Getting their Hands Stuck in the Cookie Jar

- STUDENTS' SECURITY AWARENESS IN 1:1 LAPTOP SCHOOLS

FREDRIK HELLQVIST
SWEDISH BUSINESS SCHOOL
ÖREBRO UNIVERSITY
SWEDEN
FREDRIK.HELLQVIST@GMAIL.COM

SAMIR IBRAHIM
SWEDISH BUSINESS SCHOOL
ÖREBRO UNIVERSITY
SWEDEN
SAMIR-IBRA@HOTMAIL.COM

ROBIN JATKO
SWEDISH BUSINESS SCHOOL
ÖREBRO UNIVERSITY
SWEDEN
ROBIN_JATKO@HOTMAIL.SCOM

ANNIKA ANDERSSON
SWEDISH BUSINESS SCHOOL
ÖREBRO UNIVERSITY
SWEDEN
ANNIKA.ANDERSSON@ORU.SE

KARIN HEDSTRÖM
SWEDISH BUSINESS SCHOOL
ÖREBRO UNIVERSITY
&
DEPARTMENT OF MANAGEMENT AND ENGINEERING
LINKÖPING UNIVERSITY

International Journal of Public Information Systems, vol. 2013:1
www.ijpis.net

SWEDEN
KARIN.HEDSTROM@ORU.SE

Abstract

This paper presents results from an ongoing research project studying schools that have implemented one-to-one-laptops (1:1). The research is interpretative and builds on interviews and survey-responses from students and teachers in two public 1:1 schools in Sweden. We are focusing on the students' security awareness and compliance by researching into whether the students in 1:1 schools comply with the school's information security policy (ISP). Theoretically, a security awareness perspective is drawn up based on three parts - formal, cognitive and behavioral awareness - that should be in parity with each other. This means that the students' psychological perception and actual behavior should be in parity with the schools' ISP. Our findings show that the schools have communicated their ISPs well and that the students' security awareness in most areas is equivalent to the schools' ISPs. However, we also found many instances where it was not the case that the formal, cognitive and behavioral security awareness was in parity with each other. In the analysis of the students' behavioral security awareness we found that despite the fact that they were aware of the rules they occasionally violated them – most notably when file-sharing and the downloading of software were involved. We conclude by arguing that non-compliance can only be understood based on an understanding of the students' underlying reason for following or not following the policies and regulations, and that in order to create a secure information environment, school managers must talk to the students to understand their reasoning. In a situation where 1:1 is spreading rapidly among schools, studies regarding students' security awareness and behavior are urgent, but so far the field is under-examined.

Keywords: Public schools, 1:1 laptops, security awareness, security compliance, case study

1. Introduction

The use of computers in schools is rapidly increasing – today most notably through the 1:1 programs that are being implemented all around the world (Learning Cultures Consulting Inc, 2009). One of the first larger 1:1 initiatives took place in Maine, USA, during 2002-2004 when 27,000 students and 1,700 teachers were equipped with a personal laptop (Silvernail and Lane, 2004). Thereafter the 1:1 initiatives have spread throughout the world - not least in the Nordic countries, including Sweden, where this research takes place. The 1:1 programs can be seen as a reflection of the increased use of computers in our society in general (Bjelvenmark, 2011), but the programs also come

with many new pedagogical ideas. Initial hopes were that giving every student a laptop would improve the learning in many different ways (Bebell and Kay, 2010, Peck and Sprenger, 2008, Hadeed, 2000), but due to recent reports of decreased learning (e.g., Fried, 2008) the improvement of learning is still very much under debate. The research presented in this paper is part of a large research project in Sweden monitoring the effects of 23 schools' 1:1 initiatives and focuses on the students' security awareness and behavior. In a student survey we had found that there were inconsistencies in the students' answers (from the same school) regarding the rules with regards to what they were allowed to download and install and whether they were allowed to take the computer home or not. These findings were the basis of the decision to investigate the students' security awareness and behavior in greater depth. The objective of this paper is to investigate whether secondary school students comply with information security policies, and, if so, to what extent.

