Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2011 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

9 July 2011

A Call For Research On Home Users' Information Security Behaviour

Ying Li
University of Oulu, ying.li@oulu.fi

Mikko Siponen
University of Oulu, mikko.t.siponen@jyu.fi

ISBN: [978-1-86435-644-1]; Full paper

A CALL FOR RESEARCH ON HOME USERS' INFORMATION SECURITY BEHAVIOUR

Ying Li, Department of Information Processing Science, University of Oulu, Oulu, Finland, ying.li@oulu.fi

Mikko Siponen, Department of Information Processing Science, University of Oulu, Oulu, Finland, mikko.siponen@oulu.fi

Abstract

The number of home computer users is increasing faster than ever. Home users' security should be an important research topic in IS security research, not only from the perspective of protecting home users' personal or work information on their home computers, but also because hijacked home computers have become an ideal breading ground for hackers attacking organizations, and distributing illegal or morally questionable material. Despite the importance of studying home users' security behaviour, the primary focus of the behavioural IS security research has been on an organizational context. While this research at an organizational context is important, we argue that the "home users" context require more attention by scholars. While there are similarities between "home users' IS security behaviour" and "employees' compliance with IS security procedures at organizational context", it is necessary to understand their differences, to allow research and practice on "home users security behaviour" to develop further. We argue that previous research has not paid attention to such differences. As a first step in remedying the gap in our understanding, we first theorise these differences, we consider, that there are at least nine contextual factors that may result in an individual's behaviour inconsistency in the workplace and home, and because of this, we argue that the same theories may not explain the use of security features in home and organizational contexts. Based on this conceptualization, we present a research agenda for studying home users' security behaviour.

Keywords: Home user, Information security behaviour, Contextual factors, Individual's behaviour inconsistency.

1 INTRODUCTION

The number of home computer users is rapidly increasing. In 2008, Gartner, an American research firm published that the number of personal computers in use around the world had surpassed 1 billion; this number will double by early 2014. The large number of individual home users represents a significant point of weakness in achieving the security of the cyber infrastructure (Anderson and Agarwal 2010). While home users have a high chance of providing valuable information to intruders (e.g., information on emails, Internet banking, online shopping, instant messaging, and online stock trading), home users' information security should also be a concern for organizations. This is the case, since hijacked home computers are great breading grounds for hackers and distributors of illegal or morally questionable material. Indeed, Stafford and Urbaczewski (2004) report that 85% of all personal computers (PCs) are infected by spyware. It is essential for home users to recognize the risks and take appropriate precautions in their computer security. Despite the importance of studying home users' security behaviour, the main focus of behavioural IS security research has been on an organizational context, studying such issues as "employees' compliance with IS security procedures" (Herath and Rao 2009; Bulgurcu 2010; Li, Zhang et al. 2010; Puhakainen and Siponen 2010; Siponen and Vance 2010). While this research in an organizational context is important, we argue that the "home users" context requires more attention by scholars. While there are similarities between "home users' IS security behaviour" and "employees' compliance with IS security procedures at an organizational context", it is necessary to understand their differences, in order for research and practice on "home users security behaviour" to develop further. We argue that previous research has not paid attention to such differences. As a first step in remedying the gap in our understanding, we first theorise these differences, we consider, that there are at least nine contextual factors that may result in an individual's behaviour consistency in the workplace and home, and argue that the same theories (or their constructs) may not explain the use of security features in the home and organizational context. Finally, we present a research agenda for studying home users' security behaviour.

The rest of the paper is organized as follows. The second section reviews previous studies about end users' IS security behaviour. The third section theorizes the differences between organizational and home use. The fourth section presents an agenda for future research. The fifth section summarizes the findings of the paper.

2 PREVIOUS WORK ON INFORMATION SECURITY BEHAVIOUR

In order to better understand the research status quo of individual information security behaviour, we summarize and review the literature in two main categories: research in the workplace setting and research in the home setting.

2.1 Previous research in the workplace setting

Behavioural studies regarding IS security have been emphasized in recent years. There are three main issues in the context of an organization that have attracted many scholars in the IS field: (1) security awareness training/education; (2) IS misuse/abuse; (3) security policy compliance.

