

Petri Puhakainen

I suggest two topic areas related to human dimension of information security. It is possible to have several papers within both areas. These topic areas suit to all kinds of students. However, dealing with human behavior is never an easy task:)

Topic areas:

Topic area (1): Information security issues related to user behavior in pervasive computing environment

Topic area (2): Increasing pervasive system users' information security awareness

Background

Organizations will increasingly use pervasive systems for business purposes. It is obvious that the expected wide use of pervasive computing devices will attract criminals and information systems abusers. Consequently, not only the users' privacy and personal information, but also valuable business related information will be threatened. Many of the threats can be managed with the help of technology and procedural countermeasures. However, concentrating on technical and procedural aspects of information security alone is inadequate as users may not follow the existing technical and procedural information security measures. Effective information security requires that users are aware of and follow their security mission as described in their organizations' information security policies and instructions. Given this problem, it is important to explore user related information security issues in pervasive computing (Topic area 1) as well as means to solve these issues by increasing users' information security awareness (Topic area 2). In this case, awareness should be regarded as users' understanding of information security and, optimally, committing to it. As such, improved awareness should appear as users' behavioral changes towards compliance with information security policies and instructions.

Example references:

Topic area (1):

Zeckhauser RJ & Viscusi WK (1990) Risk Within Reason. Science 248: 559-563.

Fischhoff B, Slovic P & Lichtenstein S (1979) Weighing the risks: Which risks are acceptable?. Environment 21: 17-20, 32-38.

Fischhoff B, Slovic P, Lichtenstein S, Read S & Combs B (1978) How

safe is safe enough: A psychometric study of attitudes toward technological risks and benefits. Policy Sciences 9: 127-152.

Ajzen I (1991) The Theory of Planned Behavior. Organizational Behavior and Human decision Processes 50(2): 179-211.

Schlienger T & Teufel S (2002) IS security Culture: The Socio-Cultural Dimension in IS security Management. Proceedings of IFIP TC 11.

Sasse A, Brostoff S & Weirich D (2001) Transforming the 'weakest link' a human / computer interaction approach to usable and effective security. BT technology journal 19(3): 122-131.

Topic area (2):

Kabay ME (2002) Using Social Psychology to Implement Security Policies. In: Bosworth S & Kabay ME (eds) Computer Security Handbook, 4th edition. John Wiley & Sons, 32.1-32.16.

Parker DB (1999) Security motivation, the mother of all controls, must precede awareness. Computer Security Journal 15(4): 15-23.

Peltier T (2000) How to build a comprehensive security awareness program. Computer Security Journal 16(2): 23-32.

Straub DW (1990) Effective IS Security: An Empirical Study. Information Systems Research 1(3): 255-276.

Roper CA, Grau JA & Fischer LF (2006) Security Education, Awareness and Training: From Theory to Practice. Elsevier.

Herold R (2005) Managing an Information Security and Privacy Awareness and Training Program. Auerbach Publications.