Sweden has a relatively long history of computer use in schools and the government continuously updates its directives to the Swedish National Agency for Education regarding how to encourage and support the use of ICTs in schools. One of the major projects to promote computers in schools was launched in 1999. The project was called ITiS (Information Technology in School) and was a national school development programme in Sweden that lasted for 8 years (Andersson, 2006). During the first three years of this programme 1, 3 billion SEK were spent on technology and 200 million SEK on teacher training (including more than 50% of all teachers in Sweden at the time). Changes in school policies during recent years have made the ICT focus to be even stronger. Today computer-labs are being closed down and Swedish students are instead being provided with mobile laptops, phones and tablets. 250 municipalities (of Sweden's 290 municipalities) have started - or are in the planning stages of - implementing 1:1 classrooms in their schools. These 1:1 programs are run on a municipal level and include students from pre-school to the final year of the upper-secondary level (Johannesson, 2011). While the distribution of laptops is rapidly increasing in Swedish schools, little knowledge is, however, being created about the benefits and drawbacks of the various uses with regards to these laptops. Against this backdrop, 23 schools decided to join forces and to have their 1:1 implementation evaluated by researchers. It was decided that a research group consisting of researchers from both Educational Science and Informatics should follow the development of these schools over a period of three years. The name of the research project is UnosUno and stretches over the period 2010-2013. During these three years the research group was supposed to monitor and analyze the effects of the 1:1 initiatives. The evaluation criteria relate to the students' learning and development, the teachers' roles and methods, school management's guidance and steering, in addition to the cooperation and relationship between the school and the home. As previously

mentioned, the research presented in this paper is part of this larger study and focuses on the students' security awareness and behavior.

Previous research argues that university students are more prone to risky behavior and security attacks because of their lack of experience (Rezgui and Marks, 2008) and that risky unsafe Internet use does not decrease over the years (Valcke et al., 2011). Younger people can be more naïve concerning security risks (Atkinson et al., 2009) and this should also be true for younger secondary school students, who have little or no experience of cyber-attacks or fraud in general, while, at the same time they are surrounded by and use many different types of technologies such as mobile devices, laptops, and gaming consoles for connecting on-line.

In the research field, Information Security, it is a well-known fact that the behavioral and social aspects of information security are critical for creating secure information systems in practice (e.g., Sipponen et al., 2008, Stanton et al., 2005). This, together with the knowledge that the majority of information security breaches are caused by people inside an organization (Stanton et al., 2005, Nash and Greenwood, 2008), thus the management of the behavior of internal personnel is an important aspect if the requirement is to create a secure information environment (Gaunt, 2000, Williams, 2008), makes security awareness by young people in schools a very important issue to investigate. Managers commonly use information security policies and codes of conducts as tools for guiding and controlling security behaviors. These policies and guidelines must be complemented with information security awareness in order to create a secure information environment. This is the reason for the choice to investigate whether students do comply with information security policies, and if so, to what extent. In order to answer this question we also investigate how the ISPs have been communicated to the students - i.e., which prerequisites do the students have to comply with regarding the policy?

2. Theoretical Background

2.1 Security Awareness and Compliance

Security awareness is an expression that is broadly used in different fields dealing with how aware someone is concerning the risks in his/her environment. One of the limitations with a great deal of the security awareness discussions and research is how much of the focus is on technical issues, when research has shown that the socio-behavioral aspects of information security are crucial for creating a secure information environment (e.g., Sipponen et al., 2008, Stanton et al., 2005). User behavior with respect to security policies, i.e., compliance, has been recognized as an important and under-studied area for

information security research (von Solms and von Solms, 2004, Herath and Rao, 2009). Whether a person chooses to comply or not with the information security policy is significantly influenced by his or her values and beliefs (Bulgurcu et al., 2010, Hedström et al., 2011c). It has also been estimated that about half of the security breaches are accidental (Vroom and von Solms 2004), illustrating how behaviors causing these security breaches can be unintentional as well as intentional. It is therefore necessary to have security measures that are able to deal with both the intended as well as the accidental.

Information security management includes a number of security countermeasures for safeguarding information and preventing the misuse with regards to information systems (Baker and Wallace, 2007). The countermeasures for improving the security practices of information systems can be in the form of technical countermeasures, different administrative routines and guidelines, and awareness raising countermeasures such as education. In order to create a secure information environment it is necessary to ensure that the users are aware of, and act upon, the security policies (Puhakainen, 2006, Dhillon, 2007). The failure of users to comply with the security policies poses a significant threat (Siponen and Mahmood, 2010), thus making it crucial that the employees are security aware. Puhakainen (2006) suggests three approaches in relation to increasing security awareness: persuasive communication and education; active participation in the design of information policies; and punishments and rewards. It is also beneficial if users understand the importance of following security policies and guidelines and, the risks of security threats to the organization if they fail to do so. Atkinson et al (2009) also suggests using peer education to raise security awareness among young people.