Awareness training and education on IS security in an organization are most commonly suggested in literature (Puhakainen and Siponen 2010). Some literatures are practitioner oriented, presenting practical methods and approaches to call employees' attention to IS security. According to the characteristics of human behavioural change, scholars suggest respective programs in different stages (Telders 1991; Guttman 1995; Desman 2002). Some focused on the media, such as on the use of video (Murray 1991; Peltier 2000; Mitnick and Simon 2003), booklets and newsletters (Murray 1991; Spurling 1995; Peltier 2000), and screen savers (Spurling 1995). In terms of the forms and contents in an awareness programme, Perry (1985) suggests means to impact user behaviour, for example, a

senior officer attending an IS security seminar, hiring a consultant to review the organization's IS security program, and so on. de Zafra et al. (1998) propose three fundamental training content categories: knowledge of laws and regulation, security programme, and system life cycle security. Other literatures are theory oriented. Models have been established to explain managerial perceptions of systems risk, including IS security training (Goodhue and Straub 1991). The main reason for IS security training is to communicate severity and the certainty of sanctions to employees (Straub and Welke 1998). Also, some scholars propose the steps of an awareness training programme from an academic view (Vroom and Solms 2002; Vroom and von Solms 2002; Tudor 2006). As the fruit of contents, forms, and specific procedures, awareness training and education play important roles in an organization to help employees set up security concept of information systems and conduct security behaviour.

"**Computer abuse**" was first defined by Parker (1976), and refers to "the unauthorized and deliberated misuse of assets of the local organizational information system by individuals", including the misuse of hardware, software, data, and computer services (Straub and Straub 1990; Harrington 1996; Lee 2004; D'Arcy, Hovav et al. 2009). Studies on computer abuse and misuse have applied theories in criminology, such as deterrence theory (Straub and Straub 1990), which predicts that abuse will decrease as a function of the severity and certainty of the expected punishment, and situational crime prevention (Willison 2006), which aim to reduce the opportunities for specific computer crimes. Harrington (Harrington 1996) found that codes of ethics act as deterrents. Computer abuse is commonly seen as deviant within an organization. Deterrence theory and situational crime prevention aim to decrease the occurrence of the deviance. The premise of these theories is that an organization has the same mechanisms as society, which can regulate the members' behaviour through policies and norms.

The studies on **security policies and end-user policy compliance** are also abundant (Siponen, Pahnila et al. 2007; Herath and Rao 2009; Herath and Rao 2009; Bulgurcu 2010; Puhakainen and Siponen 2010; Siponen, Pahnila et al. 2010). Employees are expected to obey the rules and conduct security behaviour when they are at work. Deterrence theory is most commonly applied in this stream of research. Certainty and security of sanctions positively associate with one's perceived cost of noncompliance (Bulgurcu 2010), significantly influencing employees' compliance intention (Herath and Rao 2009), or behaviour (Siponen, Pahnila et al. 2007; Siponen, Pahnila et al. 2010). Another commonly used theory is protection motivation theory. Protection motivation focuses on the effect of threat appraisals and coping appraisals. In the context of IS security, threat appraisals are assessments of individual's levels of security risks, while coping appraisals refer to assessments on whether individuals are capable of complying with security policies and whether such compliance is effective in reducing security risks (Siponen, Pahnila et al. 2006). Pahnila et al. integrated protection motivation and deterrence to explain security policy compliance in an organization, but found that sanctions had no significant impact on compliance behaviour (Pahnila, Siponen et al. 2007). Similarly, Herath and Rao also found that detection probability and security risks have significant impacts on employees' compliance intention, but sanction severity does not (Herath and Rao 2009). There are also other theories that greatly contribute to this issue. Siponen and Vance (2010) applied neutralization theory to explain that employees may use neutralized techniques to rationalize their rule-breaking behaviour. Bulgurcu (2010) analyzed employees' compliance from a benefit-cost view based on rational choice theory.

2.2 Previous research in the home setting

Compared to studies in organizations, behavioural studies about IS security in the home setting seem deficient. Anderson and Agarwal (2010) did two-phase studies to examine the home computer user security behaviour. One study established an integrated model based on protection motivation theory and theory of planned behaviour. The result shows that the relation between normative belief and home users' intention to perform security-related behaviour is not supported, which is mostly supported in the organization setting. The second phase study drew upon the concepts of goal framing and self-view to examine how the proximal drivers of intentions to perform security-related behaviour. It would help design effective marketing messages to encourage home users' security behaviour

(Harrington, Anderson et al. 2006). Theories applied in home user security behaviour are quite insufficient. Several studies are TPB-based, like Ng and Rahim (2005) who proposed an extended theory of planned behaviour focusing on the social influence, especially the mass media's effect on home users' intention to practice computer security. Lee and Kozar (2008) also proposed an extended TPB model to investigate home users' adoption of anti-spyware software. They added constructs drawn on innovation diffusion theory, and IT ethics/morality into the model. Theories explaining employees' information security behaviour, like deterrence theory and rational choice theory have not been examined in the home context.

