steps to improve the security. Question 2 (Q2) of the survey deals with this question. Survey questionnaire is given in Appendix - A.

b) E-mail and online security: There are four questions in this category. The purpose of these questions is to find out how responsibly users behave when they check e-mail. Q3, Q4, Q5 and Q6 are designed find e-mail and online security behaviour. Survey questionnaire is given in Appendix - A.

c) Password usage and Management: There are three questions in this category and they are used to find out how members of the AST manage their home computer passwords. Survey questions Q16, Q17, and Q18 fall in this category. Survey questionnaire is given in Appendix - A.

d) Security software usage: There are five questions in this section. The purpose of these questions is to find out the respondents' security software usage pattern and behaviour. The questions that belong to this section are Q10, Q11, Q12, Q14, and Q15. Survey questionnaire is given in Appendix - A.

e) Operating system updates: There are two questions in this category. These questions find out if users use the latest service packs on their computer and if auto update is enabled or disabled in their home computer. Survey questions Q7 and Q8 belong to this category. Survey questionnaire is given in Appendix - A.

f) Proactive security behaviour: There are three questions in this category to test the proactive security behaviours of the respondents. The questions that belong to this category are

Q.9) Do you check /monitor the status of the operating system updates?
Q.14) How often do you perform full system an antivirus scan?
Q.15) How often do you backup your home computer?

Section B is designed to collect demographic details of the respondents and this contains multiple choice questions. The age, sex and nationality are not collected because this would help to identify the respondents as the population is small. Survey questionnaire is given in Appendix - A.

- *Distribution of the Questionnaire:*

In this research, the questionnaire is created using Survey Monkey, a web based tool. A web-based tool is adapted as this is faster, more cost effective, convenient, and automates the data collection (Warde *et al.* 2001). Also the web guarantees the anonymity of the respondents. This questionnaire was sent to all 46 members of the AST through e-mail. The purpose of this questionnaire is to collect the security practices of these professionals in their home setting.

- *Development of the face-to-face Interview:*

A semi-structured face-to-face interview was conducted among 10% of the respondents, making comments on the specific behaviours of the respondents. This interview consists of four questions. These interviews were not audio taped. However, notes and comments were taken during the interview.

The purpose of the interview was to get answers for the 'why' questions that were identified during the analysis of the data. Because of this it was conducted after the data collection and primary analysis of the data was completed. Four members of the AST were asked to comment on following questions.

1) Why do system professionals score low on firewall usage?
2) Why are system professionals reluctant to use security software?
3) Why do users show poor password management?

3.12 Analysis of the Data

3.12.1 Quantitative data analysis

The responses for the survey questionnaires were either 'Agree/Disagree' or 'Yes/No'. Since it is difficult to analyse the data in this format, responses were converted in to dichotomous values. To prepare the data for analysis, coding was applied to make sense to the data. Coding is the process of converting information from responses into a value that can be analysed. The coding that we used for this analysis is 0=No, 1=Yes. This doesn't mean that 'Yes' is bigger than 'No' or 'No' is bigger than 'Yes'.

After converting the responses into dichotomous values, Excel data analysis was used for the initial analysis. Using Excel's histogram data analysis, the percentage of the frequency of selection of safe and unsafe practices was identified. For the purpose of a more detailed study the questionnaires were further divided into two categories: High Impact and Low Impact security practices. The High and Low Impact questions are given in Appendix D. The High Impact categories are the ones that can make one's own computer vulnerable and can spread infection to other computers. The High and Low Impact security practices were analysed using a histogram to find a trend in the way respondents answer the questionnaire.

An inferential statistical analysis will be performed on the High Impact and Low Impact practices against their safe or unsafe behaviour using Chi-Square. Chi-square tests for goodness of fit, whether one categorical variable differs from an hypothesised distribution. Also a X2 test for association tests whether two categorical variables are associated was used.
The formula for Chi-Square is:

X^2 = Sum ((observed - expected)^2 / expected))

The Chi-Square analysis method will be applied on the High Impact and Low-Impact practices against the behaviour. If the probability value **p** is less than or equal to 0.05 the null hypothesis will be rejected and if the p value is > 0.05 the null hypothesis will be accepted.

Attitude analysis of the AST towards security incidents were collected using the attitude question that was explained in 3.7.4. The coded responses will be filtered using Excel based on respondent's attitudes towards High and Low Impact practices to see if attitude has any impact on security practices. Also different categories of data will be compared against the attitude of AST. The results of these findings will be compared with the literature reviews and the comments received in the face-to-face interview.

Further analysis will be performed to find out the proactive security behaviours of AST. The results of these findings will then be compared against the literature review and the theme of the face-to-face interview.

3.12.2 Analysis of the face-to-face interview.

The purpose of face-to-face interviews is to get comments on the specific behaviour of system professionals that are identified in the data analysis of the quantitative study. The comments received during interviews are categorised and coded based on the responses to understand the pattern and their interpretation is used to shed light on their behaviour.

3.13 Research Ethics

Ethics in research has been a serious concern ever since research began. It is no possible to define good ethics and bad ethics. Ethics concerns in research reached a peak in the 1960s when the story of the infamous Nazi concentration camp research was released. Bryman (2012). As cited by Bryman (2012) there are four guidelines to consider when doing research such as whether there is harm to participants, whether there is lack of informed consent, whether there is an invasion of privacy and whether deception is involved. Trochim (2006) suggested that the research participation must be voluntary and the informed consent must be sought from the respondent and the identity of the participants must be kept anonymous throughout the research even to the researcher.

To protect the rights and welfare of the participants and to comply with the law of the land ethics approvals are necessary. A Research Ethics committee set up by Trinity College oversees the ethical issues that can arise during the research study. Therefore before the research is conducted, an application for ethical approval was submitted to the College Ethical committee and upon reviewing the research documents and procedures the permission to conduct the research was granted. All participants will be given a copy of the “Participants Information Sheet” and an “Informed Consent Form”. The Participants Information Sheet details the purpose of the research, methods and procedures, and explains the anonymous and voluntary nature of this study. Participants information sheet is given in Appendix I. All participants are requested to sign the “Informed Consent Form” before answering the questionnaire. Since the questions are published online, the online survey is designed in such a way that the participants must read and agree before they take the questionnaire. To ensure the anonymity of the respondents, the survey questions are published through Survey Monkey.

4 Findings and Analysis

4.1 Summary

This chapter summarises the analysis and findings of the data collected using the survey questionnaire and the semi-structured interviews. The purpose of this case study research is to find out how advanced system users (information system professionals) who are aware of information security best practices manage their home computers.

To help identify the behaviour the following research questions were developed.

1) How do the security behaviours of system professionals differ from novice home computer users?
2) How does the attitude towards security influence the security practices of system professionals with their home computer?
3) How do systems professionals respond to manufacturer enforced security settings on their computers?

From the literature review it was found that academics expect knowledgeable users to show more secure behaviour when it comes to security. However this case study did not support that argument. This research did not show a great deal of security practice from the advanced system users. However it was found that manufacturer enforced security best practice settings remain intact, unless users purposefully change them and this could be a new way forward. There were instances in which knowledgeable users disable security settings for their convenience and prevent the enforced settings from taking effect.

The research was carried out as explained in the previous chapter. The primary source of data for analysis was collected using an online survey to collect the demographic information of the respondents and the responses for the questionnaire. The data collected using the face-to-face interviews and literature reviews was used as secondary data.

4.2 Background of Advanced Support Team

The Advanced Support Team (AST) which is a part of the Enterprise Expert Centre (EEC) consists of 46 highly experienced system professionals who work as last level support for customers for their complex technical issues. The team was formed in 2002 with seven support professionals and due to the continuous growth of the business the team has expanded and has currently 46 members. The AST has professionals from 11 different nationalities.

4.3 Demographic Profile of Respondents

Survey requests were sent to 46 system professionals in the AST and 42 respondents or 91% completed the survey. All responses received were complete and valid. The work experiences of respondents range from 8 to 25 years. The survey collected the amount of time each respondent was employed with the current employer. The survey also collected details of the industry recognized certifications each respondent possessed. It is found that between the respondents there were a total of 76 industry standard certifications.

This is a great number to show that all respondents are truly professional and have advanced IT knowledge. Figure 4.1 shows the number of certifications in each technology. This shows the level of experience of people who participated in this survey. The experience varied from 10 years to 25 years. Figure 4.2 shows the distribution of work experience among the AST. This indicates that these respondents have been in the industry over a decade and have seen the way the information technology and security requirements changed over the years.

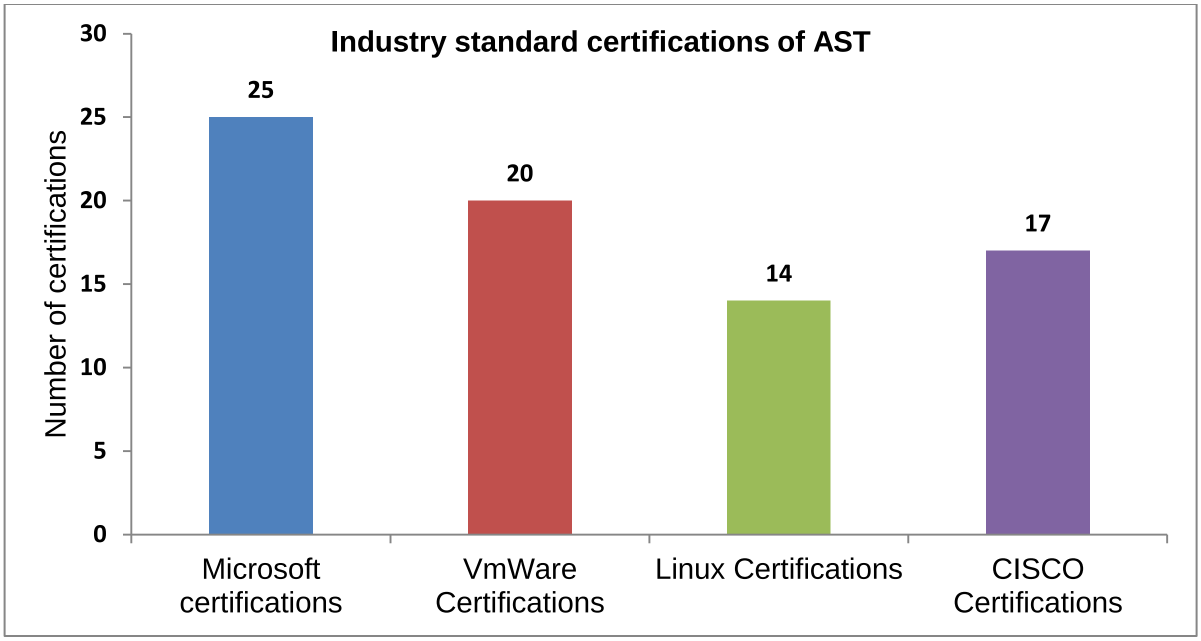


FIGURE 4.1 - Number of certifications in AST.