The goals of our researched 1:1 schools are that the users should comply with the school's ISP and that the users behave accordingly, simply because"IS security solutions lose their usefulness, if users do not follow them" (Puhakainen, 2006, p. 57). Our view in relation to security awareness and how it can be achieved is inspired by Roger & Kincaid's convergence model of communication (Rogers et al., 1981) with regards to how we believe that security awareness can be achieved through communicative mutual understanding and that it is necessary to create security awareness in line with organizational culture (von Solms and von Solms, 2004). A recent study on non-compliance with HIPAA (The Health Insurance Portability and Accountability Act) showed that the work environment and organizational limitations are important factors for users' non-compliance (Liginlal et al., 2012). There can be a number of reasons why users do not comply with security policies. Accidental misuse can be an effect of inadequate knowledge of the system, stress or a genuine lack of knowledge of the rules.

Intentional misuse can be caused by insiders who carry out data theft due to personal differences or deliberate ignorance of the rules (Magklaras and Furnell, 2004). The most common misuse from legitimate users was the storage and dissemination of pornographic material (Magklaras and Furnell, 2004). The second most common misuse was theft or alteration of commercially sensitive information in 24 % of the cases, while e-mail abuse accounted for 16% of the cases (Magklaras and Furnell, 2004).

We thus view security awareness as consisting of three interrelated and interdependent parts that are required to be mutually understood and in balance: formal security awareness, cognitive security awareness and behavioral security awareness. This means that the social reality that the school is facing is a combination of the ISP that is communicated, how this policy is cognitively understood and how the students act upon this awareness. Security awareness is thus about understanding the information security policies, as well as complying with them.

2.1.1 Formal Security Awareness

Formal Security Awareness concerns the content of the ISP and how it has been communicated to the users. It is important at this point to track how the ISP is changing and the ability of the schools to adapt and make changes to ensure that the ISP is being communicated to the users. In our cases, the municipalities of the two schools had previously developed guidelines for IT use in schools that both schools has used as a basis for formulating their respective ISPs. This ISP is what we refer to as the physical reality that the school and its users have to relate to.

2.1.2 Cognitive Security Awareness

Cognitive Security Awareness refers to the users' perceptions about what security awareness is, i.e., the psychological reality the user exhibits in relation to the ISP the schools have communicated. Here, we address how the users have interpreted and understood the content of the security policies, as well as the consequences if they fail to comply. Thus, it is important to have an understanding of the security risks faced by the organization. The cognitive security awareness is thus a complicated psychological reality where the user does not always have to be aware of the perception he or she has. Complex factors such as the user's ethics and morals may have an influence in this case.

2.1.3 Behavioral Security Awareness

Behavioral Security Awareness concerns the actual behavior of users, i.e., how the users, in everyday IT practices, do or do not comply with the ISP. Here we have to consider how changes in the security behavior may cause changes in the user's cognitive perception. The Behavioral Security Awareness is what the user exhibits, which practices actually

occur, and is a result of how the school has been able to mediate its policy as well as how the policy is enacted in everyday practice.

In summary, our perspective with regards to security awareness is that the user's behavioral security awareness is grounded in his/her cognitive security awareness. All users have their own perceptions about potential threats and consequences that their behavior may have on others or themselves. This perception is, among other things, based on education, friends, routines and personal experiences. The user's perception, the cognitive idea of IT-security, is therefore an important factor leading to the actual behavior associated with the system.

Before we move on Figure 1 below summarizes our view on security awareness.

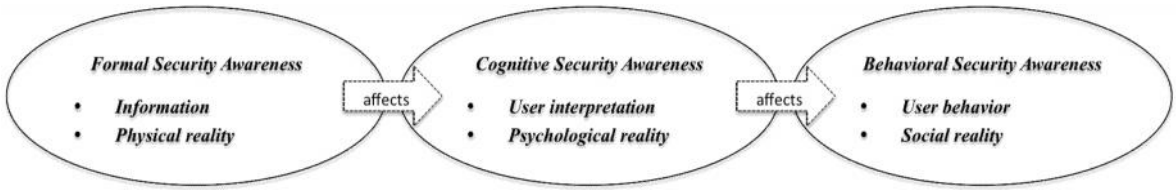

Figure 1. Security awareness as we see it

2.1.4 Contribution

Whereas security awareness is well researched in the IS field (see e.g., Albrechtsen and Hovden, 2010, Vroom and Von Solms, 2004), the idea that users do not always comply due to rational reasons is rather new and has, in recent years, been put forward as an alternative to the idea of the "vicious user" (Hedström et al., 2011b, Vaast, 2007, Albrechtsen and Hovden, 2010). Research within the field of 1:1 schools from the perspective of students' security awareness has still to be conducted.

3. Materials and Methods

This research is based on a case study in two public schools in Sweden that have recently implemented 1:1. The research is interpretative in assessing whether the students in 1:1 schools comply with the school's ISP. Using both quantitative and qualitative data we analyze our findings using a security awareness model mainly based on Puhakainens' work (Puhakainen, 2006).