To sum up, the key focus of the behavioural IS security research has been on an organizational context. We argue that while there are similarities between "home users' IS security behaviour" and employees' behaviour at organizational context, it is necessary to understand their differences. Provided that previous research has not paid attention to such differences, we first theorise these differences, we consider, that there are at least nine contextual factors that may result in an individual's behaviour inconsistency in the workplace and home, and because of this, the same theories may not explain the use of security features in home and organizational contexts. Based on this conceptualization, we present a research agenda for studying home users' security behaviour.

3 UNDERSTANDING OF INFORMATION SECURITY BEHAVIOUR

With the popularization of computers, individuals can use computers in a variety of circumstances, or contexts. These contexts can be the work place, home, or other places where offer public computers or networks. We argue that individuals' information security behaviours under different contexts may be complex and changeable.

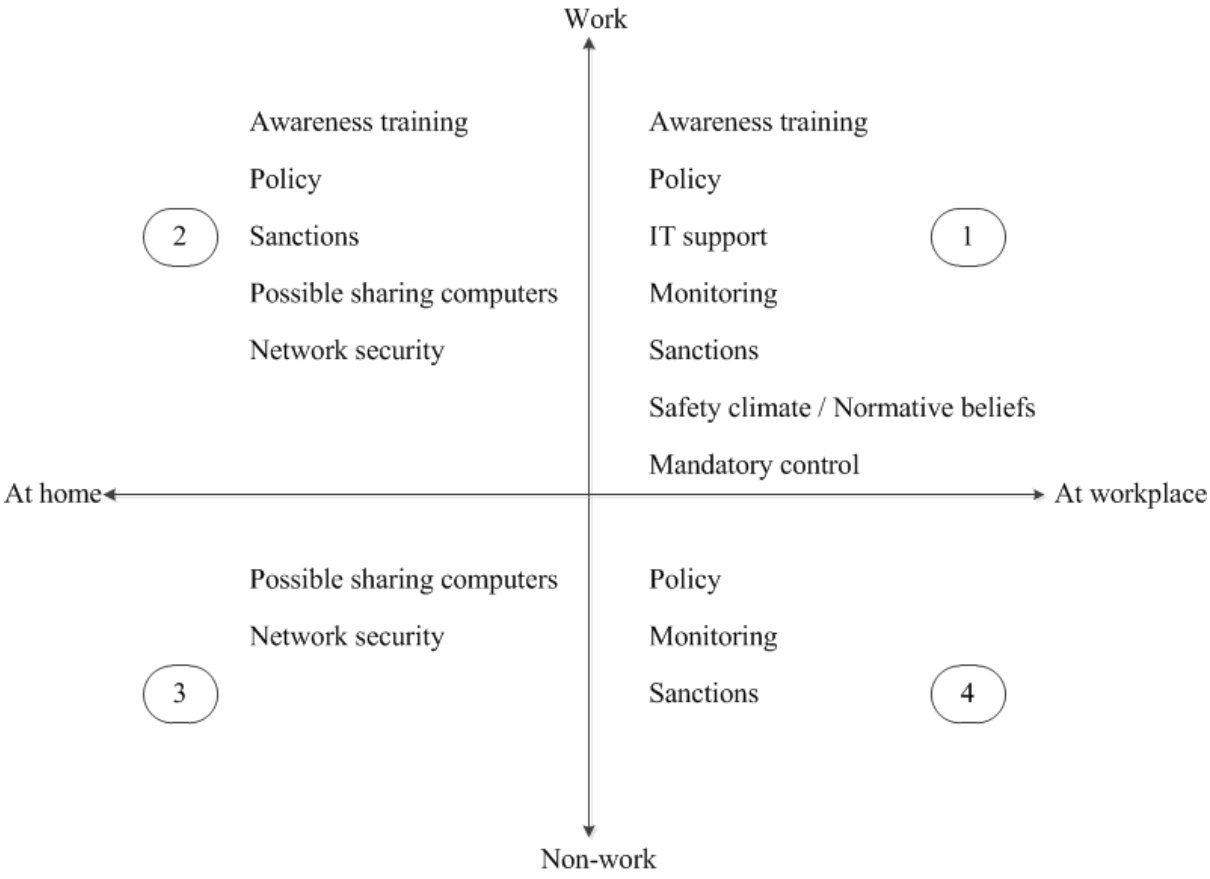

Figure 1. Features of four contexts

3.1 Individual security behaviour inconsistency between home and work

In the home context, individuals can choose whether and how to conduct security behaviour. Since the home user's choice is subjective and voluntary, and the environment and conditions differ from in an organization, there are possibilities that home user's behaviour might be inconsistent with that in the workplace. For example, employees do not need to install anti-spyware by themselves because the IT administrator does this work, while home users should install it by themselves. Home users may judge whether the computer has risks, whether they need the software, and any other factors when they decide to install it. This example shows that organizations have IT support, while home users don't, which might influence users' decisions and actions to protect their computers. This results from contextual factors. Another example is password habit; employees may keep their work-related password secret as there is a strict security policy and employees should account for the trouble caused by disclosing work-related password to others. However, there may be no regulations on their personal passwords. People may share non-work related password to friends, families, or colleagues. This difference relates to the type of use, work or non-work. Next we discuss four types of uses, which are not explicitly recognized by extant IS security research.

3.2 Type of use: work or non-work

To understand individuals' information security behaviour differences, we analyse four types of use that are divided into two dimensions. One dimension is place. Due to the flexibility of office models such as telework, people can also work outside, not subject to a fixed workplace. We chose the work place and home to discuss, which are the two typical contexts for most computer users. Another dimension is work or non-work related tasks that individuals are doing on computers. Work use refers to individual's using computers for the purpose of finishing work tasks. Non-work use refers to individual's using computers for a personal purpose. It is a key factor for individuals to determine whether to conduct information security behaviour or not. We are going to describe the four types of use and discuss contextual features (see Fig.1) in details.

