INFORMATION TECHNOLOGY AND SECURITY IN SCHOOLS
A Research Agenda

Hannakaisa Isomäki
Department of Mathematical Information Technology, Computer Science Teacher Education, University of Jyväskylä
P.O.Box 35, 40014, Finland

Keywords: Information security, Schools, e-Learning, End-user security behaviour, Information security culture, Pedagogical software, Security management, Research methods.

Abstract: In this position paper I discuss a research agenda for studying security issues particularly related to secondary and high schools. I argue that despite of its topicality and significance to successful functioning of schools, the issue of information technology (IT) and security in schools is not getting enough research input. In the educational environment, which includes various areas of computer-supported learning, the scope of security ranges from human-centred to technology-centred issues. Both of these deal with information security in a socio-technical educational context, the first emphasizing human activity and the latter IT. I present these categories as necessary research proposals here. The human-centred topics include end-user security behavior – as intertwined with the use of technology while learning and teaching in socially embedded virtual worlds – and information security culture in schools. The technology-centred topics include information security of pedagogical software and IT applications for the management of school security.

1 INTRODUCTION

A pertinent recent societal change concerns the security and safety of learning, teaching and administration within the educational system. Traditionally, school security has been evaluated through incidents of random schoolyard violence and physical threats to students and staff (e.g., Agron and Anderson, 2000). However, this viewpoint does not address the whole issue of security in learning, teaching and school management.

While educational technologies are increasingly used as promoters of various types of E-learning practices, it is essential to study students', teachers' and school managements' interrelationship with information security, particularly of users' security related activities in IT-supported educational environments, and the demands for information security and privacy protection capabilities of educational technologies.

Users of IT at large are considered to be a major threat for information security in organisations (e.g., Leach, 2003; Furnell, 2008). Regarding educational environments, it is essential to consider information security of on-line learning from the viewpoint of end-users (Furnell and Karweni 2001). In schools, information security should be seen as a tool for providing E-learning environments that meet students' and teachers' needs for safe and secure spaces for studying and teaching. In these kinds of educational spaces students can feel as belonging to a certain group, feeling trust, respect and social bonding (Allan and Lewis, 2006; McInnerney and Roberts, 2004).

Due to the ongoing pervasive reconfiguration of contemporary society's technical and social infrastructures integrated by digitalization (Tilson, Lyytinen and Sörensen, 2009), school information security and safety needs to be addressed from the viewpoint of infrastructure. Infrastructure refers to hardware (computers and communication technologies), network services (software, file services, FTP etc.), and human infrastructure (knowledge, skills and experiences) (Broadbent, Weill and St. Clair, 1999). Nowadays, information security services should be seen as part of infrastructure, for example, Furnell, Onions, Knahl, Sanders, Bleimann, Gojny, and Roder (1998) argue that carrying out network-based studying and learning demands paying attention to information security aspects such as authentication

Isomäki H. (2010).
INFORMATION TECHNOLOGY AND SECURITY IN SCHOOLS - A Research Agenda.
In *Proceedings of the 2nd International Conference on Computer Supported Education*, pages 325-330
DOI: 10.5220/0002853603250330

and accountability, access control, intrusion detection, protection of network communications and non-repudiation issues.

In brief, the scope of IT-related security in the educational environment, including various types of computer-supported learning, covers both human-centred and technology-centred issues. These both deal with information security in a socio-technical educational context, but while the first emphasises human activity the latter puts stress on IT. The socio-technical approach focuses here to the mutual interactive effects between humans and technology when technology both constitutes human practice and is constituted by human agency (Orlikowski, 1992). From a human-centred view, when constituting human practice, technology both facilitates and constrains human endeavour. The way technology facilitates or constrains security in educational environments is of utmost importance regarding successful functioning of learning, teaching and studying in contemporary secondary and high schools. In particular, it is important to investigate how pupils and teachers experience IT related security and safety, i.e., how technology facilitates or constrains their work in schools in terms of IT related security. From a holistic viewpoint, it is essential to clarify how IT related security appears in schools in the level of organisational culture.

From a technology-centred view, i.e., technology being constituted by human agency, it is essential to design and develop IT security applications with respect to end-user security behaviour and awareness. Special attention is required to both create appropriate guidelines for E-learning related risk assessments and build slick implementations for both pedagogical software and security maintenance in school organisations. However, despite its topicality and significance to successful functioning of schools, the issue of IT and security in schools is not getting enough research input.