3.1 Data Collection

Since we define security awareness as consisting of three interrelated parts, we have designed our study in relation to these parts. It was firstly necessary to capture the formal security awareness as reflected in the schools IT-policies and how this policy has been communicated to the students. Secondly, we analyzed the cognitive security awareness, i.e. the students' psychological reality, how they perceived the ISP. Finally, the behavioral security awareness was analyzed, which is the social reality where the students interpret the policy that leads to action and behaviors.

Considering these different aspects of security awareness, a mix of quantitative and qualitative data collection methods has been used. The quantitative part, the survey, above all captures the students' behavioral security awareness whereas the qualitative part, the interviews, mainly focuses on the cognitive security awareness.

3.1.1 Informants

Two public 1:1 schools from different municipalities (hereafter referred to school or municipality A and B) were selected for this research. Whereas there are numerous 1:1 schools in Sweden these two were selected due to their proximity (easy access) and their willingness to participate (commitment and assistance). In both schools we targeted secondary schools students in grade 7 and 8 (13-14 years of age). One of the schools had just started their 1:1 initiative whereas the other had been involved with it for a year. Our main informants are students, but teachers have also been interviewed because it was important to know how the ISP had been communicated to the students.

In school A, we distributed the survey to four classes (two in 7th grade and two in 8th grade) and interviewed seven students and two teachers. In school B we distributed the survey to all 7th graders and interviewed four students and three teachers. In both schools the mean age of students was 13 years. Table 1 below shows the material that formed the basis of this research.

Table 1

The data material used for this research

Data collection tool	Number of informants
Student survey	137
Student interviews	11
Teacher interviews	5

3.1.2 Questionnaire

137 questionnaires were distributed and 55 answers were received from our school in municipality B (response rate 82%) and 82 (response rate 100%) in municipality A. Whereas the main aim associated with these questions was to capture the students' behavioral security awareness, some questions also touched upon the formal- and cognitive aspects of security awareness (see Appendix A). The questionnaires were distributed on site in the respective schools and since we were fully aware that some of the questions may be of a sensitive character we informed the students that their responses would be treated anonymously and with strict confidentiality (Oates, 2008). The same guarantees were given during the interviews.

3.1.3Interviews

Our interviews with the students and teachers were semi-structured using an interview-guide (Merriam, 2009). The interview guide consisted of seven questions, one of which only targeted the teachers. The main aim of the questions was to capture the students' cognitive security awareness, but the additional question directed to the teachers concerned the formal security awareness with regards to how the ISP had been communicated to the students (see Appendix B). The interview guide was used in order to ensure that all the questions were covered, but, it proved necessary for there to be additional follow-up questions and re-formulations of questions. In order to measure the cognitive security awareness the questions were asked in such a way that it allowed the informants to openly elaborate on their perceptions regarding what was meant by security awareness. The discussions were thus not concerned with whether there was a right or wrong answer but rather the idea was to stimulate the respondent to dig more deeply into their cognitive security awareness.

Altogether 16 interviews were conducted on site in the respective schools – eleven with students and five with teachers. All interviews were recorded and thereafter transcribed.

3.2 Analysis

The data from the questionnaires were categorized according to the three levels of awareness: 1) formal, 2) cognitive and 3) behavioral. The questionnaires were compiled in a spreadsheet program in order to provide rapid and accurate calculations. The results for the two schools were merged but, were also compared in order to identify any differences. The qualitative data was transcribed and coded around the same three themes of security awareness. The coding strategy was thus selective and we intentionally looked for themes that could fit into one or more of these categories. The interviews were compared across and between the schools in order to identify differences and similarities.

All the findings were compared to, and viewed in the context of, the schools' formal ISPs. All transcripts were coded by the three first authors independently and thereafter compared in order to arrive at a shared interpretation. Two answers from two different interviewees were removed since the questioning was determined to have been too leading.

4. Findings

The findings concerning how students in 1:1 schools comply with the school's ISP will be presented, firstly with regards to the findings for each security awareness level and thereafter by providing a more holistic assessment, combining the three levels.