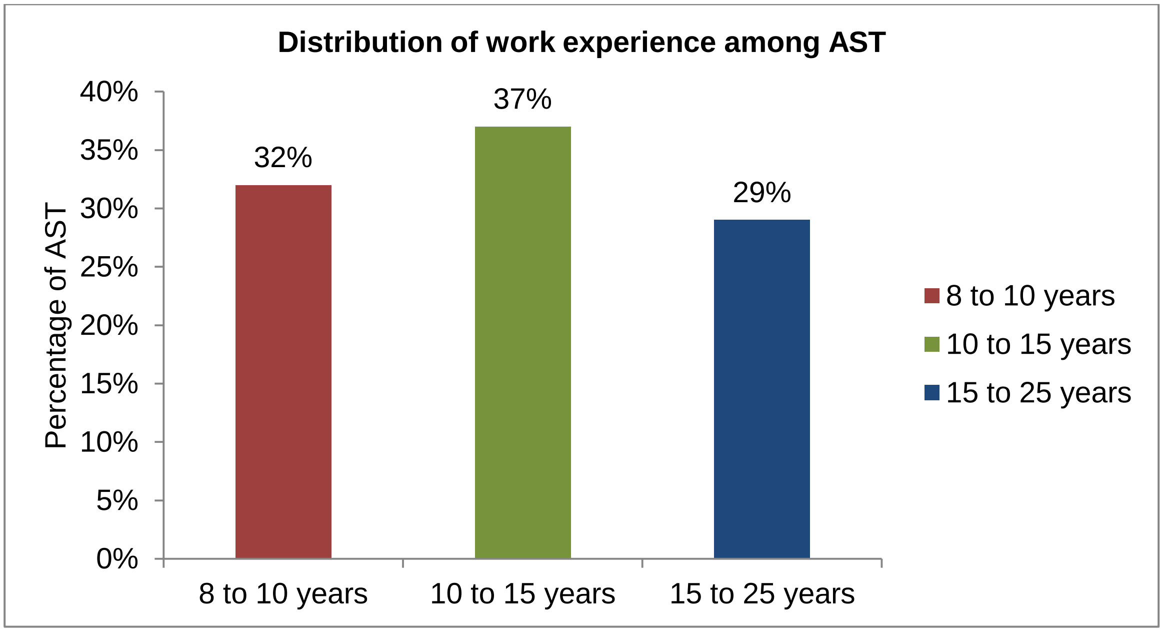


FIGURE 4.2 – Distribution of work experience among AST.

4.4 Security Behaviours of System Professionals

Based on the analysis of the data it is found that there is not much difference between the behaviours of system professionals and home users. This would indicate that people who are aware of security practices follow or exhibit the same behaviour as novice home users. This section gives analysis details of the research question: “How do the security behaviours of system professionals differ from novice home computer users?” The analysis is based on the frequency distribution analysis of security behaviour on different security questions. Analysis of the responses shows that the security awareness, experience or knowledge of security best practices does not influence the security behaviour. The frequency analysis performed on the responses showed that 72% of practices followed by system professionals are safe and 28% are unsafe. Figure 4.3 shows the distribution of security practices among AST.

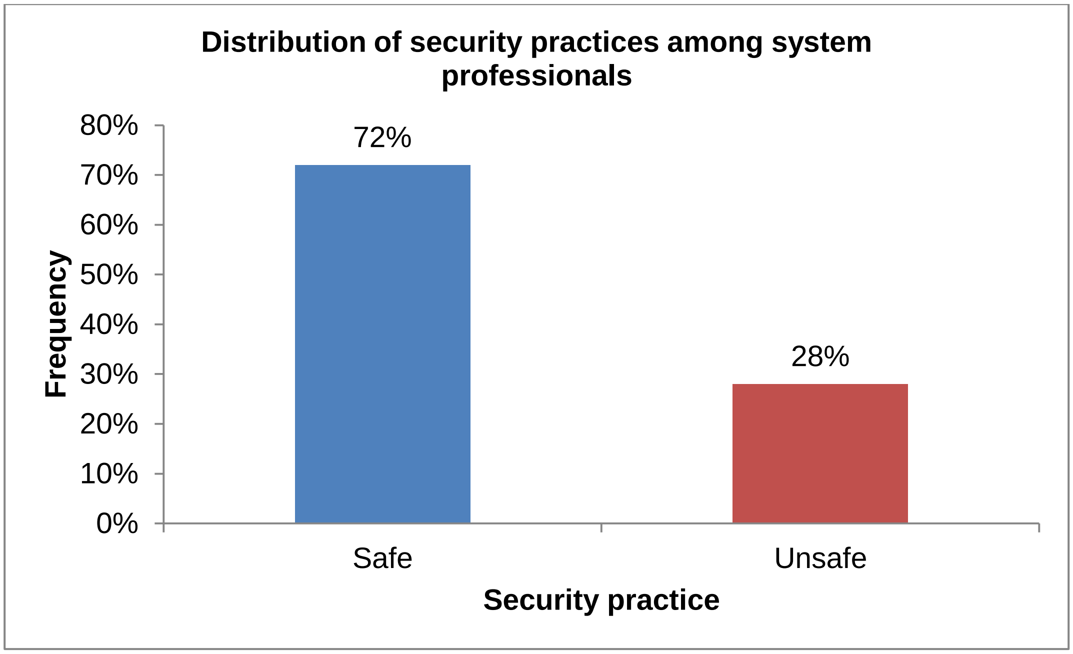


FIGURE 4.3 – Distribution of security practices among system professionals

To get a deeper understanding of the behaviour, survey questions were divided based on the severity of the security activity called High Impact (high risk) security action and Low Impact (low risk) security action. High impact security actions are those actions that are critical for the safety of the home computer. Not following them could put the computer at high risk. Following these practices will help users to keep the computer safe free of malicious activities. Low impact security actions are mostly proactive actions that are recommended for ensuring

the security of the home computer. The analysis was done using the histogram frequency analysis, and found that system professionals follow more High Impact practices than Low Impact practices. Figure 4.4 shows the graphical representation of the High Impact and Low Impact distributions. The separation and questions belonging to both categories are given in Appendix D. 78% practices that fall in the High Impact (High risk) category followed by members of AST are safe practices and 22% of them are unsafe. It is also found that within the Low Impact security practices 66% of practices that are followed by respondents are safe and 34% of practices followed by system professionals are unsafe. With the kind of knowledge and experience possessed by the AST, the safe security practices must be above 90%.

The behaviour of the advanced systems users are against the findings of Howe *et al.* (2012), Furnell *et al.* (2007) and Claar (2011) that we discussed in the literature review. All of them argued that users with high security awareness behave securely when it comes to computer security. However, this research shows that there is not any evidence supporting this argument. Ernst and Young (2004) identified security awareness as the most important activity to overcome dangers of information security. However this appears to be not true. These system professionals are very experienced in systems security and know the dangers of following these security practices.