In this position paper I present both human-centred and technology-centred topics as research proposals to promote information security and safety in schools in terms of IT. The topics include end-user security behavior as intertwined with the use of technology while learning in socially embedded virtual worlds, and information security culture in schools. Technology-centred topics include security of pedagogical software and information technology applications for the management of school security. In addition, I disclose theoretical and methodological commitments for studying the topics.

2 END-USER SECURITY IN E-LEARNING

E-learning is often seen as an activity of technology-enhanced learning communities involved in computer-supported collaborative learning that is promoted by new technologies, such as Web 2.0 and social media (Pöysä and Häkkinen, 2009). End-user security in this context concerns individuals' prospects to be safely involved in virtual worlds and E-learning communities. The information security risks here concern both external and internal risks for security and privacy violations. External risks, for example, identity theft, phishing, worms, IP spoofing and other malicious attacks, require competence in protecting against malicious software or other attacks with anti-virus and firewall programs, and knowledge about how to control access to one's computer or user account (Osika Reed and Sharp, 2003). The issue here is that the use of such general security technologies is seen difficult and unmotivating to pupils and even teachers (e.g., Lampson, 2009). One essential line of research confronting these problems concerns usability of security software (e.g., Chatziapostolou and Furnell, 2007).

Unfortunately, information security risks may also appear in E-learning communities and virtual worlds. Internal risks such as social engineering and knowledge breaches may violate students' privacy while studying. Given that users' in general seem quite unaware of security risks (e.g., Rezgui and Marks, 2008), it is worth noticing that students still feel information security potentially having an impact also on studying and learning processes that take place in computer-supported collaborative learning communities (Isomäki, Päykkönen and Räisänen, 2008).

In order to develop understanding on how to build students' trust in various types of E-learning, their experiences of information security in E-learning environments should be intensively studied. An adequate approach would be in line with theorisations of user experience (UX), which disclose an experiential perspective on users' internal state, characteristics of the system in use, and the interaction context (Hassenzahl and Tractinsky, 2006). With a framework combined of these three viewpoints, the UX approach could open up the human side of information security, which is seen as a major threat to securing information (e.g., Leach, 2003; Furnell, 2008), and the weakest link of the security chain (Tjhai & Furnell, 2007), also in educational environments.

The UX approach employs methodologies rooted in phenomenology, such as cultural studies on UX (McCarthy and Wright, 2004), and other qualitative methods used, for example, in investigations on co-experiences (Battarbee, 2003). Users' experiential interaction with applications of educational technologies in school context is seen as a continuum of processes within which users actively engage with learning experiences. With the UX approach, for instance students' awareness of information security in learning settings and many experiences of information security's impact on different types of E-learning could be clarified. In the same way, the UX approach could be employed in users' demands for information security and privacy protection capabilities of educational technologies, as well as in their strategies for managing security in socially embedded virtual worlds.

To be able to consider information security in schools from a viewpoint that facilitates socio-technical understanding of IT-related security on an organisational level that incorporates the behaviour of individuals and groups of people to the organisational facilities and norms, the concept of information security culture (ISC) needs to be implemented in the study of schools. ISC is a newish concept, and its definition is not yet stabilised. In literature, ISC is considered from many viewpoints, namely: ISC as an aid in protecting valuable assets, ISC as a holistic issue forming a part of the broader corporate culture, ISC as a solely human aspect, ISC as information security governance, and ISC as an issue of organisational learning and knowledge creation in enterprises (Mazhelis and Isomäki, 2009). Some researchers also connect the combination of corporate culture, governance and information security to information security obedience (Thomson and von Solms, 2005).

The theoretical commitments that seem most appropriate for understanding information security culture in school settings include a constructionist stance, the view of learning as socially constructed and mediated (e.g., Lave and Wenger, 1991), and an insistence that information security culture should be studied on the basis of concrete discursive practices and interactions while using IT in learning, teaching, or management of the school. Analyses of ISC in schools would disclose various organisational level issues of end-user security behaviour intertwined with the use of educational technology. A qualitative approach facilitates also the study of different genres or social rules producing social order within information security culture and its dissemination, students', teachers' and rectors' authentic strategies for managing security as an everyday problem, and power relations inherent in a particular information security culture.