Type of use 1: Work at workplace. The information security problems that occur in this situation include employees' non-compliance with organizational security policies. Here, employees do not follow the information security requirements during the working procedure, for example, unauthorized access, not logging out when they leave their workstation, copying confidential data, etc. (Siponen and Vance 2010). There is also another possible noncompliance. This is when people use their computers for personal tasks at the workplace, which we will analyse later. Most of the studies on employees' compliance do not distinguish between these two kinds of noncompliance, and only discuss compliance in a broad sense (Myyry, Siponen et al. 2009; Bulgurcu 2010; Bulgurcu, Cavusoglu et al. 2010; Johnston and Warkentin 2010).

Type of use 2: Work at home. Most information security behaviour problems that happen in the workplace cannot be avoided at home since home provides a much more relaxed work environment for employees. In principal, employees should conform to all the policies and regulations because they should be responsible for their work data no matter where they are working. Also, because of the lacking of supervision and management, it is a much bigger challenge for an organization to keep an employee conducting secure behaviour. In this setting, an individual's information security behaviour may rely on personal awareness and decisions.

Type of use 3: Non-work at workplace. Most organizations are concerned with this problem. Employees use organizational IS resources for personal purposes during and after working hours. This behaviour may lead to a waste of IS resources and even a loss of assets. Most organizations expressly exhibit this behaviour. Hence, this can be seen as another kind of employees' noncompliance with procedures. Behavioural studies on abuse and misuse of IS recourses give rich explanations on this phenomenon (Tuglular and Spafford 1997; Lee and Lee 2002; Lee, Lim et al. 2005; Willison 2006; D'Arcy, Hovav et al. 2009; Li, Zhang et al. 2010).

Type of use 4: Non-work at home. Compared to work at the workplace, non-work at home has different types of use and a different environment for individuals. It is a different setting from an

organization context. Individuals have more computer activities at their disposal. Examples include online shopping, playing online games, web chatting, online stock trading, downloading software and music, and so on. These computer activities provide many enjoyable experiences to the individual, which are different from work activities. So, taking the types of use and the context into consideration, an individual's attitude towards information security and actual behaviour can be different from previous studies in an organization context. Next, we show that there are at least nine contextual factors that are different among the types of use. By term home use, we especially refer to type of use 4 (non-work at home).

3.3 Contextual factors

With the development of information and communication technologies, people can work with computers both at an organizational workplace and home. We argue that individuals' information security behaviour under different contexts (e.g., between type of use 1 and 4) might be different. The contextual factors have an important impact on individuals' perceptions and could then influence actual information security behaviour.