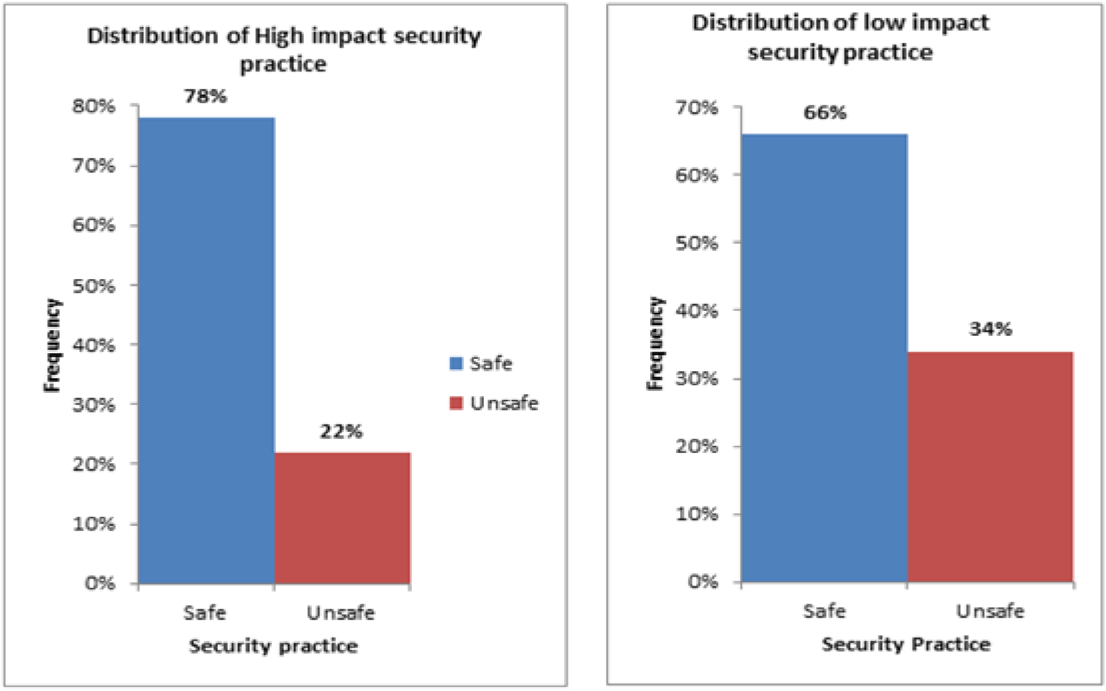


FIGURE 4.4 – Distribution of High and Low impact security practices

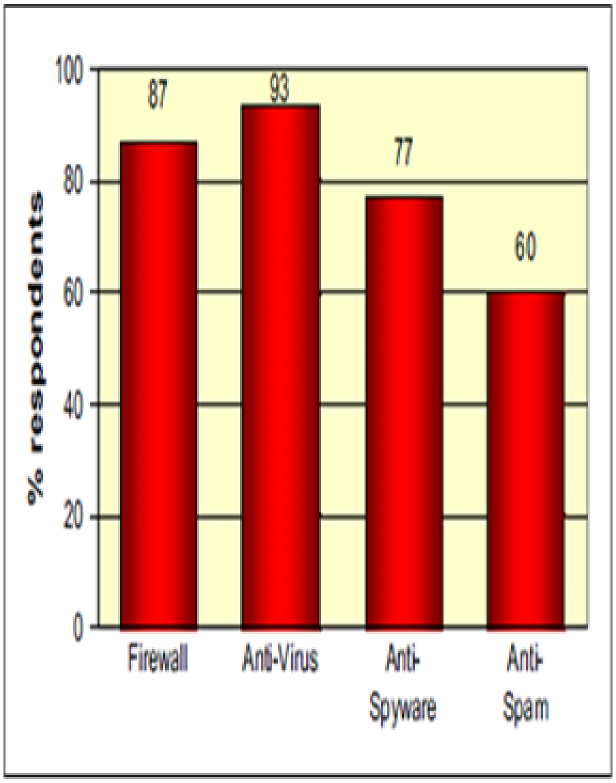
Chi-square test analysis was performed on the data to find out the probability value p to understand the statistical significance. The null hypothesis H0 was that the behavior is independent of security impact. That means there is no significant difference between behavior and security impact and the alternate Hypothesis H1 was that behavior is dependent on the security impact. Based on the analysis of the data given in the Appendix - G; it is found that the p value is 0.002. Since the p value is less than 0.05 the null hypothesis was rejected and the alternate hypothesis was accepted. This implies that based on the statistical evidence the security behavior is dependent on the security impact.

As discussed in the literature review, Larose *et al.* (2008) pointed out that users with increased threat susceptibility install regular operating system and browser updates. However their findings could be accidental because update installation happen automatically in computers. Analyzing our survey results it is found that 93% of respondents use the latest service pack and 89% of them use the auto update feature. Appendix - D shows the graphical representation of these details.

Viruses and spyware cause severe damage to computers around the world. It is estimated that there are more than one hundred thousand viruses and their variants in circulation around the globe. It is estimated that more than ten thousand new viruses are released every month. These are alarming figures. The purpose of each of virus is different. Governmental agencies, spy organisations, countries that are engaged in cyber wars fund their cyber army to release virus and spyware for their purposes. Also organised criminals use spyware to attack their targets and steal information and money from the vulnerable. Anti-virus and anti-spyware play a crucial role in protecting computers. There is large number of anti-virus and anti-spyware software on the market. Some are considered good, some are not. Evaluating anti-virus software is outside the scope of this research. However, what is important in choosing an anti-virus is its ability to automatically download and install updates whenever there is a new ant-virus signature release.

Most anti-virus manufactures enforce this setting in their application. This helps users to update the anti-virus automatically. In the questionnaire respondents were asked to specify how often they perform a full system anti-virus scan. A full system scan is not an enforced setting. The purpose of this question was to know the extra effort that the respondents make to protect their computer. As revealed in the literature review, Howe *et al.* (2012) conducted research to identify the behavior of home computer users and studied the efforts taken by users to avoid security issues. Based on the survey analysis, they found that 92% had anti-virus software, 87% had firewalls and 77% had anti-spyware software. These are great numbers considering the knowledge of home users. Furnell *et al.* (2007) also conducted similar research among 412 home users and received 87%, 93% and 77% for Firewall, Anti-virus and Anti-spyware usage on their home computer. Figure 4.5 taken from Furnell *et al.* (2007) shows the usage of security software by novice home users.

While analyzing the data collected on system professionals' usage of Firewall, Anti-virus and Anti-spyware it was found that all participants use an operating system that comes with a pre-installed firewall, so the firewall usage is analyzed based on the firewall status being disabled or enabled. These results are comparable to the findings of Furnell et al (2007) on his research among home users. Comparing to their research system professionals showed poor security usage habits. Fig 4.6 illustrates the usage of security products by system professionals. Several researchers Claar (2011), Davison and Silence (2010), Phippen *et al.* (2008) recommended security awareness for users to increase their home computer security.



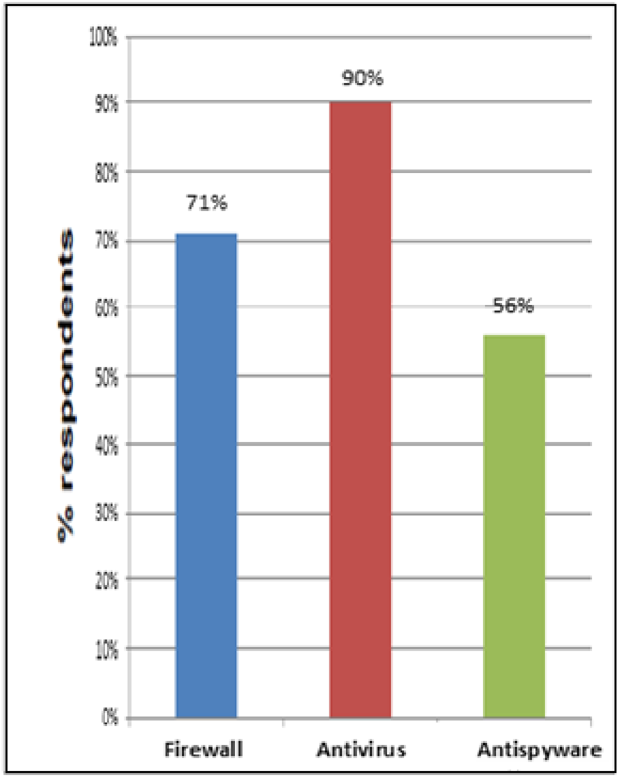


Fig 4.5 Source: Furnell (2007).Usage of security products by home users

Fig 4.6 Usage of security products by systems professionals

In the face-to-face interviews respondents were asked to comment on security software usage and some of those comments are below:

"Most of the time these security software are a nuisance. It impacts the performance of the machine. I lost faith in them as my computer got infected even when I had up-to-date anti-virus. I am capable of addressing it if something goes wrong."

"Even if some security issues happen I am capable of resolving it also the subscription charges for some of these good anti-spywares are high"

Above results showed that awareness may not be the key factor in deciding the usage of security products in home computers. As shown in Table 4.1 the trend that we saw in the face-to-face interview was the respondent’s confidence to fix the issues stopping them from implementing best practices or using security software.

The main purpose of home computers is to check e-mail, browse the internet and shop online. Internet and e-mail have become a part of our daily life. There are hundreds of thousands of e-mails sent and received daily. Of these, a large number of e-mails are malicious and spam. The most common method of virus delivery is through e-mails. Virus infected or virus containing attachments are sent to a large amount of random e-mail accounts and when users download and open these attachments the virus take control of the system and start malicious activity including sending infected e-mails to contacts in the address list. The best and most effective way to minimise the risk of spreading the virus through e-mail is by opening e-mails and attachments from trusted sources by verifying the subject, sender and the attachment of an e-mail. A large number of financial scams and identity theft attempts happen through e-mail. It is important to check for “https” in the address link before clicking on the link. Another best practise in managing online accounts is using unique passwords. As these things are best practices to keep computers safe, questions based on these best practices were asked in the questionnaire.

System professionals who participated in this case study showed a great deal of security conscious behaviour in e-mail and internet usage. Figure 4.7 shows the details of the responses received for the e-mail and online security category. It is found that more than 81% of respondents follow best practices when they check e-mail, open attachments and select web links. However, when they were asked to state if they use the same password for multiple online accounts, the majority of respondents (about 67%) admitted that they do. This indicates high risk behaviour by these professionals. Figure 4.7 shows the consolidated analysis chart.