3 INFORMATION SECURITY OF PEDAGOGICAL SOFTWARE

Typical for the development of information security guidelines and practices of pedagogical software is that there are both generic and E-learning specific requirements (e.g., Eibl and Schubert, 2008; Furnell, Onions, Knahl, Sanders, Bleimann, Gojny, and Roder, 1998). (Weippl 2005) also attends to both generic and E-learning specific security requirements for systems used in IT-supported learning. The generic requirements include secrecy, integrity, availability and non-repudiation. Secrecy denotes that users may obtain access only to those objects for which they have received authorization, whereas integrity means that only authorized users or processes are permitted to modify data or programs. According to Weippl (2005, 5), availability is also a security concern. Justification for this is pedagogical in that students' productivity decreases dramatically if network-based learning applications, such as WebCT, FirstClass and Optima, are too slow or not available due to denial-of-service attacks. Non-repudiation presumes that users are able to plausibly deny having carried out certain actions, or, if a user has provided or changed a certain piece of information he or she cannot deny having done it. For instance, if some grades of students are altered, it must be possible to reliably trace the source of those changes.

The generic requirements do not usually require any specific skills or performance of IT support staff in educational institutions but are included in nondescript security risk analyses and maintenance. Non-repudiation issues can, however, be cumbersome in that they may cause risks for users' privacy. For instance, if students' all actions are made traceable in the net by using, e.g., spyware, it may endanger privacy and diminish trust building in E-learning environments.

Information security requirements for E-learning often concern unauthorized use of digital content, trust, exams, and organization (Weippl, 2005, 6). The first of these may be tricky to address, because in addition to people who do not have authorized access to the content, people who have legitimate access to the content may copy or modify it without permission and/or disseminate it further.

As mentioned above, trust is essential in the context of learning. A fundamental security requirement regarding trust is that students must be able to rely on the accuracy of the content and that they are provided space for unobserved reading. In addition, they must be able to trust that the authors' identity is authentic. This is of utmost importance because especially undergraduate students tend to trust all kinds of information sources and accept whatever they read as true (Graham and Metaxas, 2003). Exams are a usual concern in terms of reliable performance by students. Non-repudiation issues regarding educational institutions' software used in teaching often concentrate on exams, especially when teachers attempt to find out how to prevent students from cheating in electronic tests (Graf, 2002).

Finally, organization refers to the human side of information security, and in that sense it is reminiscent of the issues unfolding the information security culture in schools. Weippl (2005, 8) argues that the security procedures put into use in educational organisations must be simple in order to guarantee the compliance of users.

Information security of pedagogical software is a theme that needs a lot attention from research and development. Successfully implemented information security solutions have potential to raise students' experiences of trust and safety, support the forming of a secure virtual community, and thus promote learning in socially embedded virtual worlds. Generic information security issues (confidentiality, integrity, availability, authenticity and non-repudiation) may or may not be covered in educational organisations. In addition, special attention is required to both create appropriate guidelines for E-learning related risk assessments, increase pupils' information security awareness, and to build slick implementations of security maintenance and control for pedagogical use of E-learning software. Because information security of software used for pedagogical purposes is a context-dependent issue, the socio-technical paradigm is needed in research. This way the fundamental nature and also everyday practices of E-learning are included as a focus areas in investigations. From the methodical viewpoint, research efforts of this topic necessitate a design science approach (Hevner, March, Park and Ram, 2004) with implications from software engineering and UX studies regarding educational technologies.

4 IT APPLICATIONS FOR MANAGEMENT OF SCHOOL SECURITY

At present, capabilities for developing and maintaining school security and safety are regarded highly, and several training programmes are carried out to increase awareness and skills for secure and safe working in schools. A central aim is to be prepared for creating policies that integrate different sectors of security, i.e., occupational safety, rescue operations and civil defense, into a single plan which serves as the blueprint for a workable procedure in a particular school. Despite a severe need for security in schools, IT-supported applications for security maintenance, management and control for schools are scarce.

Nevertheless, prior experiences in the United States have shown that IT-supported tools could have several advantages both in crisis management and school security in general (National Institute of Justice). Further, the traditional security surveillance technologies, such as video surveillance cameras and metal detectors, are disliked especially by boys (Brown, 2005). Modern IT-based applications, which are transparent to and interactive with the users, could help to improve both pupils' attitudes and school ambience towards a general acceptance of operations for school information security and safety.