Awareness training

Organizations usually design training programmes for security purposes. The programmes aim to change employees' attitudes towards IS security, emphasize the importance of IS security, clarify the rules and policies and highlight employees' responsibilities regarding IS security issues. In terms of content, awareness training commonly includes security events that usually occur in organizations, the risks confronted, the basic concepts of IS security, how to establish good security habits, and recommended supports available when facing security problems. In terms of communication of the awareness or training programs, organizations have many options, such as, newsletters, videos, handouts, leaflets, etc. (Murray 1991).

In the home context, end users hardly receive any formal IS security awareness training. Knowledge of IS security mostly comes from self-learning and self-experience. Of course, some people may have received training at their workplace, but there is no empirical evidence indicating whether that transfers to increase home security. In the case of home users, security awareness often comes out with panic after end users encounter threats such as viruses, Trojans, worms, or when they consequently lose data. There is also another way to influence home users' security awareness, with social factors. Ng and Rahim's (2005) study shows that mass media, family and peers play important roles in promoting computer security. To sum up the findings with respect to our first contextual factor, we hypothesize that:

Information security awareness sessions provided by organizations has more influence on type of use 1 than type of use 4.

Policies

IS security policy is an important component of a management system in an organization. Usually, the policy contains regulations on the following aspects: network, devices, data, operation, sanctions, and so on. The policy is not only a guideline for security management, but is also a code of conduct for employees. It instructs employees how to use IS resources correctly and safely, while it deters employees from violating the policy. An IS security policy greatly contributes to keeping IS safe. Policy is therefore an important feature in the organization context. However, most information security policies are not confined to work place. If employees are working outside the office, they also have the responsibility to ensure the safety of organizational materials. Some of the policies take effect no matter where the employees are working. Hence, we hypothesize that:

The effect of information security policy is related to work, and hence, has more influence on individuals' behaviour in type of use 1than 4.

IT support

Organizations have the capability to implement the security plan. They invest large amounts of money, time and resources. This makes it easy for employees to get security support on software and

hardware, and also timely human assistance. However, for the end user in the home context, investment on security is limited, or non-existent. Insurance for security is missing. Another point is that organizations offer IT support only for work purposes, not for personal use, which has no relationship with work. Therefore, IT support only exists in type of use 1. This means that IT support regarding IT and information security is much most limited in type of use 4 with the result that home users need to use their own expertise to secure their PCs. Therefore, we hypothesize that:

Due to IT support at organization context, the level of information security is lesser in type of use 4 than type of use 1.

Monitoring

Monitoring mechanisms are commonly used in organizations to gain compliance with rules and regulations (Urbaczewski and Jessup 2002). Monitoring systems will track employees' computer and Internet use, record network activities, and perform security audits (Panko and Beh 2002; Urbaczewski and Jessup 2002). Monitoring, as a control method will, to some extent, constrain employees' behaviour. Since they know their activities will be recorded, employees will not conduct insecure behaviour. Obviously, in the home context, there is no such monitoring mechanism due to privacy protection, so it is not a feasible approach to promote home users' security behaviour. As we analyse above, we hypothesize that:

Due to monitoring at organization context, the level of information security is lesser in type of use 4 than type of use 1.

Fear factors

Fear factors are examined in papers on IS security management in organizations (Siponen, Pahnila et al. 2007; Lee and Larsen 2009; Schuessler 2009; Johnston and Warkentin 2010; Li, Zhang et al. 2010). There are mainly two theories explaining individuals conducting security behaviour due to fear. They are deterrence theory and protection motivation theory. Deterrence theory focuses on formal sanctions that employees receive if they violate security policies. The certainty and severity of sanctions motivates employees' compliance. Protection motivation theory focuses on threat appraisals and coping appraisals. An employee assesses the level of security risks to the organization and whether he or she has the ability to deal with the situation. Sanctions are occur only in organizations, and not in the home context. While, protection motivation factors are applicable to both an organization (Siponen, Pahnila et al. 2007; Lee and Larsen 2009) and home context (Woon, Tan et al. 2005; Anderson and Agarwal 2010), but the focus of threat appraisal in home context are the risks confronted by home computers. Since the fear factors in organization context are related to employees' responsibility, but in home context, they are not, and sanctions are missing as well. Hence, we hypothesize that:

Fear factors have more influence on individuals' behaviour in type of use 1 than type of use 4.