4. 1 Formal Security Awareness

The two schools ISPs have been analyzed, as has how these policies have been communicated to the students, the reason being in order to set the baseline with regards to what it is that the students have to comply with and how well they are aware of this. Both policies are substantial, covering everything from areas of responsibility to copyright protection, measures to be taken when violations occur, what is and is not allowed to be done. The two ISPs are similar in relation to restrictions and prohibitions. There is one difference, however – the school in municipality B has additional rules dealing with the maintenance of the laptop. For example, this school's ISP also includes rules concerning how the laptop should be transported to and from school (for a full comparison go to appendix C). The ISPs are communicated by teachers at meetings with students and parents, through signed contracts and via the schools' homepage:

> "We were informed during a meeting with our supervisor and then we had this parent-teacher meeting and then we signed this contract with all the rules"

Both teachers and students mentioned these channels for communication and the ISPs have thus been communicated as intended. On a day-to-day basis it was discovered that the preferred channel for inquiries about the ISP is the teacher. Only 11 students (8%) use the homepage when they are unsure about the rules. 74% of the students state that when in doubt they turn to their teacher:

> "The teachers are the ones who told us the rules and they do it on a continuous basis – especially if they discover a violation of the rules"

In practice, this means that it is the teacher who communicates the policy on a daily basis – something which places significant responsibility on the many different teachers with regards to the mediation of the exact official ISP. It would, in this regard, have actually been better if the students had, instead, used the homepage, as it would then be possible for the school to ensure that the ISP, including any potential changes, is communicated with the same message, simultaneously, to all students. Being a student in a 1:1 school (i.e., being provided with your personal laptop) provides the opportunity to access the homepage at any single minute of the day.

In summary, an investigation in relation to the formal security awareness, which is the schools' ISPs, they were found to be both comprehensive and broad. The schools have also managed to communicate the ISP, i.e., they have used the communication channels available and teachers and students verify that the ISP has been communicated and understood.

4.2 Cognitive Security Awareness

Our analysis of interview transcripts and questionnaires shows that, overall, the students are aware of the school's ISP. All the interviewed students stated that they had been informed about the school's ISP. In both of our researched schools, the rule is that no student can receive a laptop until they have been thoroughly informed about the ISP and signed a contract including the rules. The ISP is communicated through these contracts and through the teacher. However, being informed does not automatically mean that the students fully understand the policy or why it is important to comply with it. One observation made when reading through the policy on the respective homepages was how formal and bureaucratic the language was, thus, possibly making it difficult for 13-14 years-olds to understand. In the questionnaire two test-questions about the ISP were included in order to determine whether they really knew what the policy prescribed. The question regarding whether the school had the right to check the content of the computer, something which was explicitly described in the ISPs, yielded a positive answer from 64% of the students, but the others were unsure about this aspect. The other "test"-question concerned whether the students were aware that there would be consequences if the school's ISP was broken and this, likewise, was a fact that was not known by all – with only 52% of the students being aware of this.

When asked how they protect their computer and the schools IT-system, the students answered with physical and practical aspects relating how they handle the laptop gently, how they use laptop cases, keep the computer on the table or desktop or how they do not lend it to someone else.

> "I am very careful with it, I do not lend it to anyone, I put it away in the locker, I turn it off, I lock it"

Other interview questions had the intention of capturing which rules the students thought were important to follow and what they were not allowed to do. The most common replies with regards to what they are not allowed to do refer to illegal downloading and surfing on illegal sites. Additional aspects mentioned were "no Facebooking during lessons", "not damage the computer", "not visit pornographic sites and not use UTorrent or Piratebay":

> "You're not allowed to drop the laptop on purpose, you're not allowed to hit it, and you're not allowed to enter inappropriate sites, inappropriate sites such as Piratebay and the like"

One central behavior of interest to us was regarding how often the students talk about the ISP. Our belief was that the more frequently the ISP was discussed, the more cognitively aware the students would be and that this cognitive awareness would influence their behavior. We wanted to know if this was a"living document" in the everyday practices of the school. Our students, however, did not see themselves as frequently discussing the policy – 56% said they never or rarely discussed the policy whereas 36% said they "sometimes" discussed the policy.

In acknowledging that the ISP has been well communicated and that most students are cognitively well aware of the policy, the next section presents how the students act on this formal and cognitive awareness.

4.3 Behavioral Security Awareness

Our findings show that, in the majority of cases, the students comply with the ISP. Some security behaviors of interest to us concerned passwords and other physical protections of the laptop. In this case,, it was determined that a majority of the students (59%) did not use the same password when logging on to the school-network as when logging on at other places. In the ISP, this is formulated more as a personal responsibility, but the students appear to take this seriously (more seriously than most people we know of!). The students also change their password regularly, generally assisted by their teacher.