Research efforts to fill the gap in computer-supported security management, maintenance and control of school security should be enhanced. New technologies, such as multimedia-based interactive IT-applications, could provide interactive and transparent tools for holistic school-specific security management. Methodical determinations in the development of new information systems are in line with the design science approach (Hevner, March, Park and Ram, 2004) with implications from software engineering and human-centred information systems development (Isomäki and Pekkola, forthcoming). This way the framework of design science entails more detailed software design issues, which are informed by human-centred development guidelines with respect to end-user security behaviour concerning learning, teaching or studying with IT applications. A special task would be to implement new methods for school specific security risk analysis, which generally includes identification of assets, estimation of threats and risks, setting priorities, implementation of controls and counter measures, and monitoring risks of the effectiveness of counter measures (Weippl, 2005).

Applications of IT have a lot of unexplored potential to contribute to management, maintenance and control of school security and safety. The results of this kind of research would benefit educational organisations in terms of the state of their security and safety, and would also be very useful tools for teachers, students and rectors in their everyday practices of schoolwork. The results would be useful also in security related training. Informing students and school staff about IT-supported security management and information security could increase their awareness of security and safety, not just for their work but their life in current information society. Increased security awareness is especially important to adolescents who need to participate in taking care of their virtual selves.

5 CONCLUSIONS

In this position paper I have discussed information technology and security in schools in terms of a research agenda. I have insisted that school security is of utmost importance requiring substantial input to research and development activities. Security in the educational environment including various types of computer-supported learning, teaching and management activities focuses on both human-centred and technology-centred issues. In the current holistic and interactive reconfiguration of contemporary society's technical and social infrastructures, both human-centred and technological issues need to be scrutinised in their socio-technical educational context.

Important human-centred topics include end-user security behaviour as intertwined with the use of technology while learning in virtual worlds, and information security culture in schools. In educational settings the issue of end-user security behaviour should be seen as multidimensional phenomenon interlaced with the use of technology, learning, communicating, and teaching. The theoretical commitments and central arguments that seem most appropriate for understanding information security culture and also end-user security behaviour in school settings include a constructionist stance, the view of learning as socially constructed and mediated, and an insistence that information security culture should be studied on the basis of concrete discursive practices and interactions while using IT in learning, teaching, or management of the school. Adjustments of theories and concepts for empirical research require conceptual-theoretical approach.

The necessary technology-centred topics include security of pedagogical software and applications of IT for maintaining school security. The first requires that our attention is destined for both generic and E-learning specific information security requirements for systems used in IT-supported learning. The latter discloses that IT-supported applications for security maintenance, management and control for schools are scarce. However, up-to-date IT-based applications, which are transparent to and interactive with users, could help to improve students' attitudes and school ambience towards acceptance of operations for school information security and safety. A special task in this area is to implement some procedures of a school specific security risk analysis into the IT applications development method. Methodical determination regarding technology-centred topics is in line with the design science approach with implications from software engineering and human-centred information systems development. This way the prescriptive framework of design science entails more detailed software design issues informed by human-centred development guidelines with respect to end-user security behaviour in educational environments.

REFERENCES

Agron, J., Anderson, L. 2000. School Security by the Numbers. *American School & University*, School security supplement.

Allan, B., Lewis, D. 2006. The Impact of Membership of a Virtual Learning Community on Individual Learning Careers and Professional Identity. *British Journal of Educational Technology*, 37(6), 841–852.

Battarabee, K. 2003. Defining Co-experience. *In Proceedings of the 2003 Designing Pleasurable Products and Interfaces (DPPI) Conference* (pp. 109-113). New York: ACM Press.

Broadbent, M., Weill, P., St. Clair, D.R. 1999. The Implications of Information Technology Infrastructure for Business Process Redesign. *MIS Quarterly* 23(2), 159-182.

Brown, B. 2005. Controlling Crime and Delinquency in the Schools: An Exploratory Study of Student Perceptions of School Security Measures. *Journal of School Violence*, 4(4), 105-125.

Chatziapostolou, D., Furnell, S.M. 2007. Recording end-users security events: A step towards increasing usability. In P.S. Dowland and S.M. Furnell (Eds.) *Proceedings of the 2005-2006 Conference on Advances in Networks, Computing and Communications 4* (pp. 11-18). University of Plymouth, U.K.

Eibl, C.R., Schubert, S.E. 2008. Development of E-Learning Design Criteria with Secure Realization Concepts. In *Proceedings of the 2008 ISSEP Confer-*

ence, LNCS 5090, (pp. 327-336). Berlin: Springer-Verlag.

Furnell, S. 2008. End-user Security Culture: A Lesson that Will Never be Learnt? *Computer Fraud & Security*, 4, 6–8.