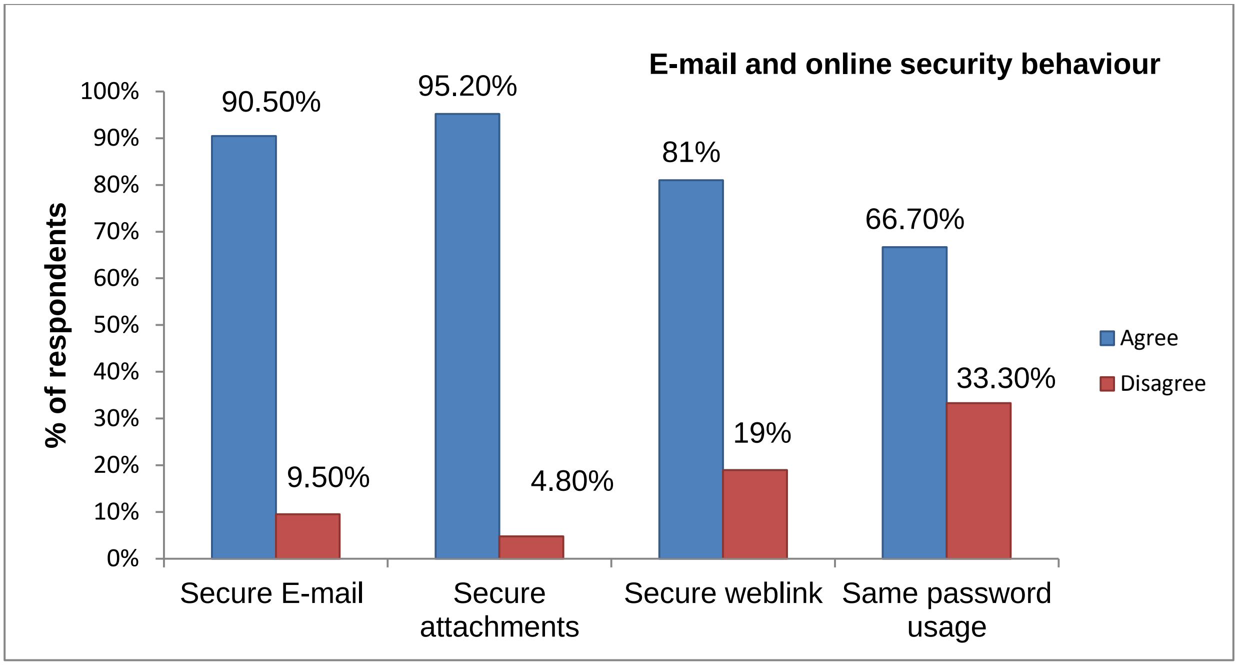


FIGURE 4.7– Analysis of e-mail and online security behaviours

In the semi-structured interviews all participants were asked to comment on why users keep the same password for multiple online accounts. Analysis of the face-to-face interviews are given in the Table 4.1. This shows that the main reason why users use same passwords for multiple accounts is for their convenience. Some of the comments received are given below.

"I have at least 10 online accounts. I use them for e-mails, social media, online gaming, and shopping accounts. It is impossible to remember passwords if I use separate passwords for all accounts."

This indicates that even though users are aware of the reasons why they should use separate passwords for their online accounts they give importance to convenience. As detailed in the literature review, Campbell *et al.* (2011), Ives *et al.* (2004) also pointed out this behaviour in their research. Tam *et al.* (2010) studied the psychology of password management and his findings were in line with the responses that were received in the interview. While concluding their research Tam *et al.* (2010) stated that it is very complex to explain the motivation behind the selection and management of passwords and users sacrifice security for convenience. They found that users go with convenience when it comes to security. They also found that users use strong passwords only if they are willing to give-up convenience. In this research when participants were asked if they use strong passwords on their home computer, 74% answered “Yes” and for the questions 'how often do you change the home computer password?' - 69% answered they never changed the password. This is in line with the findings of Tam *et al.* (2010) that was detailed in the literature review.

It appears that user’s knowledge and experience doesn’t have a large effect on their behaviour. The analysis shows that e-mail and online behaviours of knowledgeable professionals is on par with that of novice internet users.

Firewalls play a vital role in protecting a computer and networks. Firewalls are designed to protect computers by blocking or allowing internal traffic based on set of access rules. Nowadays operating system manufactures deliver their systems with built-in firewalls. Survey questions in this category are aimed at finding out if advanced users disable their built-in firewall that comes with the operating system. From the survey results it is found that 93% of system professionals use an operating system that comes with a built-in firewall. However only 71% of them stated that a firewall is enabled and active on their computer, 26% admitted that the firewall status is “disabled and inactive” and 3% answered unknown. This indicates that even though the firewalls are active and enabled by default, system professionals purposefully disabled them. In the face-to-face interview users we requested to comment on this behaviour and the summary is given in Table 4.1. Some of the comments received in face-to-face interviews regarding firewall usage are as follows.

> *“I have a small home network where I connect our home computers together. Having to turn-on the firewall causes access problems between them. So I disable it. I am confident that if something goes wrong I would be able to fix it. “*

> *“Built-in firewall that comes with the operating system causes access issues and people tend to disable it. Configuring separate rules takes more time.”*

As stated in the literature review, a strong password is one of the most important first steps to securing the computer from security threats. Passwords are the first line of defence. Not having a password is like keeping your front door open which invites burglars. Having a strong password to log in to a computer is a basic requirement. Operating system makers are forcing computer users to use a password to log-in to their computer. But often times users ignore them and continue the unsafe practice. By exploiting this hackers would be able to take control of the computer and use it as a host to spread their illegal activity. However it is recommended to use strong passwords whenever creating a password. According to Microsoft a strong password must contains at least eight characters including a combination of uppercase/lower case and alpha numeric characters.

Even though a good number of respondents (90%) admitted of using a password to login to their home computer; the graph shown in Appendix H; the password changing behaviour showed poor results. The trend that we saw in the password changing habit is below standard. Only 15% of respondents changed their passwords at least every year. 69% answered that they never changed the password of their home computer. A detailed response received for the password changing behaviour is given in Figure 4.8. In the previous section it was found that these respondents have a habit of using the same password for multiple accounts. When we interpret both these findings it reveals an unhealthy behaviour. Using similar passwords in multiple accounts and not changing them is a serious security loop hole.

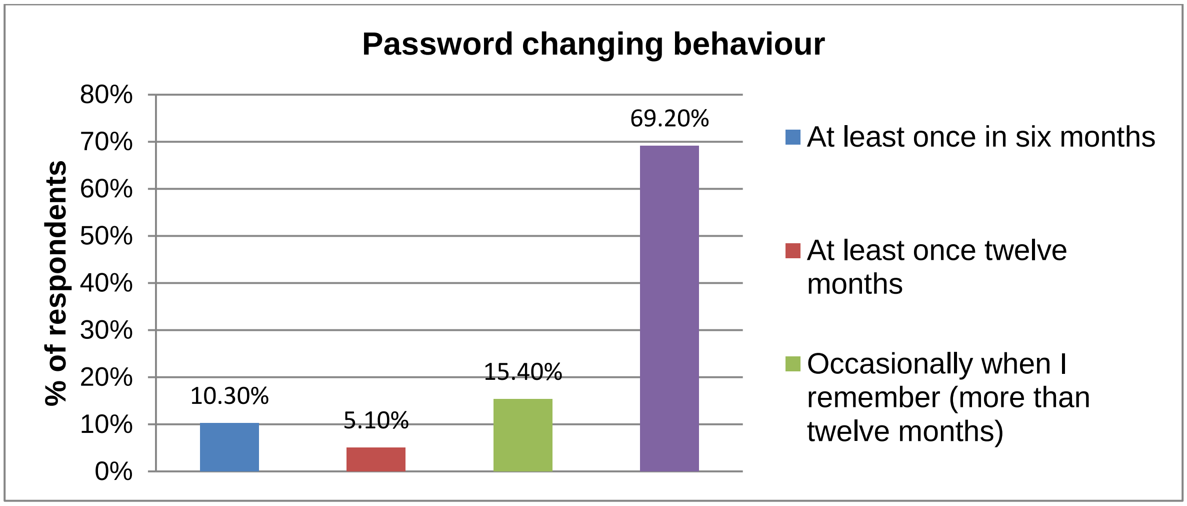
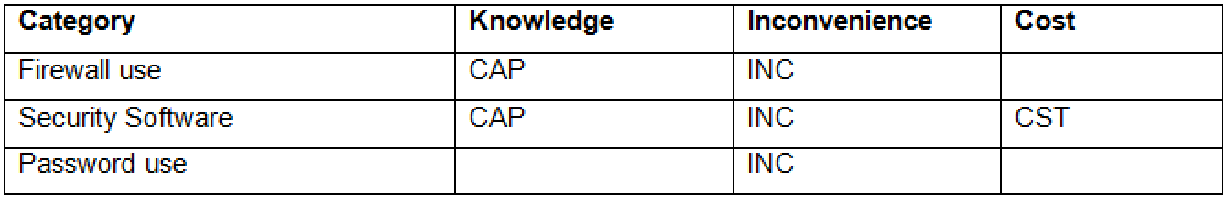


FIGURE 4.8 – Password changing behaviour

From all these different analyses it is found that knowledgeable users did not show high quality security behaviour in their home computers. In some of the categories they showed more vulnerable behaviours than novice home users.

To understand the reason for different behaviours, face-to-face interviews were conducted among randomly selected respondents. The responses were analysed and categories were created based on the theme of their responses and codes were applied on their responses. Table 4.1 summarises the reasons why system professionals show poor results.

TABLE 4.1: Summary of Face to face interview



Category	Knowledge	Inconvenience	Cost
Firewall use	CAP	INC	
Security Software	CAP	INC	CST
Password use		INC	

(CAP=Capable of Resolving the issue, INC=Inconvenience, CST=Cost)

Appendix E shows the details of the responses. As pointed out in the literature review, West (2008) stated that the cost of implementing the security can come in the way of security as users won't be willing to pay much money as subscription. Aytes (2004) also supported this argument. This also came up in the face-to-face interview. One of the comments that was received in the face-to-face interview was of special interest.

