# Chapter VI
# Information Security Culture as a Social System: Some Notes of Information Availability and Sharing

**Rauno Kuusisto**
*Finland Futures Research Center, Turku School of Economics, Finland*

**Tuija Kuusisto**
*Finnish National Defense University, Finland*

## ABSTRACT

*The purpose of this chapter is to increase understanding of the complex nature of information security culture in a networked working environment. Viewpoint is comprehensive information exchange in a social system. The aim of this chapter is to raise discussion about information security culture development challenges when acting in a multicultural environment. This chapter does not introduce a method to handle complex cultural situation, but gives some notes to gain understanding, what might be behind this complexity. Understanding the nature of this complex cultural environment is essential to form evolving and proactive security practices. Direct answers to formulate practices are not offered in this chapter, but certain general phenomena of the activity of a social system are pointed out. This will help readers to apply these ideas to their own solutions.*

## INTRODUCTION

Information security issues can be considered as balancing between information availability and confidentiality. Organizations should be able to understand what kind of information shall be and will be available to ongoing and future activities and which parts of that shall be secured. This

information depends on situation and those phenomena that emerge from the complex networked working environment. Information security culture affects behind security management and technology. Understanding the nature of this complex cultural environment is essential to form evolving and proactive security practices. Direct answers to formulate practices are not offered in this chapter, but certain general phenomena of the activity of a social system are pointed out. This will help readers to apply these ideas to their own solutions.

System can be considered as a comprehensive wholeness that is constructed of nodes and connections between them (Castells, 1996). Nodes can be human beings, organizations, communities, technological systems, natural systems, or sub-systems of various entities (e.g., Checkland & Holwell, 1998; Checkland & Scholes, 2000). Information is something that is required to launch activity while moving between nodes. Security can be considered as a comprehensive concept that enables activities to be conducted in an environment that is stable and predictable enough to gain desired objectives. Culture is a social structure that tends to maintain certain patterns. This pattern maintenance is driven by information called values and valuations. Each actor has their own kind of cultural structures and values and their interpretation of other values (Schein 1992). It is obvious that a system contains several cultural phenomena that are exchanging value and other information. Culture itself is thus a *complex system* that evolves during time while various interacting actors are exchanging information.

The theoretical background is based on the theory of communicative action by Jurgen Habermas (1984, 1989). In this theory, Habermas is constructing a communicative system consisting of structures, activities, and information interacting in a social context on the basis of the sociological ideas of Talcott Parson. We are using this systemic construction as a basis, against which we are applying the concept of information security culture. Some examples of information sharing practices of various actors are presented to learn certain phenomena concerning the development of information security culture.

Interest in the security of information and knowledge has increased together with the development of coalitions between states and networks between public and private organizations. It is obvious that security activities are needed for protecting information vital to the functions of the states and organizations. (e.g., Finnish Government 2003 & OECD, 2002) The emphasis of security activities has been on the means to protect the confidentiality and integrity of information flows on those networks. However, keeping information confidential is not as challenging as the identification of critical information and core knowledge from all of the information available. That is the reason why we focus here on information availability. Modern societies and organizations depend on information and knowledge. They need to identify critical information and core knowledge and put them available either for internal use or for external use visible to customers, partners, and competitors to survive or to gain competitive advantage. So, states and organizations have to find a balance between the confidentiality and availability of information. They need this balance to identify and communicate information that suits their goals.

Information security culture can be seen as a concept that provides means to reach the balance between confidentiality and availability of information. Edward Waltz (1998) defines three major information security attributes as follows:

1. Availability provides assurance that information, services, and resources will be accessible and usable when needed by the user.
2. Integrity assures that information and processes are secure from unauthorised tampering (e.g., insertion, deletion, destruction, or replay of data) via methods such as encryption, digital signatures, and intrusion detection.