Furnell, S.M., Onions, P.D., Knahl, M., Sanders, P.W., Bleimann, U., Gojny, U., Roder, H.F. 1998. A Security Framework for Online Distance Learning and Training. *Internet Research*, 8(3), 236–242.

Furnell, S.M., Karweni, T. 2001. Security Issues in Online Distance Learning. *VINE*, 123, 28-35.

Graf, F. 2002. Providing Security for eLearning. *Computers & Graphics* 26(2), 355–365.

Graham, L., Metaxas, P.T. 2003. Of course It's True: I Saw it on the Internet!: Critical Thinking in the Internet Era. *Communications of the ACM*, 46(5), 70-75.

Hassenzahl, M., Tractinsky, N. 2006. User Experience: A Research Agenda. *Behaviour and Information Technology*, 25(2), 91-97.

Hevner, A.R., March, S.T., Park, J., Ram, S. 2004. Design Science in Information Systems Research. *MIS Quarterly* 28(1), 75-105.

Isomäki, H., Päykkönen, K., Räisänen, H. 2008. Secure Collaborative Learning Practices and Mobile Technology. In Putnik, G.D. & Cunha, M.M. (Eds.) *Encyclopedia of Networked and Virtual Organizations*. Vol III. (pp. 1407-1412). Idea Group Publishing.

Isomäki, H., Pekkola. S. (Eds.) (forthcoming). *Reframing Humans in Information Systems Development*. London: Springer-Verlag.

Lave, J., Wenger, E. 1991. *Situated Learning: Legitimate Peripheral Participation*. Cambridge: Cambridge University Press.

Lampson, B. 2009. Usable Security: How to Get It. *Communications of the ACM* 52(11), 25-27.

Leach, J. 2003. Improving User Security behaviour. *Computers & Security*, 22(8), 685–692.

Mazhelis, O., Isomäki, H. 2009. Information Security Culture in SMEs: State of the art. *Reports of the JIID project*. Information Technology Research Institute, University of Jyväskylä. (to be submitted to INC'10 conference).

McCarthy, J. & Wright, P. 2004. *Technology as Experience*. Cambridge, MA: MIT Press.

McInnerney, J., Roberts, T. 2004. Online Learning: Social Interaction and the Creation of a Sense of Community. *Educational Technology & Society,* 7(3), 73–81.

National Institute of Justice. The Appropriate and Effective Use of Security Technologies in U.S. Schools. *Research Report NCJ-178265*.

http://www.ojp.usdoj.gov/nij.

Orlikowski, W. J. 1992. The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science* 3(3), 398-427.

Osika Reed, E., Sharp, D.P. 2003. Minimum technical competencies for distance learning students. *Journal of Research on Technology in Education*, 34(3), 318–325.

Pöysä, J. and Häkkinen, P. 2009. Designing for contemporary learning communities dwelling with technologies. In Isomäki, H., Häkkinen, P. and Viteli, J. 2009 (Eds.) *Future Educational Technologies*. Reports of Information Technology Research Institute 20/2009. Jyväskylä: University of Jyväskylä Printing House.

Rezgui, Y., Marks, A. 2008. Information Security Awareness in Higher-education: An Exploratory Study. *Computers & Security*, 27(2), 241–253.

Tilson, D., Lyytinen, K. and Sörensen, C. 2009. Desperately seeking the Infrastructure in IS Research: Conceptualization of "Digital Convergence" as the co-evolution of social and technical infrastructures. In Isomäki, H., Häkkinen, P. and Viteli, J. 2009 (Eds.) *Future Educational Technologies*. Reports of Information Technology Research Institute 20/2009. Jyväskylä: University of Jyväskylä Printing House.

Tjhai, G.C., Furnell, S.M. 2007. Strengthening the Human Firewall. In P.S. Dowland and S.M. Furnell (Eds.) *Proceedings of the 2005-2006 Conference on Advances in Networks, Computing and Communications 4* (pp. 223-230). University of Plymouth, U.K.

Thomson, K.-L., von Solms, R. 2005. Information Security Obedience: A Definition. *Computers & Security* 24(1), 69-75.

Warren, M., Hutchinson,W. 2003. Information Security – An E-Learning Problem. *In Proceedings of the 2003 ICWL Conference,* LNCS 2783, (pp. 21-26). Berlin: Springer-Verlag.

Weippl, E.R. 2005. Security in e-learning. *eLearn Magazine* 3, 3-9.