> *"Most of the time the security software's are a nuisance. It impacts the performance of the machine. I lost faith in them as my computer got infected even when I had an up-to-date antivirus. I am capable of addressing it if something goes wrong"*

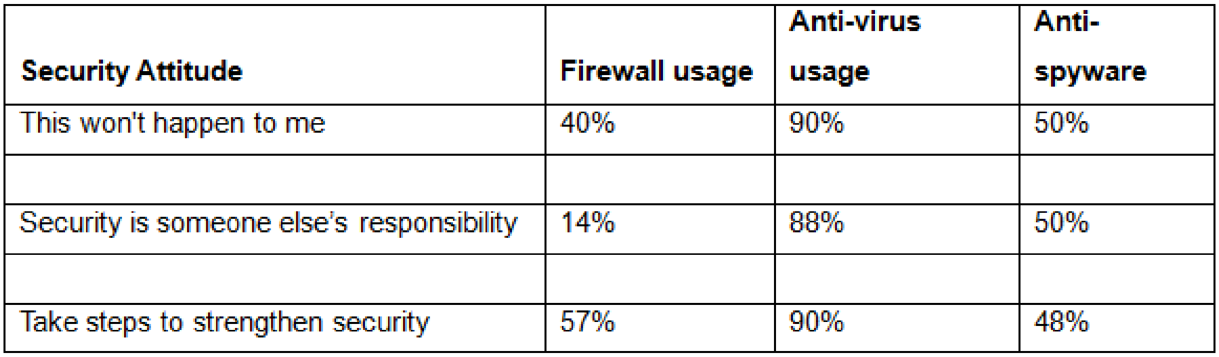
This sums it all. Knowledge gives advanced users the extra confidence to deal with the security situation. This also makes them irresponsible and hence ignores security best practises.

4.5 Security Attitude and Security Behaviour

The purpose of this section is to analyse the research question: “How does the attitude towards security influence the security practices of system professionals' home computers?” Analysis of the data showed clear evidence for the lack of attitude towards security incidents. However there isn’t any evidence that supports the hypothesis that the security practices are dependent on the attitude towards security.

West (2008) pointed out that users possess a “this won’t happen to me” attitude when it comes to security and this attitude can influence their choice, selection and practice when it comes to security. Lack of awareness towards security is quite evident in the survey analysis. While analysing the survey results 25% of the respondents have a “this won’t happen to me” attitude, 21% of the respondents answered that they think “security is someone else’s responsibility” and 54% responded that they take steps to strengthen security. Table 4.2 shows the security product usage of system professionals based on their security attitudes. It appears that there isn’t any significant change in the security product usage behaviour with attitude.

TABLE 4.2 – Usage of security products based on attitude.



Security Attitude	**Firewall usage**	**Anti-virus usage**	**Anti-spyware**
This won't happen to me	40%	90%	50%
Security is someone else's responsibility	14%	88%	50%
Take steps to strengthen security	57%	90%	48%

However there is significant difference in the firewall usage. In spite of all system professionals using an operating system that comes with a pre-installed firewall a lot of them have disabled the firewall. The suggestion made by Phippen *et al.* (2008 and Furnell *et al.* (2007) are very relevant here. They suggested security policy enforcement on home computers before they are granted internet access. If a computer is without a firewall or latest security updates those systems should not be given access to the internet. The practicality of implementing such functionality should be discussed as it may not be easy to implement such monitoring for 2 billion home users.

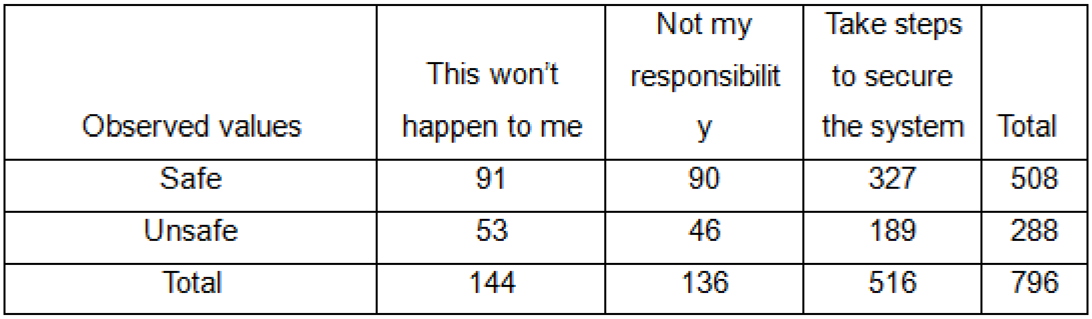
To test the validity of the hypothesis that the security behaviour is dependent on the attitude towards security, a Chi-square test was carried out on the frequency of responses. Two hypotheses are developed for this test.

Null hypothesis H0 – Security behaviour is independent of the attitude towards security.

Alternate hypothesis H1 – Security behaviour is dependent on the attitude towards security.

Below table shows the observed values used in the Chi-square test.

TABLE 4.3 – Observed frequency of security attitude vs. behavior



Observed values	This won't happen to me	Not my responsibility	Take steps to secure the system	Total
Safe	91	90	327	508
Unsafe	53	46	189	288
Total	144	136	516	796

Using the Chi-square functions in Excel 2010, we found that Chi-square (X^2) = 0.4 with a degree of freedom of 2. The corresponding probability value was *p* = 0.82. Since the p value is greater than 0.05 the test accepts the null hypothesis H0. This indicates that the security behaviour and attitude are independent of each other.

In the literature review it was pointed out that the use of fear appeal and persuasive messages can have an impact on user's behaviours. A number of researchers supported this argument. Research conducted by Siponen (2000), Witte (1992), Johnston (2010), Allan (2000) all supported this argument. Operating system manufactures have implemented "System at Risk" warnings when it detects the absence of anti-virus software or firewalls. However these may not have any effect on the users who have a different attitude towards security. This research shows that security attitudes and behaviours are two independent variables.

4.6 Manufacturer Enforced Security Settings

Operating system makers have been enforcing security settings to ensure continuous security by implementing automatic updates, scheduled virus scans and firewalls. The empirical survey queried the status of these settings and found that almost all respondents use the benefit of automatic updates and most of them have the latest service pack in their home computer. This is a great trend.

As we have seen in the literature review, the purpose of automatic updates is to resolve issues whenever security issues are identified in an operating system otherwise these systems will remain vulnerable (Luettmann and Bender 2007). To address this, operating system manufacturers release security updates and service packs. Service packs are a consolidated package that contains OS improvements and fixes that were released since the last service pack. However, non-technical users did not bother to check for updates and this made their computers vulnerable. To address this, operating system manufactures have introduced automatic updates. How this works is that, on a specified day computers connect to the remote patch download servers and perform a silent installation of these patches without disturbing the end user.

All professionals who participated in this survey showed great responsibility in updating their home computers. 97% of respondents answered that they use the latest service pack in their computer. This is a large percentage. Also for 95% of respondents run update installations at least once a month. This is a great number. It shows the effectiveness of manufacture enforced security. Also 97% of the respondents use anti-virus auto update features. These manufacture enforced auto update features help home users to keep their computer up-to-date and unlike the firewall setting this setting remains intact on a home computer. However when it comes to firewall status, the results weren’t promising. Even though 97% of users admitted to using a system that comes by default with a firewall, only 71% of them were keeping it enabled and active. This is a low number compared with the 97% that manufacturers had enabled.

For people with good computer security knowledge one would expect it to be as high as 100%. The reasons for this behaviour were discussed in the face-to face interview and found out that, users with knowledge on how to change settings do so for convenience. Especially, when certain firewall features function with their way of doing things. As seen in the literature review suggested by Furnell *et al.* (2008) self-auditing security implementations can be useful in these scenarios allowing/denying access based on the set of rules.

One of the worrying trends that is observed in these surveys is that if a particular security setting is enforced users tend to continue to use it, however the percentage of people who proactively do things to ensure safety are decreasing. For example for question 14, users were asked “How often you perform Full system scan?”. By default anti-virus developers schedule a quick scan which is effectively a partial scan of your computer. To ensure the computer is without any malicious software it is advised to perform frequent full system anti-virus scans. From the survey results only 33% of system professional surveyed proactively perform a full system anti-virus scan. While 38% of respondents claimed that they perform a “Full system” anti-virus scan “Occasionally (When they remember)” and 19% mentioned that they “Never performed” a full system anti-virus scan. To make sure users follow security best practices it is better to enforce them.

As part of the data analysis process an attempt was made to compare and understand the proactive nature of the system professionals' behaviour to see if enforcing the settings are important or not. Most of the proactive practices like, Full system anti-virus scan, password change, and computer backup were not performed frequently. The trend that showed in the analysis was disappointing.

Computers are more reliable than ever. This makes people not do backups. Backups help us to restore our data in case of a data loss. Backups are more important than ever as we can lose data because of hard drive failure, theft, accidental deletion and viruses that delete data. If a computer is infected with a virus most of the time people would be advised to format their hard drive and start from scratch. As seen in the literature review, it is a best practice to make frequent data backups of computers. The trend that is shown in the analysis is that respondents are not so keen to take the backup of their computer.

From the analysis of backup behaviour it is found that only 40% of respondents make backups of their computers every six months. It is shocking to know that 29% of advanced system users do not make any sort of backup to protect their data from hardware or software malfunction. If we add the occasional (more than twelve months) backup takers to the "never take backup" group it become 55%. This is another example that if best practices are not enforced users may not always follow it.

5 Conclusions and Future Work

5.1 Introduction

The purpose of this chapter is to discuss the conclusions of the findings of this case study research to answer the research question. This chapter also contains important observations and future research sections.

5.2 Conclusions

The purpose of this research is to study the security behaviors of system professionals on their home computer. There are three research questions that were used help find out the behavior. Those were: **“**How do the security behaviours of system professional’s differ from novice home computer users?”, “How does the attitude towards security influence the security practices of system professionals in home computer?”, “How do system professionals respond to manufacture enforced security settings in home computers?”.

5.2.1 How do the security behaviours of system professionals differ from novice home computer users?

Based on the empirical research it is found that there isn’t much difference between the behaviors of system professionals and home users. Analyzing the data showed that almost all of the respondents use a system that comes with built-in firewall however only 71% them keep it enabled, 90% of them use a firewall and 56% use a firewall in their computer. The respondents know the importance of the firewall and the necessity to keep it enabled. This is against the common belief that knowledgeable users behave more securely when it comes to security. However there is also an equal chance that knowledgeable users could change security settings the way they want.