In the schools' ISPs there are also rules about not allowing other people to use the computer – a rule that the students comply with rather well. In municipality B, there is an explicit rule about the computer not being allowed to be borrowed by a third party since

this is not covered by the insurance policy. In municipality A, the policy states that the computer is not allowed to be left unattended. The students clearly abide by this rule – 96% of the students claim that they never lend their computer to someone else or, that in those cases when they do, they sit next to that person. The students are also very careful about not leaving the laptop unattended. If they have to leave the computer for a short while they either lock it (54 %) or ask a friend to take care of it (41 %).

In the schools' ISPs, advice is provided with regards to avoiding viruses entering the laptops but nothing is stated regarding what to do if this does occur. When asked what the students do when, or if, a virus is found on their machine, the majority (58 %) of students say they contact the IT-support. A few others remove the virus themselves or ask friends for assistance. A surprisingly large number of students claim that they never have viruses on their computers.

So far, the students' actions are in parity with the school's ISP. However, when the questions turn to games, file-sharing programs and so forth, the picture of the all-complying students starts to fall apart. From the interviews it was determined that the students are aware that they are not allowed to download copyright-protected or illegal material, but, from the questionnaire responses, it was discovered that more than half of the student population (52 %) do download copyright-protected material. It is possible that the students are not aware that this is copyright-protected material or, possibly, this was not of importance to them (ethics/moral) - many of the students also reported that they were not aware that the school had the authority to check their computers and that there would be consequences associated with violations.

In investigating which programs the students have on their computers, and what they do when they require a new program to be installed, it was; again, felt that it was necessary to firstly consult the ISPs. It was determined that in municipality B no other programs, other than those which were pre-installed, were allowed (not even Spotify, Skype etc) whereas municipality A , places more emphasis on the student's responsibility and judgment (illegal and copyright-protected material is of course strictly forbidden).

In the students' responses it was found that 47% of the students in municipality B, despite the rules, have Spotify on their computers and, in municipality A, 51 % of the students have Utorrent installed (and 87 % Spotify). Additionally, it was determined that when the students want to use programs, other than those provided by the school, 40 % of the students in municipality B download and install programs from free downloading sites. In municipality A, the equivalent is 60%. Hardly any of the students buy a license or install programs from a CD.

When asked whether the same rules for illegal downloading applied at home – something which both ISPs are very clear about – it was discovered that over a third (38%) thought that totally different rules applied at home. 53 % of the students admit to illegal

downloading on their computers when they are at home. Apart from illegal downloading, what differentiates the computer activities at home is that the students chat, play games and browse the Internet more:

> "… at home I tend to surf around more unless I have homework to do"

A final question concerned whether the students had, at any time, deliberately violated the ISP and 41 % of the students admitted to this. The violations admitted to referred to the illegal downloading of films, music or games, having the laptop in their lap and Face booking during class. However, a significant difference was found between the two schools. In municipality A, 62 % admitted to this whereas, the equivalent for municipality B was only 11 %. The few that broke the rules in municipality B also mentioned rather mild violations such as having the laptop on their lap:

> "Yes, for instance I have had the computer on the lap on occasions - something which is not allowed"

4.4 Students' Security Awareness and Compliance

In summary, we have discovered that the vast majority of students (82 %) use the correct channels for information desired by the schools when in doubt regarding the ISP rules. The students have also signed a contract and do turn to their teachers when this is required. The students are thus well aware of what is allowed and what is not. Despite this, it has been determined that almost half of the students in municipality B have Spotify installed on their computers (which is forbidden) and 62 % of the students in municipality A admit to breaking the ISP rules. These students, who intentionally break the rules by their actions, still have a cognitive security awareness that is in harmony with the ISP. The behavioral security awareness obviously has some shortcomings that will now be discussed.

5. Discussion

Thus, how well do students in 1:1 schools comply with the school's ISP? Our findings show that the students' security awareness corresponds, to a large extent, with the schools' ISPs, but the findings also show that the formal, cognitive and behavioral security awareness are not always in harmony with each other. In the analysis of the students' behavioral security awareness, it was found that, despite the fact that they were aware of the rules, they occasionally violated them. As previously mentioned, an efficient

ISP requires the users to be aware of it and act upon it (Puhakainen, 2006) and any shortcomings should be dealt with. Puhakainen (2006) also suggests three approaches regarding how to influence the users' behavior: persuasive communication and education; active participation and; punishments and rewards. However, communication and education of the policies has already been conducted, active participation (i.e., involving students in the design of ISPs) has not been possible, and the punishment and reward approach (reward of not being punished) is already implemented in the schools. So how can security compliance in 1:1 schools be improved?