Safety climate

Safety climate in an organization was first proposed by Zohar (1980). Zohar suggested that employees who perceived a strong safety climate in the organization worked more safely. The perception was derived from observance of organizational management, superiors', and peer attitudes (Chan, Woon et al. 2005). Chan et al. (2005) conducted an empirical study, and results showed that the information security climate encouraged employees' compliance behaviour. In comparison, the safety climate is hard to form at home. It relies on the security awareness, desires, and requirements of each family member. Security climate can only be formed with all family members' efforts. Based on this, we hypothesize:

Safety climate provided by organizations has more influence on individuals' behaviour in type of use 1 than type of use 4.

Mandatory control

Mandatory control is a characteristic of an organization that is a compulsory procedure by organizational management to ensure employees behave in a certain manner (Boss, Kirsch et al. 2009).

For example, in an organization, the adoption of anti-spyware or anti-malware on computers has the feature of compulsory, meaning that the adoption decision is made by the organization -not the employees. Employees have no rights to choose. However, in the home context, end users have far more independent options. They can choose whether to install protection software or not, or what kind of protective technology to use. It is absolutely voluntary. Therefore, we hypothesize that:

Due to IT support at organization context, the relevant security behaviours differ between different types of uses, especially between type of use 1 and 4.

Network security

Network security on one hand depends on the safeguard of hardware and software. Due to the IT support that organizations offer, such as firewalls, anti-malware software, and so on, organizations are well prepared for Internet attacks. However, in the home context, people might invest less on hardware and software, which may result in a low level of network security. On the other hand, network security relies on the user's maintenance of the system. In an organization, there are IT specialists to explore potential network risks and solve problems. In the home context, unless the user has related knowledge and problem-solving capability, most home users who do not take measures to safeguard networks face the possibility of being attacked by intruders. Hence, we hypothesize that:

The level of network security has influence on security behaviours in different types of use, especially between type of use 1 and 4.

Sharing computers

Unlike in an organization where end users may use their own computers, in the home context, there are often several users to one home computer. This increases the difficulty of managing computer security. Therefore, we hypothesize that:

Sharing computers in home deceases the level of security behaviour in type of use 4, compared to 1.

We summarize the features for each type of use in Fig. 1. Taking type of use 1 for example, if an individual is doing work-related tasks in the work place, the following contextual factors have an impact on his or her information security behaviour: awareness training, policy, IT support, monitoring, sanctions, safety climate and mandatory control.

4 AGENDA FOR FUTURE RESEARCH ON HOME USERS' INFORMATION SECURITY BEHAVIOUR

Based on our conceptual argument on the differences between home users and organizational employees with respect to information security behaviour, we outline a research agenda with seven research streams for the home users' information security behaviour (especially, type of use 4).

The first stream of research endeavours to empirically prove our argument that the nine contextual factors make a difference between the behaviour of home and organizational users. One way to justify this is to design a theory-testing study. A model comparison approach in both home and organizational contexts is called for. Different results in different contexts are expected, which will provide empirical evidence that home users' information security behaviour constitutes its own research area.

The second stream of research focuses the differences between all kinds of types of uses. In this paper, we mainly argued that the different types of uses are not discussed by IS security research, and we provided four potential types of uses. We also argued that there difference between these, especially between types of uses 1 and 4. Future research is needed to study the other types of uses.

The third stream of research is aimed at exploring the types of relevant behaviour, which should be studied as "dependent variables", for home users. For example, employees use of anti-spyware software might not be relevant behaviour for studying employees' compliance with organizational IS security procedures, given that it is good security policy that ordinary employees should not have

privileges to install any programs. However, the use of anti-spyware software could be a relevant issue for home users. Similarly to Siponen and Vance (2010), who interviewed 56 IS security managers to find out the key problems for employee compliance with organizational IS security policies, there is need to explore the required key information security behaviours for home users.

The fourth stream of research could adopt a theory-testing research setting and explore, based on our nine contextual factors, what behavioural theories could best explain home users' information security behaviour. A number of potential theories exist in the area of psychology, social psychology and criminology. Another possibility in addition to finding out which behavioural theories explain the best home users behaviour, is to try to form a unified theory for home users security behaviour à la UATAUT.

The fifth stream of research is theory-development. While the third stream of research called for theory-testing, we also see that inductive and qualitative approaches are needed. The limitation of the theory testing setting is that it merely tests if existing theory is supported or not. Such an approach would approach the problem from a clean table without any theories in mind by asking that home users report the reasons why they adopt information security measures. Ideally, this would come up with new constructs, concept and even new theories that explain home users' information security behaviour. Such in-depth interview studies could also reveal a process, which covers the stages for adopting an information security behaviour or technique. Possible methods for analysing the interviews include phenomenography or grounded theory.