In the course of the research some respondents were interviewed to identify the cause of the behavior and it was revealed that the knowledgeable users follow unsafe practices because of convenience and they have an attitude that if something goes wrong they will be able to fix it.

Using the frequency analysis on the distribution of responses it is found that 72% of participants fall in under safe behavior and 28% of them fall under the unsafe category. To test the relationship between the security behavior and severity of security practice, a Chi-square test was applied on the response counts and found that the security behavior of system professional depends on the security impact of the practice. Frequency analysis showed that 78% behave securely on High Impact practices and 66% behave securely on Low Impact practices. This is an expected behavior. This guarantees that when a particular practice can have high impact on the security, knowledgeable users tend to follow that.

5.2.2 How does the attitude towards security influence the security practices of system professionals in home computer?

The purpose of this research question is to find out if the attitude of advanced users influences their security practice. Based on the empirical research it is found that there is no direct influence of attitude and safe or unsafe behaviour. The research showed that users exhibit mainly three kinds of attitude towards security and those are this won’t happen to me, Security is someone else’s responsibility and Take steps to strengthen the security. Using statistical analysis on the frequency of responses isn’t any visible influence of attitude against the behaviour.

5.2.3 How do system professionals respond to manufacture enforced security settings in home computers?

Analyses of the research data showed that manufacturer enforced settings are an effective way of implementing security. However, when it comes to firewall settings it doesn’t seem to be very effective. As identified in the findings, the participants tend to disable settings based on their convenience. Whenever they find firewalls are blocking something that is against their will, instead of creating separate firewall rules, they tend to disable them altogether and eliminate the purpose of using a firewall.

5.3 Additional Observations of Interest

An interesting concept that came out of this research is about "self-auditing security implementations". This is an exciting concept that could improve the overall security of the internet. Before giving access to the internet, every computer should be automatically checked for the status of firewall, antivirus and auto updates. If there is an inconsistency in the status of these components the system should automatically deny access to the wireless or network. Enterprises use a similar concept to ensure the security of their computer networks. What is important in implementing such a feature in home computers is that users should not be given the option to enable or disable such a setting. If they are given the opportunity for this; as seen in the firewall status analysis knowledgeable users would stop it or re-configure it for their convenience.

5.4 Opportunities for Further Research

This study is based on convenience sampling as it is practically challenging to include the entire system professionals' community for the study. The scope of this study is members in an Advanced Support Team in a multinational. The main drawback of the convenience sampling is the lack of generalizability.

To have a deeper understanding of the security behavior the scope of the research could be expanded to system professional in multiple organisations using a multiple case study strategy. Moreover, there isn't any other study conducted on the security practices of advanced system users. This research can be used as a reference point for future research.

References

Ajzen, I., (1991) ‘The Theory of Planned Behavior’. *Organizational Behavior and Human Decision Processes*. 50:179-211.

Anderson, C. L. and Agarwal, R., (2008) ‘Practicing Safe Computing: A Multi-Method Empirical Examination of Home Computer User Security Intentions’. *MIS Quarterly*, 20(2): 65-173.

Aytes, K. and Connolly, T. (2004) ‘Computer security and risky computing practices: A rational choice perspective’. *Journal of Organizational and End User Computing*, 16(3): 22-40.

Benbasat, I. Goldstein, D. K. and Mead, M. (1987) ‘The case research strategy in studies of information systems’. *MIS quarterly*, 369-386.

Blaikie, N. (2009) ‘*Designing social research’*. Cambridge: Polity.

Blumberg, B. Cooper, D. R. and Schindler, P. S. (2005) ‘*Business Research Methods’*. Berkshire: McGraw-Hill Education.

Bryman, A. (2012). *Social research methods*. Oxford: Oxford university press.

Buchanan, T. Paine, C. Joinson, A. N. and Reips, U. D. (2007) ‘Development of measures of online privacy concern and protection for use on the Internet’. *Journal of the American Society for Information Science and Technology*, 58(2): 157-165.

Bulgurcu, B. Cavusoglu, H. and Benbasat, I. (2010) ‘Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness’. *MIS quarterly*, 34(3): 523-548.

Campbell, D. T. and Fiske, D. W. (1959) ‘Convergent and discriminant validation by the multitrait-multimethod matrix’. *Psychological bulletin*, 56(2): 81.

Campbell, J. Ma, W. and Kleeman, D. (2011) 'Impact of restrictive composition policy on user password choices'. *Behaviour & Information Technology*, 30(3): 379-388.

Claar, C. L. (2011) *The Adoption of Computer Security: An Analysis of Home Personal Computer User Behavior Using the Health Belief Model.* Unpublished Doctoral dissertation, Utah State University.

Cline, J. (2008) Opinion: 8 Growing Risks of Employee Home Offices. Available at: http://www.computerworld.com/s/article/9060280/Opinion_8_Growing_Risks_of_Employee_Home_Offices (Accessed 15 June 2013)

Cobanoglu, C. Warde, B. and Moreo, P. J. (2001) 'A comparison of mail, fax and web-based survey methods'. *International journal of market research*, 43(4): 441-452.

Computerweekly (2009). Millions of web users at risk from weak passwords. Available at : http://www.computerweekly.com/news/1280096996/Millions-of-web-users-at-risk-from-weak-passwords (accessed on 15 March 2013).

Culnan, M. J. Foxman, E. R. and Ray, A. W. (2008) 'Why IT Executives Should Help Employees Secure Their Home Computers'. *MIS Quarterly Executive*, 7(1): 49-56.

D'Arcy, J. Hovav, A. and Galletta, D. 2009 "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research,* 20(1): 79-98.

Davinson, N. and Sillence, E. (2010) 'It won't happen to me: Promoting secure behaviour among internet users'. *Computers in Human Behavior*, 26(6): 1739-1747.

Davis, G (2012) 2012 Online Safety Survey – Majority Of Americans Do Not Feel Completely Safe Online. Available at http://blogs.mcafee.com/consumer/online-safety-survey2012 (Accessed 7 June 2013).

Dobson, P. (2002) Critical realism and information systems research: why bother with philosophy? Available at http://informationr.net/ir/7-2/paper124.html. (Accessed 27 May 2008).

Earnest and Young (2004). Information Survey 2004. Available at http://www.issa-motorcity.org/files/GlobalInformationSecuritySurvey2004.pdf (Accessed 16 February 2013).

Frank, R. 2008 "Managing intellectual property". Journal of Accountancy 206 (2): 37.

Furnell, S. M. Bryant, P. and Phippen, A. D. (2007) 'Assessing the security perceptions of personal Internet users'. *Computers & Security*, 26(5): 410-417.

Furnell, S. Valleria T. and Phippen, D. (2008) 'Security beliefs and barriers for novice Internet users'. *Computers & Security*, 27(7): 235-240.

Gill, J. and Johnson, P. (2002) '*Research methods for managers'*. London: Sage.

Guba, E. (1990) '*The Paradigm Dialog'*. London: Sage

Howe, A. E. Ray, I. Roberts, M. Urbanska, M. and Byrne, Z. (2012) 'The psychology of security for the home computer user'. Security and Privacy (SP): 2012 IEEE Symposium, pp. 209-223.

Hussein, A. (2009) 'The use of Triangulation in Social Sciences Research: Can qualitative and quantitative methods be combined'. *Journal of Comparative Social Work*, 1: 1-12.

International Organisation for Standardisation (2005) ISO 17799:2005 Coverage of Information Security Awareness Available at:
http://iso-17799.safemode.org/index.php?page=ISO_17799_and_information_security_awareness
(Accessed 17 June 2013)

International telecommunication union, (2012) Key statistical highlights: ITU data release June 2012 Available at:

http://www.itu.int/ITU-D/ict/statistics/material/pdf/2011%20Statistical%20highlights_June_2012.pdf (Accessed 19 January 2012)

Ives, B. Walsh, K.R. and Schneider, H. (2004) ‘The domino effect of password reuse’. *Communications of the ACM*, 47 (4): 75–78.

Johnson-Laird, P. N. Girotto, V. and Legrenzi, P. (1998) ‘Mental models: a gentle guide for outsiders’. *Sistemi Intelligenti*, 9(68): 33.

Johnston, A. C. and Warkentin, M. (2010) ‘Fear appeals and information security behaviors: an empirical study’. *MIS Quarterly*, 34(3): 549.

Klenke, K. (2008) *Qualitative research in the study of leadership*. Bradford: Emerald Group Publishing

Kuhn, T. (2010) The Scientific Revolution. Philosophy of Science for Nursing Practice: Concepts and Application, 87.

Kumar, N. Mohan, K. and Holowczak. R. (2008) ‘Locking the door but leaving the computer vulnerable: Factors inhibiting home users’ adoption of software firewalls’. *Decision Support System,* 46(1): 254-264.

LaRose, R. Rifon, N. J. and Enbody, R. (2008) ‘Promoting personal responsibility for internet safety’. *Communications of the ACM*, 51(3): 71-76.

Liang, H. and Xue, Y. (2009) ‘Avoidance of Information Technology Threats: A Theoretical Perspective’. *MIS Quarterly*, 33(1): 71-90.

Luettmann, B. M., & Bender, A. C. (2007) ‘Man-in-the-middle attacks on auto-updating software’. *Bell Labs Technical Journal*, *12*(3): 131-138.

MacGibbon, A. and Phair, N. (2011) Password Security: A survey of Australian attitudes toward password use and management. Available at: https://www.paypal-media.com/assets/pdf/fact_sheet/cis_paypal_whitepaper_final.pdf (Accessed 06 July 2013).

Mejias, R. J (2012) ‘An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk’. *45th Hawaii International Conference on System Science.* Hawaii, USA, 4-7 January 2012. Hawaii: IEEE Xplore pp. 3258-3267.