We believe that non-compliance should be understood based on an understanding of the users (Hedström et al., 2011a) and the users' underlying reasons for following or not following information security policies and regulations. This means that non-compliance should be addressed through a study of the rationality of the user. Social actions, such as information security behaviors, can be rational as well as non-rational, and effective countermeasures should address both these types of social actions. Security countermeasures should, from this perspective, be chosen based on the cognitive processes underlying the behavior of the users regarding information security. We believe that such a perspective will create more usage of secure information systems, as countermeasures targeting the cognitive process underlying users' security behavior will last longer than targeting overt behavior (cf. with security culture Von Solms and Von Solms 2004). This is very clear in the examples from this case, where the students choose to download copyright protected or illegal material (software piracy) to their computers, in spite of the countermeasures in place. In order to effectively manage information security, and create a secure information environment, the managers must talk to the students, and understand why they choose to misuse the IT-systems at school. It is also necessary to provide a better explanation to the students as to why it is important to comply with such a rule and what the consequences are for them, as well as for the school, if they caused a security breach. At this point, perhaps peer education could be effective. The policies must also be contextualized and in harmony with the organizational culture. If not, the policies and guidelines should be developed in order to make them practical. The rule about not having the computer in your lap appears to be illogical. It might be sensible to take a closer look at that rule, and change it, as well as explain it, so that it makes sense to the students. Rules will not be followed if they appear to be meaningless.

Viewing these findings from the perspective of the increasing number of 1:1 schools, it is necessary for teachers and adults in general, to be aware of the students' security awareness and behavior appears to be within these schools. Not only because there is a risk for the very schools themselves but because the students' behavior will be reflected in how they think and act upon security issues in their future life and work environment.

As discussed in the introduction section, risky unsafe Internet usage does not decrease by itself, but, consideration is given as to how schools shape their students and prepare them for the future – it should be possible for this to also be tackled in relation to security awareness. As also discussed, students are generally more prone to risky behavior because they are less experienced and, in this regard, teachers in 1:1 schools have an important role to play. Teachers in these schools have a golden opportunity to discuss and explain the safety risks involved in relation to the use of a computer. In doing so, they should also be aware of the students' underlying motives for violating the rules – our findings show that, otherwise, these discussions are futile.

6. Conclusion

The objective of this paper was to investigate whether, and to what extent, secondary school students comply with information security policies. Our findings show that while the students' security awareness does, to a large extent, correspond with the schools' ISPs, it was also discovered that most students do, occasionally, violate the rules. The violations mainly referred to the downloading of copyright protected or illegal material, but also to "minor" violations such as using Facebook during class or having their laptop on their lap. Whereas this non-compliance may not be a surprise, from an information security perspective, it is important to know how to address the violations. We believe that the way forward is to address this non-compliance by investigating the rationality of these students. It is necessary to determine why the students behave in this manner, i.e. why they intentionally or unintentionally violate the rules. In order to effectively manage information security, teachers and school management should simply sit down and talk to the students, and they must also provide a better explanation to the students regarding the content of the ISP as well as why it is important to comply with the rules.

The article contributes to the field of computers in public education by better conceptualizing the notion of rationality when discussing security compliance in 1:1 schools. Whereas most security discussions revolve around the ideas of students "misbehaving" and the technical measures requiring to be taken, we believe the focus should shift to the many very different reasons why students do not always comply with security policies. In a situation where the 1:1 approach is spreading rapidly among schools, studies of students' security awareness and behaviour are urgent, but so far the field is under examined.

References

ALBRECHTSEN, E. & HOVDEN, J. 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security,* 29**,** 432 – 445.

ANDERSSON, S. B. 2006. Newly qualified teachers' learning related to their use of information and communication technology: a Swedish perspective. *British Journal of Educational Technology,* 37**,** 665-682.

ATKINSON, S., FURNELL, S. M. & PHIPPEN, A. 2009. Securing the next generation: enhancing e-safety awareness among young people. *Computer Fraud & Security,* July**,** 13-19.

BAKER, W. H. & WALLACE, L. 2007. Is information security under control? Investigaing quality in information security managment. *IEE security & privacy,* January/February**,** 36-44.

BEBELL, D. & KAY, R. 2010. One to One Computing: A Summary of the Quantitative Results from the Berkshire Wireless Learning Initiative. *The Journal of Technology, Learning, and Assessment,* 9**,** 5-59.

BJELVENMARK, J. 2011. *One to One - a student perspective on computer use in Swedish high school.* Bachelor, Linköpings universitet.

BULGURCU, B., CAVUSOGLU, H. & BENBASAT, I. 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly,* 34**,** 523-548.

DHILLON, G. 2007. *Principles of information systems security: text and cases*, John Wiley & Sons.

FRIED, C. B. 2008. In-class laptop use and its effects on student learning. *Computers & Education,* 50**,** 906-914.