The sixth stream of research examines to what extend possible training the employees have received in their organizations transfers to increased home security. Given that some employees may have received IS security training at their organizations, one might postulate that this knowledge transfers to home context. On the other hand, there are a number of reasons as to why one may argue that IS security training at organizations may not reach to home context. First, IS security training at organizations may typically focus on organizational issues (Puhakainen and Siponen 2010). As a result, employees may feel that what they have learned do not apply home context; after all, perhaps in the case of IS security training at organizations there was no persuasive message about the importance on protecting one's home computer. Hence, it is an open question future research whether IS security training at organizations influence home context.

The seventh stream of research calls for experimental studies. The aim of these studies is to observe how home users' information security behaviour can be changed with some kind of treatment, such as theory-based training or campaigning. Following experimental research settings, the participants will be divided into two groups. The experimental group will get a persuasive intervention, while the control group will not. Pre and post tests are then used to evaluate the effect of the treatment. Such experimental research is important, because the ultimate goal of the research under the domain of home users' security behaviour is not only to explain how things are, but to change them, here through training and campaigning.

5 CONCLUSIONS

The number of home computer users is increasing faster than ever. Home users' security should be an important research topic in IS security research, not only from the perspective of protecting home users' personal or work information on their home computers, but also because hijacked home computers have become an ideal breading ground for hackers attacking organizations, and distributing illegal or morally questionable material. Despite the importance of studying home users' security behaviour, the primary focus of the behavioural IS security research has been on an organizational context. While this research at an organizational context is important, we argue that the "home users" context require more attention by scholars. While there are similarities between "home users' IS security behaviour" and "employees' compliance with IS security procedures at organizational context", it is necessary to understand their differences, to allow research and practice on "home users security behaviour" to develop further. We argue that previous research has not paid attention to such differences. As a first step in remedying the gap in our understanding, we first theorised these differences between the contexts and behaviours of home users and employees at organizations. As a

part of this conceptualisation, we pointed out that there are at least nine contextual factors that may result in an individual's behaviour inconsistency in the workplace and home, and because of this, we argued that the same theories may not explain the use of security features in home and organizational contexts. Based on this argumentation, we present a research agenda for studying home users' security behaviour.

References

Anderson, C. L. and R. Agarwal (2010). "Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions." *MIS Quarterly* **34**(3): 613-643.

Boss, S., L. Kirsch, et al. (2009). "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security." *European Journal of Information Systems* **18**(2): 151-164.

Bulgurcu, B. (2010). "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS Quarterly* **34**(3): 523-548.

Bulgurcu, B., H. Cavusoglu, et al. (2010). Quality and Fairness of an Information Security Policy As Antecedents of Employees' Security Engagement in the Workplace: An Empirical Investigation, IEEE.

Chan, M., I. Woon, et al. (2005). "Perceptions of information security at the workplace: linking information security climate to compliant behavior." *Journal of Information Privacy and Security* **1**(3): 18–41.

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

de Zafra, D., S. Pitcher, et al. (1998). "Information Technology Security Training Requirements: A Role-and Performance-Based Model." NIST Special Publication: 800-816.

Desman, M. (2002). Building an information security awareness program, Auerbach Pub.

Goodhue, D. and D. Straub (1991). "Security concerns of system users* 1:: A study of perceptions of the adequacy of security." *Information & Management* **20**(1): 13-27.

Guttman, B. (1995). An introduction to computer security: the NIST handbook, DIANE Publishing.

Harrington, S. (1996). "The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions." *MIS Quarterly* **20**(3): 257-278.

Harrington, S., C. Anderson, et al. (2006). "Practicing Safe Computing: Message Framing, Self-View, and Home Computer User Security Behavior Intentions." *ICIS 2006 Proceedings:* 93.

Herath, T. and H. R. Rao (2009). "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness." *Decision Support Systems* **47**(2): 154-165.

Herath, T. and H. R. Rao (2009). "Protection motivation and deterrence: a framework for security policy compliance in organisations." *European Journal of Information Systems* **18**(2): 106-125.

Johnston, A. C. and M. Warkentin (2010). "Fear appeals and information security behaviors: an empirical study." *MIS Quarterly* **34**(3): 549-566.

Lee, J. and Y. Lee (2002). "A holistic model of computer abuse within organizations." *Information Management and Computer Security* **10**(2/3): 57-63.