Microsoft (2011) Windows XP Service Pack 2 (Part 5): Virus protection. Available at: http://support.microsoft.com/kb/889739. (Accessed on 15July 2013).

Microsoft Security Intelligence Report (2013). Operating system statistics. Available at http://www.microsoft.com/security/sir/story/default.aspx#!why_upgrade (Accessed 17 June 2013).

National Cyber Security Alliance (2013). 10 Ways to protect your privacy and identity on a windows computer. Available at: http://www.staysafeonline.org/blog/10-ways-to-protect-your-privacy-and-identity-on-a-windows-computer. (Accessed 10 June 2013)

Market Share Statistics for Internet Technologies (2013). Market share reports. Available at: http://www.netmarketshare.com (Accessed 15 July 2013).

Ng, B. Y and Rahim, M. A (2005) ‘A Socio-Behavioral Study of Home Computer Users Intention to Practice Security’, *9th Pacific Asia Conference on Information Systems.* Bangkok, Thailand, July 2005.

Olsen, W. (2004) ‘Triangulation in social research: qualitative and quantitative methods can really be mixed’. *Developments in sociology*, 20:103-118.

Polkinghorne, D. E. (1995) ‘Narrative configuration in qualitative analysis’. *International journal of qualitative studies in education*, 8(1): 5-23.

Robson, C. (2002) *Real world research: A resource for social scientists and practitioner-researchers.* Edition 2. Oxford: Blackwell.

Rogers, R. W. (1975) ‘A Protection Motivation Theory of Fear Appeals and Attitude Change’. *The Journal of Psychology*, 91(1): 93-114.

Roskos-Ewoldsen, D. R. Jessy, H. Y. and Rhodes, N. (2004) ‘Fear appeal messages affect accessibility of attitudes toward the threat and adaptive behaviors’. *Communication Monographs*, 71(1): 49-69.

Saunders, M. N. Lewis, P. and Thornhill, A. (2009) *Research methods for business students*. London: Pearson.

Scott, C. (2012) Nearly a Fifth of U.S. PCs Have No Virus Protection, Mcafee Finds. Available http://www.cio.com/article/707238/Nearly_a_Fifth_of_U.S._PCs_Have_No_Virus_Protection_Mcafee_Finds (Accessed 5 May 2013).

Siponen, M. T. (2000) ‘A conceptual foundation for organizational information security awareness’. *Information Management & Computer Security*, 8(1): 31-41.

Sriramachandramurthy, R. Balasubramanian, S. K. and Hodis, M. A. (2009) ‘Spyware and adware: how do internet users defend themselves?’. *American Journal of Business*, 24(2):41-52.

Tam, L. Glassman, M. and Vandenwauver, M. (2010) ‘The psychology of password management: a tradeoff between security and convenience’. *Behaviour & Information Technology*, *29*(3): 233-244.

Tashakkori, A. and Teddlie, C. (1998) *Mixed Methodology: Combining Qualitative and Quantitative Approaches*. Thousand Oaks, CA: Sage Publications.

Teddlie, C. and Tashakkori, A. (2009) *Foundations of Mixed Methods Research.* Thousand Oaks, CA: Sage Publications.

Temple, K. (2012) What Happens in an Internet Minute? Available at: http://scoop.intel.com/what-happens-in-an-internet-minute (Access 8 July 2013)

Trochim, W. M. K. (2006) Ethics in Research: The Research Methods Knowledge Base, Third Edition. The Web center for social research methods, Available at: http://www.socialresearchmethods.net/kb/ethics.php (Accessed on 17 March 2013).

Tsohou, A. Kokolakis, S. Karyda, M. and Kiountouzis, E. (2008) 'Investigating information security awareness: research and practice gap'. *Information Security Journal: A Global Perspective*, 17(5-6): 207-227.

Tuli, F. (2011) 'The Basis of Distinction Between Qualitative and Quantitative Research in Social Science: Reflection on Ontological, Epistemological and Methodological Perspectives'. *Ethiopian Journal of Education and Sciences,* 6(1): 97-108.

United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime, Available at: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (Accessed 17 June 2013).

US-CERT (2013) Security tip ST04-010. Using Caution with Email Attachments. Available at: https://www.us-cert.gov/ncas/tips/ST04-010 (Accessed 02 July 2013).

US-CERT (2013) Security tip ST04-002. Choosing and protecting passwords. Available at: http://www.us-cert.gov/ncas/tips/ST04-002 (Accessed 06 July 2013).

Venkatesh, V. Brown, S. A. and Bala, H. (2013) 'Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems'. *MIS Quarterly*, *37*(1): 21-54.

Warkentin, M. and Willison, R. (2009) ‘Behavioral and policy issues in information systems security: the insider threat’. *European Journal of Information Systems*, 18(2):101.

Wash, R. (2010) "Folk models of home computer security. In Proceedings of the Sixth Symposium on Usable Privacy and Security" ACM, 11.

West, R. (2008) ‘The psychology of security’. *Communications of the ACM,* 51(4): 34-40.

Witte, K. (1992) ‘Putting the fear back into fear appeals: The extended parallel process model’. *Communications Monographs*, *59*(4): 329-349.

Witte, K. and Allen, M. (2000) ‘A meta-analysis of fear appeals: Implications for effective public health campaigns’. *Health Education & Behavior*, *27*(5): 591-615.

Wynn, D. and Williams, C. K. (2012) ‘Principles for Conducting Critical Realist Case Study Research in Information Systems’. *Management Information Systems Quarterly,* 36(3): 787-810.

Xue, Y. and Liang, H. (2009) ‘Avoidance of Information Technology: A Theoretical Perspective’. *MIS Quarterly,* 33(1): 71-90.

Yeasmin, S. and Rahman, K. F. (2012) “Triangulation' Research Method as the Tool of Social Science Research’. *BUP Journal*, 1(1): 154-163.

Yin, R. K. (Ed.). (2003) "Case study research: Design and methods" London: Sage.

Zhang, J. Luo, X. Akkaladevi, S. and Ziegelmayer, J. (2009) ‘Improving multiple-password recall: an empirical study’. *European Journal of Information Systems*, 18(2): 65-176.

Appendix

Appendix – A: Survey Questionnaire:

Q1. Do you accept the above declaration and agree to participate in this survey?

Answer Options

- Yes
- No (The survey Exist)

Q2. Please indicate the degree to which you agree or disagree the following statement. When I hear/read security incidents like credit card fraud or online financial scam, -------

Answer Options

- I think this won't happen to me.
- I think online security is someone else's responsibility.
- I take steps to strengthen the security.
- Other (please specify)

Q3. Before opening an email, I will check if the subject and the sender make sense

Answer Options

- Agree
- Disagree

Q4. Before opening an email attachment, I will check if the filename of the attachment makes sense

Answer Options

- Agree
- Disagree

Q5. If I receive an e-mail that appear to be from a financial institution, I check if the web link in the e-mail contains "https:\\" before I click on the link in the e-mail?

Answer Options

- Agree
- Disagree

Q6. Do you use same password for multiple online accounts?

Answer Options

- Yes
- No

Q7. Do you use the latest service pack on your Home computer?

Answer Options

- Yes
- No
- Don't Know

Q8. How often do you run Operating system Update?

Answer Options

- Update is set to run automatically.
- At least once a month
- At least once in six months
- Occasionally, when I remember
- Never run update
- Other (please specify)

Q9. Do you check/monitor the status (success/failure) of the Operating System updates?

Answer Options

- Yes
- No

Q10. Do you use an operating system that comes with built in firewall?

Answer Options

- Yes
- No
- Don't know

Q11. What is the status of the firewall on your computer?

Answer Options

- It is disabled and inactive.
- It is enabled and active.
- Don’t know /Not Applicable

Q12. Do you have anti-virus software installed on your computer?

Answer Options

- Yes
- No
- Comments

Q13. How often do you update your anti-virus software?

Answer Options

- Update is set to run automatically.
- At least once a month
- At least once in six months
- Occasionally, when I remember
- Never
- Comments

Q14. How often do you perform a full system anti-virus scan?

Answer Options

- At least once a week
- At least once a month
- Occasionally when I remember
- Never
- Other (please specify)

Q15. Do you have anti-spyware software installed on your computer?

Answer Options

- Yes
- No
- Comments

Q16. Do you use a password to login to your home computer?

Answer Options

- Yes
- No

Q17. How often you change the login password on your computer?

Answer Options

- At least once in six months
- At least once twelve months
- Occasionally when I remember (more than twelve months)
- Never changed the password
- Other (please specify)

Q18. Do you use a strong password (at least eight characters including a combination of uppercase/lower case of alpha numeric character) in your home computer?

Answer Options

- Yes
- No
- Comments

Q19. How often do you take backup of your personal data in your home computer?

Answer Options

- At least once in six months
- At least once twelve months
- Occasionally when I remember (more than twelve months)
- Never take the backup
- Comments

Q20. Please indicate the degree to which you agree or disagree the following statement "I think my home computer is safe"

Answer Options

- Strongly Agree

- Agree
- Disagree
- Strongly Disagree

Q21. Which department do you work?

Answer Options

- Technical support
- Human Resource
- Sales
- Marketing
- Comments

Q22. How long have you been working with the current employer?

Response

Q23. How many years' experience do you have in IT profession?