GAUNT, N. 2000. Practical approaches to creating a security culture. *International Journal of Medical Informatics,* 60**,** 151-157.

HADEED, L. 2000. Effects of using the anytime, anywhere learning model (laptop program) for the enhancement of problem solving and critical thinking skills. Available: http://www.projectred.org/uploads/Effects_of_AA_Learning.pdf [Accessed March 29, 2012].

HEDSTRÖM, K., KOLKOWSKA, E. & KARLSSON, F. 2011a. Value Conflicts for Information Security Management *International journal of Strategic Information Systems,* 20**,** 373-384.

HEDSTRÖM, K., KOLKOWSKA, E. & KARLSSON, F. 2011b. Value Conflicts for Information Security Management *International journal of Strategic Information Systems,* 20**,** 373-384.

HEDSTRÖM, K., KOLKOWSKA, E., KARLSSON, F. & ALLEN, J. P. 2011c. Value conflicts for information security management *Journal of strategic information systems,* 20**,** 373-384.

HERATH, T. & RAO, R. H. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems,* 18.

INC, L. C. C. 2009. One-to-One Mobile Computing - Literature Review. *In:* EDUCATION, A. (ed.). Alberta: Department of Education and Training.

JOHANNESSON, L. 2011. *Poängen med en-till-en? Sex lärares uppfattningar av den personliga datorns roll i lärprocessen (In English: What is the point with one-to-one? Six teachers perceptions of the role of the personal laptop for the learning process).* Master, Högskolan i Jönköping.

LIGINLAL, D., SIM, I., KHANSA, L. & FEARN, P. 2012. HIPAA Privacy Rule compliance: An interpretive study using Norman's action theory5. *Computers & Security,* 31**,** 206-220.

MAGKLARAS , G. B. & FURNELL, S. M. 2004. The Insider Misuse Threat Survey: Investigating IT misuse from legitimate users. *Proceedings of the 5th Australian Information Warfare & Security Conference.* Perth Western Australia.

MERRIAM, S. B. 2009. *Qualitative Research: A Guide to Design and Implementation*, Jossey-Bass.

NASH, K. S. & GREENWOOD, D. 2008. The global state of information security CIO Magazine, PriceWaterhouseCoopers.

OATES, B. J. 2008. *Researching Information Systems and Computing,* Cornwall, Sage.

PECK, K. & SPRENGER, K. 2008. One-to-One Educational Computing: Ten Lessons for Successful Implementation. *In:* VOOGT, J. & KNEZEK, G. (eds.) *International Handbook of Information Technology in Primary and Secondary Education.* Springer US.

PUHAKAINEN, P. 2006. *A design theory for information security awareness.* PhD Doctoral, University of Oulu.

REZGUI, Y. & MARKS, A. 2008. Information security awarenes in higher education: An exploratory study. *Computers & Security,* 27**,** 241-253.

ROGERS, E. M., KINCAID, L. & BARNES, J. 1981. The convergence model of communication and network analysis. *In:* ROGERS, E. M. & KINCAID, L. (eds.) *Communication Networks: Toward a New Paradigm for Research.* New York: Free Press.

SILVERNAIL, D. & LANE, D. 2004. The impact of Maine's One-to-One Laptop Program on Middle School Teachers and Students. *In:* INSTITUTE, M. E. P. R. (ed.). Maine: Maine Education Policy Research Institute.

SIPONEN, M. & MAHMOOD, M. A. 2010. Compliance with Information Security Policies: An Empirical Investigation. *Computer,* 43**,** 64 - 71

SIPPONEN, M., WILSON, R. & BASKERVILLE, R. 2008. Power and Practice in Information Systems Security Research. *International Conference on Information Systems 2008 (ICIS 2008).* Paris, Farnce.

STANTON, M. J., KATHRYN, S. R. & MASTRANGELO, J. J. 2005. Analysis of end user security behaviors. *Computers & Security,* 24**,** 124-133.

VAAST, E. 2007. Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare. *Journal of Strategic Information Systems* 16**,** 130-152.

VALCKE, M., DE WEVER, B., VAN KEER, H. & SCHELLENS, T. 2011. Long-term study of safe Internet use of young children. *Computers & Education,* 57**,** 1292-1305.

VON SOLMS, R. & VON SOLMS, B. 2004. From policies to culture. *Computers & Security,* 23**,** 275-279.

VROOM, C. & VON SOLMS, R. 2004. Towards information security behavioural compliance. *Computers & Security,* 23**,** 191-198.

WILLIAMS, P. A. H. 2008. When trust defies common security sense. *Health Informatics Journal,* 14**,** 211-221.