Lee, O. K. D., K. H. Lim, et al. (2005). Why employees do non-work-related computing: an exploratory investigation through multiple theoretical perspectives, IEEE.

Lee, S. (2004). "An integrative model of computer abuse based on social control and general deterrence theories." *Information & Management* **41**(6): 707-718.

Lee, Y. and K. Kozar (2008). "An empirical investigation of anti-spyware software adoption: A multitheoretical perspective." *Information & Management* **45**(2): 109-119.

Lee, Y. and K. R. Larsen (2009). "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software." *European Journal of Information Systems* **18**(2): 177-187.

Li, H., J. Zhang, et al. (2010). "Understanding compliance with internet use policy from the perspective of rational choice theory." *Decision Support Systems* **48**(4): 635-645.

Mitnick, K. and W. Simon (2003). The art of deception: Controlling the human element of security, John Wiley & Sons, Inc. New York, NY, USA.
Murray, B. (1991). Running corporate and national security awareness programmes.
Myyry, L., M. Siponen, et al. (2009). "What levels of moral reasoning and values explain adherence to information security rules? An empirical study." *European Journal of Information Systems* **18**(2): 126-139.
Ng, B.-Y. and M. Rahim (2005). A socio-behavioral study of home computer users' intention to practice security. *PACIS 2005 Proceedings*.Paper 20.
Pahnila, S., M. Siponen, et al. (2007). Employees' behavior towards IS security policy compliance. HICSS 2007.156.
Panko, R. and H. Beh (2002). "Monitoring for pornography and sexual harassment." *Communications of the ACM* **45**(1): 84-87.
Peltier, T. (2000). "How to build a comprehensive security awareness program." *Computer Security Journal.* **16**(2): 23-32.
Perry, W. (1985). Management strategies for computer security, Butterworth-Heinemann Newton, MA, USA.
Puhakainen, P. and M. Siponen (2010). "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study." *MIS Quarterly* **34**(4): 757-778.
Schuessler, J. (2009). General deterrence theory: Assessing information systems security effectiveness in large versus small businesses. Large versus Small Businesses. Denton, Texas. UNT Digital Library.
Siponen, M., S. Pahnila, et al. (2006). "Factors influencing protection motivation and IS security policy compliance." *Innovations in Information Technology*, 2006: 1-5.
Siponen, M., S. Pahnila, et al. (2007). "Employees' adherence to information security policies: an empirical study." New Approaches for Security, Privacy and Trust in Complex Environments: 133-144.
Siponen, M., S. Pahnila, et al. (2010). "Compliance with Information Security Policies: An Empirical Investigation." *Computer* **43**(2): 64-71.
Siponen, M. and A. Vance (2010). "Neutralization: new insights into the problem of employee information systems security policy violations." *MIS Quarterly* **34**(3): 487-502.
Spurling, P. (1995). "Promoting security awareness and commitment." *Information management & computer security* **3**(2): 20-26.
Stafford, T. F. and A. Urbaczewski (2004). "Spyware: The ghost in the machine." *Communications of the Association for Information Systems* (Volume14, 2004) **291**(306): 291.
Straub, D. and W. Straub (1990). "Effective IS security." *Information Systems Research* **1**(3): 255-276.
Straub, D. and R. Welke (1998). "Coping with systems risk: security planning models for management decision making." *MIS Quarterly* **22**(4): 441-469.
Telders, E. (1991). "Security awareness programs: a proactive approach." *Computer Security Journal* **7**(2): 57-64.
Tudor, J. (2006). Information security architecture: an integrated approach to security in the organization, CRC Press.
Tuglular, T. and E. Spafford (1997). "A framework for characterization of insider computer misuse." Unpublished paper, Purdue University.
Urbaczewski, A. and L. Jessup (2002). "Does electronic monitoring of employee internet usage work?" *Communications of the ACM* **45**(1): 80-83.
Vroom, C. and R. v. Solms (2002). A Practical Approach to Information Security Awareness in the Organization. Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives, Kluwer, B.V.**:** 19-38.
Willison, R. (2006). "Understanding the perpetration of employee computer crime in the organisational context." *Information and Organization* **16**(4): 304-324.
Woon, I., G. Tan, et al. (2005). A protection motivation theory approach to home wireless security.
Zohar, D. (1980). "Safety climate in industrial organizations: Theoretical and applied implications." *Journal of applied psychology* **65**(1): 96.