Response

Q24. Please select the IT certification/s that you possess

Answer Options

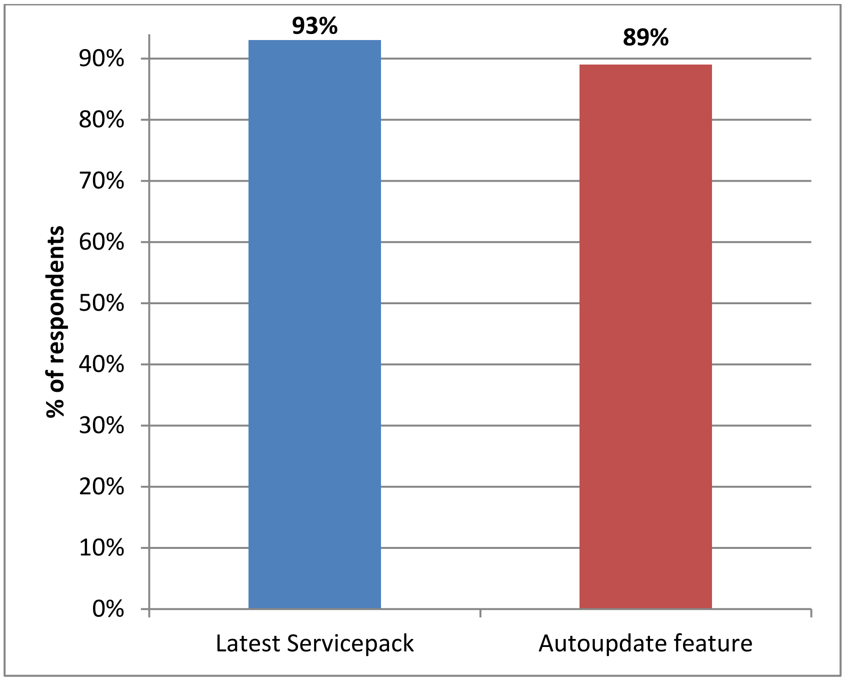
- MCP/MCITP/MCSA/MCSE (Microsoft certifications)
- "VCP/ VCAP/VCDX (VMware Certifications)"
- "RHCSA/RHCE/LPIC (Linux Certification)"
- "CCNA/CCNP/CCIE (CISCO Certification)"
- Comments

Appendix –C: High Impact (risk) and Low Impact (risk) categories

- High Impact: Q3, Q4, Q5, Q6, Q11, Q12, Q16, Q18

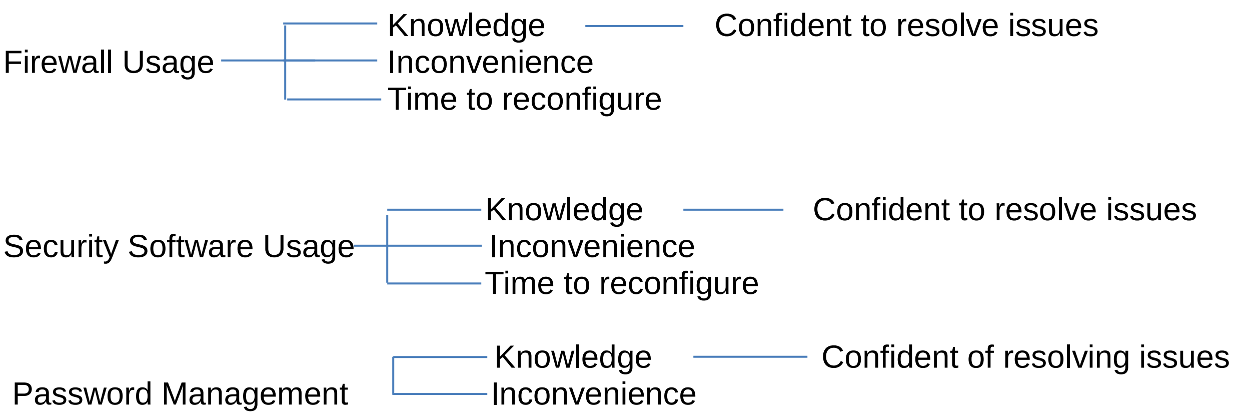
- Low Impact: Q7, Q8, Q9, Q10, Q14, Q15, Q17, Q19

Appendix D: Auto-update Vs. Service pack usage



% of system professionals who use latest service pack and auto update

Appendix E: Analysis of Face to face interview.



Appendix: F: Chi-square analysis of Attitude v/s security behaviour.

The formula for Chi-Square is:

X^2 = Sum ((observed - expected)^2 / expected)

Observed values	This won't happen to me	Not my responsibility	Secure things	Total
Safe	91	90	327	508
Unsafe	53	46	189	288
Total	144	136	516	796

Expected value	This won't happen to me	Not my responsibility	Secure things	Total
Safe	92	87	329	508
Unsafe	52	49	187	288
Total	144	136	516	796

Chi-square (X^2) = 0.4
Degree of freedom = 2
Probability *p*= 0.820

Appendix: G: Chi-square analysis of High/Low impact vs. Behaviour

The formula for Chi-Square is:

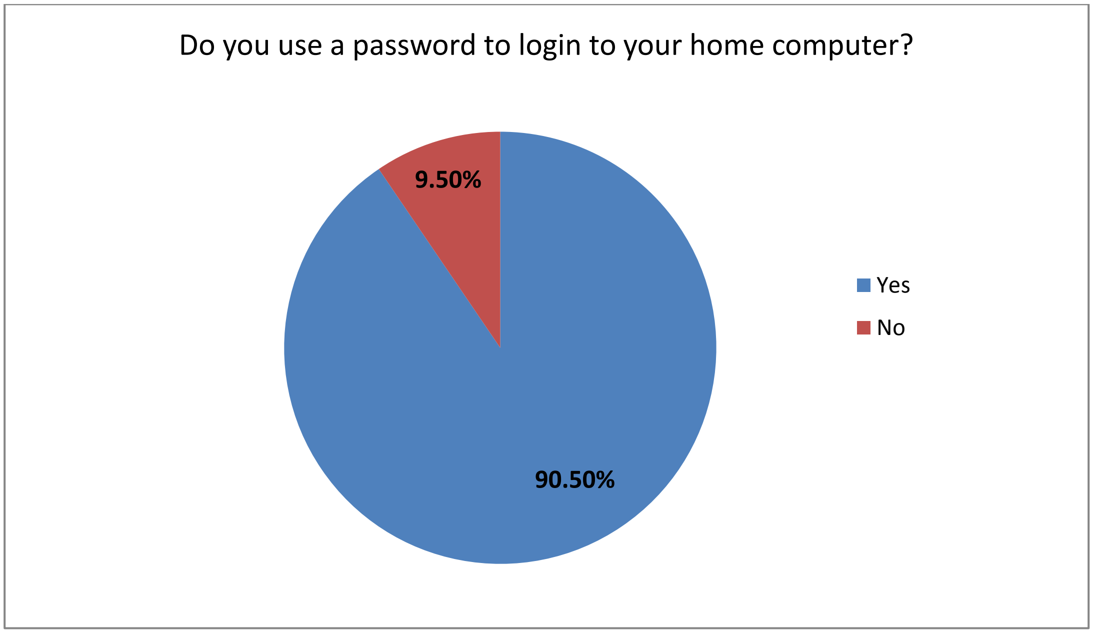
X^2 = Sum ((observed - expected)^2 / expected)

Observed	safe	Unsafe	Total
High Impact	255	71	326
Low Impact	248	118	366
Total	503	189	692

Expected	safe	Unsafe	Total
High Impact	237	89	326
Low Impact	266	100	366
Total	503	189	692

Chi-square (X^2) = 8
Degree of freedom = 1
Probability *p*= 0.0027

Appendix: H: Percentage of respondents who use password on home computer.



% of respondents who use password on home computer.

Appendix I: INFORMATION SHEET FOR PARTICIPANTS

RESEARCH TITLE:

Security behaviour of information system professionals on their home computer environment.

RESEARCHER: Jiby Jacob

BACKGROUND TO THE RESEARCH

Organisations around the globe have developed various programs to make employees aware of the importance of information security practices. These organisations have enforced technology security to keep their environment safe and secure. There isn't any study conducted on how information system professionals who are aware of computer security manage their home computer security where security is not enforced. This research is a case study research to study the security practises of information system professional in their home computer environments.

METHODS AND PROCEDURES

All participants who are willing to take part in the research project will be given a copy of this information sheet for their records and will need to sign the accompanying Participant Consent Form. You are invited for this research because this study is conducted among information systems professionals. It is important to note that your participation is voluntary, confidential and can withdraw from the study at any time without penalty or need to give any reason.

As part of the research, you will be requested to complete a set of questionnaires in an anonymous online survey which should not be more than 20 minutes. It will be appreciated if all questions are completed. However, do feel free to omit any question you are unwilling to complete as there is no penalty whatsoever. 10 % of the randomly

selected respondents will be invited at a later stage to be part of focused interviews which you can also choose to withdraw from without any penalty.
Please note the following:

- All information collected through the online survey is completely anonymous and not traceable to respondents
- All recorded individual interviews (data, interview notes, tapes) will require explicit approval before they can be used in this research
- All recorded individual interviews (data, interview notes, tapes) will be destroyed as soon as no longer required for the purpose of this study
- Interviews will not be audio taped.
- No audio recordings will be made available to anyone nor will any such recordings be replayed in any public forum or presentation of the research.
- High level encryption and password will be deployed on media containing data collected in the course of this research to ensure that no data regulation is breached
- Data collected will only be retained for this research and in line with due processes as stipulated by the Ethics committee of the SCSS, Trinity College Dublin.

RELEVANCE

This research is being carried out in partial fulfillment of the requirements for the award of a Master Degree in Management of Information Systems, School of Computer Science and Statistics, Trinity College Dublin, Ireland.

Your participation in this research will enable us to understand the security behavior of Information Security professionals in their home computer environment. The information gathered from responses to this questionnaire will be used to create a foundation for further development of Information Technology security practices researches and recommendations.

FURTHER INFORMATION

If you have further queries regarding this research or will like to have more detailed information, do feel free to contact me directly or my supervisor: Ms Susan Leavy [email: leavys@tcd.ie]. If however, you have ethical concern about the research and how it is being conducted, you may contact the ethics committee of the SCSS by email: research-ethics@scss.tcd.ie

Thank you very much for participating.

Jiby Jacob [e-mail: jjacob@tcd.ie]
Dublin, May 2013